



부록

THE ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND DATA PROTECTION, ETC.*

Extracts - the data protection provisions only

Last Amended by Act No. 10138, March 17, 2010

CHAPTER I . GENERAL PROVISIONS

Article 1 (Purpose)

The purpose of this Act is to promote the utilization of information and communications networks, to protect the personal information of users utilizing information and communications services, and to build a safe and sound environment for the information and communications networks in order to improve the citizen's lives and enhance the public welfare.

Article 2 (Definitions)

(1) The terms used herein shall be defined as follows:

1. "Information and communications networks" shall mean the information and communications system under which telecommunications facilities and equipment as prescribed in Subparagraph 2 of Article 2 of the Framework Act on Telecommunications are utilized, or the telecommunications facilities and equipment, computers and the technology of using computers are utilized together to collect, process, store, search, transmit and receive information;
2. "Information and communications services" shall mean the telecommunications services as prescribed in Subparagraph 7 of Article 2 of the Framework Act on Telecommunications, and the provision of information or the intermediation of information services utilizing the telecommunications services;
3. "Information and communications service providers" shall mean the operators of telecommunications as prescribed in Subparagraph 1 of Article 2(1) of the

* Translated unofficially by Prof. Whon-Il Park, Kyung Hee University Law School.

Telecommunications Business Act and other persons who provide information or intermediate information services for profit utilizing the services rendered by the telecommunications service providers;

4. “Users” shall mean the persons who utilize the information and communications services rendered by the information and communications service providers;
5. “Electronic message” shall mean the standardized data in the form of document in which information is electronically compiled, sent or received, or stored by equipment, including computers, etc., that are capable of doing information processing;
6. “Personal information” shall mean the information pertaining to any living person, which contains the code, letter, voice, sound and image, etc. that make it possible to identify such individual by his/her name and residence registration number, etc. (including the information which, if not by itself, makes it possible to identify any specific individual if combined with other information);
7. “Incidents” shall mean accidents caused by such attack on the information and communications networks or related information systems as hacking, computer viruses, logical bomb, mail bomb, denial of service, high-powered electromagnetic wave, etc.;
8. “Information security industry” shall mean the industry related with development, production and circulation of information security products, or consulting for data protection, etc.;
9. “Bulletin boards” shall mean the computer programs or technological devices, regardless of their names, to which the users may post the code, letter, voice, sound, image, video clips and other information for the purpose of making public by using the information and communications networks;
10. “Communications billing services” shall mean the information and communications services carrying out the business as defined in the following items:
 - a. The business which claims and collects the prices of goods or services sold or provided by others together with the charges for the telecommunications services provided by itself; or
 - b. The business which transmits or receives the transaction data electronically, or conducts the settlement of charges as a proxy or intermediary so that the prices of the goods or services sold or provided by others may be claimed and collected together with the telecommunications service charges stated in Item a.

11. “Communications billing service providers” shall mean the operators who provide the communications billing services subject to the registration pursuant to Article 53; and
12. “Communications billing service users” shall mean the persons who purchase and use the goods or services by means of the communications billing services provided by the communications billing service providers.
 - (2) The definitions stated herein, except otherwise provided for in Paragraph (1), shall be subject to the Framework Act on Informatization Promotion.

Article 3 (Duties of Information and Communications Service Providers and Users)

- (1) Any information and communications service provider shall protect the personal information of users, and contribute to the protection of the rights and interests of such users and to the enhancement of its information utilization capability by rendering the information and communications services in a safe and sound manner.
- (2) Every user shall endeavor to help a sound information society take hold.
- (3) The government may assist the organizations of information and communications service providers and the organizations of users in carrying out their activities designed to protect the personal information and the youth in the information and communications networks.

Article 4 (Policy for Promotion of Information and Communications Network Utilization and Data Protection, etc.)

- (1) The Minister of Administration and Security, the Minister of Knowledge and Economy, and the Broadcasting and Communications Commission shall formulate a policy to lay the foundation for building an information society through the promotion of utilization and the secure management and operation of information and communications networks, and the protection of personal information of users (hereinafter referred to as the “promotion of the utilization of information and communications networks and data protection, etc.”).
- (2) The policy referred to in Paragraph (1) shall contain the matters stated in the following Subparagraphs:
 1. Development and distribution of technologies related to the information and communications networks;
 2. Standardization of the information and communications networks;

3. Activation of utilization of the information and communications networks such as the development of information contents and utilization services of the information and communications networks subject to Article 11;
 4. Facilitation of joint utilization of information via information and communications networks;
 5. Activation of utilization of the Internet;
 6. Protection of personal information collected, processed, stored and utilized via information and communications networks, and development and distribution of related technologies;
 7. Protection of the youth in the information and communications networks;
 8. Enhancement of safety and reliability of the information and communications networks;
and
 9. Other matters necessary to promote the utilization of the information and communications networks and data protection, etc.
- (3) In formulating the policy referred to in Paragraph (1), the Minister of Administration and Security, the Minister of Knowledge and Economy, or the Broadcasting and Communications Commission shall endeavor to coordinate such policy with the basic plan for promoting informatization as prescribed in Article 5 of the Framework Act on Informatization Promotion.

Article 5 (Relation with Other Acts)

The promotion of utilization of information and communications networks and data protection, etc. shall be governed by this Act except specially provided for in other acts; provided, however, that, in case this Act and the Electronic Financial Transactions Act compete to apply with respect to the communications billing services stated in Chapter VII, this Act shall prevail.

CHAPTER II. PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION

Translation of the provisions of Articles not related with data protection is omitted.

Articles 6-17 *Omitted.*

CHAPTER III. UTILIZATION OF ELECTRONIC MESSAGES VIA RELAYER

Articles 18-21 *Omitted.*

CHAPTER IV. PROTECTION OF PERSONAL INFORMATION

Section 1. Collection of Personal Information

Article 22 (Consent to the Collection and Utilization of Personal Information, etc.)

- (1) Any information and communications service provider shall, when it intends to gather user's personal information, notify the user of the whole matters stated in the following Subparagraphs, and obtain his/her consent thereof. The same shall apply to any change of the following Subparagraphs:
 1. The purpose of collection and utilization of personal information;
 2. The items of personal information collected hereunder; and
 3. The period of retention and utilization of personal information.
- (2) The information and communications service provider may collect and utilize the user's personal information without consent subject to Paragraph (1) in case any of the following Subparagraphs applies:
 1. Where, as for the personal information, which is necessary to perform the contract for the provision of information and communications services, it is evidently difficult to obtain ordinary consent on account of economical and technological reasons;

2. Where it is necessary to calculate the fees for the provision of information and communications services; or
3. Where special provisions exist in this Act or other acts.

Article 23 (Restrictions on Collecting Personal Information, etc.)

- (1) No information and communications service provider shall collect the personal information, including ideology, belief and medical record, etc., which is likely to excessively infringe upon the right, interest and privacy of the relevant user; *provided, however,* that the same shall not apply where the consent of the user is obtained pursuant to Article 22(1) or the subject of collecting personal information is specified in other acts.
- (2) Any information and communications service provider shall, when it collects the personal information of users, collect the minimum information necessary to provide the information and communications services. It shall not refuse the relevant services on the grounds that the user does not provide any other personal information than the necessary minimum information.

Article 23-2 (Method to Get Membership Not Using Residence Registration Numbers)

- (1) Any information and communications service provider, by whom the relevant services are provided and the number of daily users of such services by type satisfies on average the criteria set forth by the Presidential Decree, shall provide the methods how the users may get the membership via the information and communications networks without using the residence registration number.
- (2) The information and communications service provider applicable to Paragraph (1) may allow the users to select how to get the membership by providing the methods to get the membership using the residence registration number.

Article 24 (Restrictions on Utilizing Personal Information)

No information and communications service provider shall utilize the personal information collected pursuant to Article 22 and the proviso of Article 23(1) for other purpose than the purpose consented by the relevant user or referred to in each Subparagraph of Article 22(2).

Article 24-2 (Consent to the Provision of Personal Information, etc.)

- (1) Any information and communications service provider shall, when it intends to provide user's personal information to a third party, notify the user of the whole matters stated in the following Subparagraphs except the cases falling under Subparagraphs 2 and 3 of Article 22(2), and obtain his/her consent thereof. The same shall apply to any change of the following Subparagraphs:
1. The receiver of personal information;
 2. The purpose of utilizing personal information of such receiver;
 3. The items of personal information provided hereunder; and
 4. The period of retention and utilization of personal information by the receiver.
- (2) The receiver of the personal information of users provided by the information and communications service provider pursuant to Paragraph (1) shall not provide such personal information to a third party, nor utilize such personal information for other use than the purpose of being provided except the cases specified in other acts.

Article 25 (Entrusting Handling of Personal Information)

- (1) The information and communications service providers and the receiver of the personal information of users provided by such provider pursuant to Article 24-2(1) (hereinafter referred to as the "information and communications service provider, etc.") shall, if they entrust the work of collecting, storing, processing, utilizing, providing, managing, destroying (hereinafter collectively referred to as "handling") the personal information of users to a third party, notify the user of the whole matters stated in the following Subparagraphs, and obtain his/her consent thereof. The same shall apply to any change of the following Subparagraphs:
1. The person entrusted handling of personal information (hereinafter referred to as the "trustee"); and
 2. Particulars of entrusted work of handling of personal information.
- (2) The information and communications service providers, etc. may skip the notice and consent procedure as prescribed in Paragraph (1) in case the whole matters of each Subparagraph of Paragraph (1) are made public pursuant to Article 27-2 (1) or notified to users in such a manner like sending e-mails as stated in the Presidential Decree, which is necessary to perform the contract for the provision of information and communications services. The same shall apply to any change of the Subparagraphs of Paragraph (1).

- (3) The information and communications service providers, etc. shall, when it intends to entrust handling of personal information, define the purpose in advance for which the trustee shall handle the personal information of users. The trustee shall not handle the personal information of users beyond such purpose.
- (4) The information and communications service providers, etc. shall manage and supervise the trustee lest it should violate the provisions in this Chapter.
- (5) The trustee, who caused damage to the users regarding the work entrusted hereunder in violation of the provisions in this Chapter, shall be deemed as an employee of the information and communications service providers, etc. only with respect to compensation for such damage.

Article 26 (Transfer of Personal Information following the Business Transfer, etc.)

- (1) In the event that the information and communications service providers, etc. transfer the personal information of users to others owing to the transfer of business in whole or in part, or merger, etc., they shall notify the users of the whole matters prescribed in the following Subparagraphs in such a manner like sending e-mails, posting at the Website and so forth as stated in the Presidential Decree:
 1. The fact that the personal information intends to be transferred;
 2. The name (referring to the company name in case of a juridical person; hereafter the same shall apply in this Article), address, telephone number and other contact points of a person who has received the personal information (hereinafter referred to as the “business transferee, etc.”);
 3. The method and procedure to withdraw the consent in case the user would not want the transfer of personal information.
- (2) The business transferee, etc. shall, without delay upon the transfer of personal information, notify the users of such fact in such a manner like posting at the Website, sending e-mails and so forth as stated in the Presidential Decree; *provided, however*, that the same shall not apply where the information and communications service providers, etc. have already notified the users of such fact pursuant to Paragraph (1).
- (3) The business transferee, etc. may utilize or provide the personal information of users within the scope of the initial purpose for which the information and communications service providers, etc. are allowed to utilize or provide such personal information; *provided, however*; that the same shall not apply where the users have consented specifically.

Article 26-2 (Method to Obtain Consent)

The method how to obtain the consent pursuant to Article 22(1), the proviso of Article 23(1), Article 24-2(1) and (2), Article 25(1), the proviso of Article 26(3) or Article 63(2)(hereinafter collectively referred to as the “consent to the collection, utilization, provision, etc. of personal information”) shall be stated by the Presidential Decree in view of the media for collecting personal information, the nature of business operations, the number of users, and so forth.

Section 2. The Management and Destruction of Personal Information**Article 27 (Designation of Person in Charge of Data Protection)**

- (1) The information and communications service providers, etc. shall designate the person in charge of data protection to protect the personal information of users and deal with complaints of users related with the personal information; *provided, however*, that the same may not apply to the information and communications service providers, etc. who satisfies the number of employees and users, and other criteria specified by the Presidential Decree.
- (2) In case the information and communications service providers, etc. subject to the proviso of Paragraph (1) do not designate the person in charge of data protection, their owner or representative shall become the person in charge of data protection.
- (3) Qualification requirements for the person in charge of data protection and other matters necessary to designate the person shall be prescribed by the Presidential Decree.

Article 27-2 (Disclosure of Personal Information Policy Statement)

- (1) In case of handling the personal information of users, the information and communications service providers, etc. shall establish and disclose the personal information policy statement in such a manner as stated in the Presidential Decree so that users may identify the policy with ease at any time.
- (2) The personal information policy statement subject to Paragraph (1) shall contain each and every following items:
 1. The purpose of collection and utilization of the personal information, particulars of personal information collected hereunder and the method of collection thereof;
 2. The name (referring to the company name in case of a juridical person) of a person who

- has received the personal information, the purpose of utilization, and particulars, of the personal information in case the personal information is provided to a third party;
3. The period of retention and utilization of personal information, the procedure and method of destruction of personal information (including the ground of preservation and the particulars of personal information to be preserved in case of preserving such information subject to the proviso except each Subparagraph of Article 29)
 4. The content of business for which handling of personal information is entrusted and the trustee (including the handling policy statement, if applicable);
 5. The rights of users and legal representatives, and how to excise the rights;
 6. The installation and operation of the device collecting automatically the personal information like the Internet logon files, etc. and how to deny such device;
 7. The name or a person in charge of data protection, or the department to protect the personal information of users and deal with complaints of users related with the personal information, and the contact points like telephone numbers.
- (3) In case of change of the personal information policy statement pursuant to Paragraph (1), the information and communications service providers, etc. shall make public without delay the reason and changes thereof in such a manner as stated in the Presidential Decree so that users may identify the change of policy statement with ease at any time.

Article 28 (Data Protection Measures)

- (1) In dealing with the personal information of users, the information and communications service providers, etc. shall take such technological and managerial measures as mentioned in the following Subparagraphs to prevent the loss, stealing, leakage, alteration of, or damage to, the personal information by the standard as specified by the Presidential Decree.
1. To establish and implement the in-house management plan to deal with the personal information more safely;
 2. To install and operate the access control system like firewall to block illegal access to the personal information;
 3. To take measures to prevent the forgery or falsification of logon files;
 4. To take security measures using encryption technologies in order to store and transmit the personal information more safely;
 5. To take such preventive measures as download and operation of the vaccination

softwares to protect from computer viruses; and

6. To take other protective measures necessary to secure the safety of the personal information.

(2) The information and communications service providers, etc. shall limit the persons to deal with the personal information of users to the minimum.

Article 28-2 (Prohibition of Leakage of Personal Information)

(1) Any person who deals with, or once dealt with, the personal information of users shall not damage, infringe upon or leak out the information acquired in the course of business.

(2) No one shall be provided with the personal information for profit or unjust purposes while knowing such information has been leaked out.

Article 29 (Destruction of Personal Information)

The information and communication service providers, etc. shall promptly destroy the relevant personal information in case any of the following cases applies; *provided, however*, that the same shall not apply where other acts require the preservation of such information:

1. When they have attained the purpose of collecting or utilizing the personal information consented pursuant to Article 22(1), the proviso of Article 23(1) or Articles 24-2(1) and (2), or the relevant purpose as specified by any of the Subparagraphs of Article 22(2);
2. When they get to the end of the period of retention and utilization of personal information consented pursuant to Article 22(1), the proviso of Article 23(1) or Articles 24-2(1) and (2);
3. When they get to the end of the period of retention and utilization of personal information subject to Article 27-2(2)3 in case of collecting or utilizing the personal information without the consent of users pursuant to Article 22(2); or
4. When they close business.

Section 3. User's Right

Article 30 (User's Right, etc.)

(1) Every user may at any time withdraw his/her consent given to the information and communications service providers, etc. for the collection, utilization or provision of the personal information.

- (2) Every user may request the access to, or provision of, any of the following items related with him/her, and if his/her personal information is found to be erroneous, he/she may request the correction thereof:
1. The personal information of users retained by the information and communications service providers, etc.;
 2. The content of how the information and communications service providers, etc. have utilized, or provided to a third party, the personal information of users; or
 3. The status at which the information and communications service providers, etc. have obtained consent for the collection, utilization or provision of the personal information.
- (3) In case a user withdraws his/her consent pursuant to Paragraph (1), the information and communications service providers, etc. shall take necessary measures without delay, i.e., destroying his/her personal information collected.
- (4) The information and communications service providers, etc. shall, upon receiving a request for the access to, provision of, personal information pursuant to Paragraph (2), take necessary measures without delay.
- (5) The information and communications service providers, etc. shall, immediately upon receiving a request for the correction of erroneous personal information pursuant to Paragraph (2), correct the erroneous information or take necessary measures, i.e., explaining why they failed to correct such information, and shall not utilize or provide the relevant personal information until the correction thereof; *provided, however*, that the same shall not apply where other acts require the provision of such information.
- (6) The information and communications service providers, etc. shall make the withdrawal of consent pursuant to Paragraph (1), or how to request access to, provision of, or correction of errors in, the personal information much easier than the method how to collect the personal information.
- (7) The provisions of Paragraphs (1) through (6) shall apply *mutatis mutandis* to the business transferee, etc. In this case, the information and communications service providers, etc. shall be deemed the business transferee, etc.

Article 31 (Legal Representative's Right)

- (1) The information and communications service providers, etc. shall, when they intend to obtain consent for the collection, utilization or provision of the personal information from a minor of age below 14, obtain the consent therefor from his/her legal representative.

In this case, the information and communications service provider may demand from the child the necessary minimum information, including the name, etc. of his/her legal representative, so as to obtain the consent.

(2) The legal representative may exercise the user's right as for the personal information of the relevant child pursuant to Articles 30(1) and (2).

withdraw his/her consent given under the first sentence of Paragraph (1), and request the access to, or correction of, the personal information provided by the child.

(3) The provisions of Article 30 (3) through (5) shall apply *mutatis mutandis* to the withdrawal of consent, and the request for the access to, or the correction of, the personal information by the legal representative pursuant to Paragraph (2).

Article 32 (Damages)

If a user suffers any damage caused by the violation of the provisions in this Chapter on part of the information and communications service providers, etc., such user may claim for the damages against the information and communications service providers, etc. In this case, the information and communications service providers, etc. may not be released from the damages if they fail to prove non-existence of their wrongful intent or negligence.

Section 4. Personal Information Dispute Mediation Committee

Article 33 (Establishment and Composition of Personal Information Dispute Mediation Committee)

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

(2) The Dispute Mediation Committee shall consist of not more than 15 members, including one chairman, and one of the Committee members shall be standing.

(3) The Committee members shall be appointed or commissioned by the Minister of Administration and Security from among the persons stated in the following Subparagraphs as prescribed by the Presidential Decree. In this case, not less than one person applicable to any of the following Subparagraphs shall be included in the Committee members:

1. Persons who presently serve or have served in universities as associate professors or higher positions, or in publicly recognized research institutes as senior researchers, and have specialties in a field related with data protection;
 2. Grade IV or higher ranking public officials (including generally positioned public officials in the College of High-ranking Government Officials) or persons who presently work or have worked at equivalent positions in public institutions, and have experiences in dealing with the affairs on data protection;
 3. Persons who holds the qualification of judges, public prosecutors, or attorneys-at-law;
 4. Persons who presently work or have worked as senior officers for the organizations of the users of information and communications services;
 5. The persons who presently work or have worked as senior officers for the information and communications service providers or the organizations of the information and communications service providers; and
 6. Persons recommended by non-profit non-governmental organizations established pursuant to Article 2 of the Act for Assistance of Non-profit Non-governmental Organizations.
- (4) The term of office for the Committee members shall be three years and they may be reappointed or recommissioned.
- (5) The chairman shall be appointed by the Minister of Administration and Security from among the Committee members.
- (6) A secretariat shall be established to support the Dispute Mediation Committee in the Korea Information & Security Agency (hereinafter referred to as "KISA") established pursuant to Article 52.

Article 33-2 (Petit Panel)

- (1) In order to conduct efficiently the dispute settlement, the Dispute Mediation Committee shall establish a petit panel which is composed of five or less Committee members, and one of the members shall be an attorney-at-law.
- (2) The Dispute Mediation Committee may, if necessary, delegate a part of dispute mediation to the petit panel stated in Paragraph (1).
- (3) The necessary matters with regard to the composition and operation of the petit panel stated in Paragraph (1) shall be prescribed by the Ordinance of the Ministry of Administration and Security.

Article 34 (Guarantee of Members' Status)

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

Article 35 (Exclusion, Challenge and Refrainment of Member)

- (1) Any Committee member, if applicable to any of the following Subparagraphs, shall be excluded from participating in the deliberation and resolution of a case requested for dispute mediation (hereafter in this Article referred to as the "case"):
 1. Where a Committee member, his/her spouse, or his/her former spouse is a party to the case, or a joint right holder or a joint obligator with respect to the case;
 2. Where a Committee member is or was in a kinship with the party of the case;
 3. Where a Committee member gives any testimony or expert opinion with respect to the case; or
 4. Where a Committee member is or was involved in the case as an agent, officer or employee of the party.
- (2) Any party may, when he/she finds it difficult to expect a fair deliberation and resolution from the Committee members, file a challenge application with the Dispute Mediation Committee. In this case, the Dispute Mediation Committee shall, when it deems such challenge application appropriate, determine the challenge.
- (3) Any Committee member may, when he/she falls under the case of Paragraph (1) or (2), refrain from the deliberation and resolution of the case.

Article 36 (Mediation of Dispute)

- (1) Any person, who wants any dispute over the personal information mediated, may apply for mediation of such dispute to the Dispute Mediation Committee.
- (2) The Dispute Mediation Committee shall, upon receiving an application for mediation of a dispute pursuant to Paragraph (1), examine the case and prepare a draft mediation within 60 days from the date of receiving such application; *provided, however*, that, in case of unavoidable circumstances, the Dispute Mediation Committee may resolve to extend such period.
- (3) In case the period is extended under the proviso of Paragraph (2), the applicant shall be notified of reasons for extending the period and other matters concerning the extension of

such period.

Article 37 (Request for Materials, etc.)

- (1) The Dispute Mediation Committee may request parties involved in a dispute to provide materials necessary to mediate the dispute. In this case, the relevant parties shall comply with the request if any justifiable ground is non-existent.
- (2) The Dispute Mediation Committee may, when deemed necessary, let parties involved in a dispute or relevant witnesses appear before the Dispute Mediation Committee to hear their opinions.

Article 38 (Effect of Mediation)

- (1) The Dispute Mediation Committee shall, when it prepares a draft mediation pursuant to Article 36(2), present without delay such draft mediation to each party.
- (2) Each party presented with the draft mediation pursuant to Paragraph (1) shall notify the Dispute Mediation Committee of whether or not he/she accepts the draft mediation within 15 days from the day of receipt of such draft mediation.
- (3) If the parties accept the draft mediation, the Dispute Mediation Committee shall promptly prepare a written mediation, and the chairman and the parties shall have their names and seals affixed thereon.
- (4) When the parties accept the draft mediation pursuant to Paragraph (3) and the chairman and the parties have their names and seals affixed thereon, an agreement identical to the written mediation shall be deemed reached between the parties.

Article 39 (Rejection and Suspension of Mediation)

- (1) The Dispute Mediation Committee may, when it deems that it is inappropriate to mediate any dispute in view of its nature, or that an application for mediation of any dispute is filed for an unfair purpose, reject the mediation. In this case, the reasons why it rejected the mediation shall be notified to the applicant.
- (2) In case one of the parties files a lawsuit during the course of examining a medication case, the Dispute Mediation Committee shall suspend the dispute mediation and notify the parties thereof.

Article 40 (Mediation Proceedings, etc.)

Except the provisions of Articles 36 through 39, necessary matters concerning the method of, and procedures for, mediating any dispute, and dealing with such dispute mediation, etc. shall be prescribed by the Presidential Decree.

**CHAPTER V . PROTECTION OF THE YOUTH IN INFORMATION
AND COMMUNICATIONS NETWORKS, ETC.**

*Translation of the provisions of Articles not related with
data protection is omitted. The headings are for reference.*

Article 41 (Establishing Protective Measures for the Youth, etc.)

Article 42 (Labeling of Media Materials Harmful to the Youth)

Article 42-2 (Prohibition of Advertizing Media Materials Harmful to the Youth)

Article 42-3 (Designation of Officer in Charge of Youth Protection, etc.)

Article 43 (Obligation of Provider of Visual or Sound Information to Retain Them)

Article 44 (Protection of Rights in the Information and Communications Networks)

Article 44-2 (Request for Deleting Information, etc.)

Article 44-3 (Optional Provisional Measures)

Article 44-4 (Self-Regulation)

Article 44-5 (Identification of Bulletin Users)

Article 44-6 (Request of User Information)

Article 44-7 (Prohibition of Trading Illegal Information, etc.)

Articles 44-8 and 9 Deleted.

Article 44-10 (Dispute Mediation Panel for Defamation)

CHAPTER VI. SECURING STABILITY OF INFORMATION AND COMMUNICATIONS NETWORKS, ETC.

Article 45 (Securing Stability of Information and Communications Networks, etc.)

Article 45-2 Deleted.

Article 46 (Protection of Clustered Information and Communications Facilities)

**Article 46-2 (Emergency Response of Clustered Information and Communications
Facility Operators)**

Article 46-3 (Diagnosis of Safety of Data Protection)

Article 47 (Authentication of Data Protection Management System)

**Article 47-2 (Cancellation of Designation of Authenticator of Data Protection
Management System)**

Article 47-3 (Data Protection of Users)

(1) The government may advise to the users to observe by establishing necessary standards for the data protection of users, and take necessary measures, i.e., checking the weak points and providing technological assistance, so as to prevent the incidents and block the dissemination thereof.

(2) through (4) *Omitted*

Article 48 (Prohibition of Incidents to Information Communications Networks)

Article 48-2 (Response to Incidents, etc.)

Article 48-3 (Report of Incidents, etc.)

Article 48-4 (Analysis of Incidents, etc.)

Article 49 (Protection of Secrets, etc.)

No one is allowed to damage the information of other persons or infringe upon, steal or leak the secrets of other persons, which are processed, stored or transmitted via the information and communications networks.

Article 49-2 (Prohibition of Collection of Personal Information by Means of Deceitful Activities)

- (1) No one shall collect, or entice other person to provide with, the personal information of other person by means of deceitful activities in the information and communications networks.
- (2) Any information and communications service provider shall report to the Broadcasting and Communications Commission or the Korea Information & Security Agency immediately upon finding out the violation of Paragraph (1).
- (3) The Broadcasting and Communications Commission or the Korea Information & Security Agency shall, upon receiving the report pursuant to Paragraph (2) or finding out the violation of Paragraph (1), take necessary measures prescribed in the following Subparagraphs:
 1. Collecting and disseminating the violation of Paragraph (1);
 2. Forecasting or warning of similar violations; and
 3. Emergency measures to prevent further violations including requests for blocking the access paths to the information and communications service providers.

Article 50 (Restrictions on Transmitting Advertisement Information Made for Profit)

- (1) Nobody shall transmit advertisement information made for profit against the addressee's

explicit refusal of such information by means of e-mail or other media as prescribed by the Presidential Decree.

- (2) Anybody, who intends to transmit via e-mail or facsimile any advertisement information made for profit, shall obtain the prior consent of the relevant addressee; *provided, however*, that the same shall not apply to any of the following Subparagraphs:
 1. Where somebody, who collects directly from the addressees the contact points through transactions of goods and services, intends to transmit the advertisement information made for profit to publicize such goods and services provided by himself; and
 2. Where the advertisement pursuant to Article 13(1) of the Act for the Consumer Protection in Electronic Commerce, Etc., and the telephone solicitation pursuant to Article 6(3) of the Act Regarding Visiting Sales, Etc. take place.
- (3) Anybody, who intends to transmit any advertisement information made for profit to the telephone or facsimile of the addressee during the hours from 9:00 p.m. to 8:00 a.m. the next day, shall obtain the separate prior consent of the relevant addressee in spite of Paragraph (2).
- (4) Anybody, who transmits advertisement information made for profit by means of e-mail or other media as prescribed by the Presidential Decree, shall indicate concretely the matters stated in the following Subparagraphs in such a manner as prescribed by the Presidential Decree:
 1. The types and contents of transmitted information;
 2. The name and contact points of the sender;
 3. The sources where the sender collected the e-mail addresses (only in case of transmitting e-mails); and
 4. Other matters regarding the process and means to easily indicate the refusal of unsolicited messages.
- (5) Anybody, who transmits advertisement information made for profit to the telephone or facsimile of the addressee shall indicate concretely the matters stated in the following Subparagraphs in such advertisement information in such a manner as prescribed by the Presidential Decree:
 1. The name and contact points of the sender; and
 2. Other matters regarding the process and means to easily indicate the withdrawal of previous consent to such messages.
- (6) Anybody, who transmits advertisement for profit, shall not take any technological

measure specified in the following Subparagraphs:

1. Measures to avoid and hinder the refusal or withdrawal of consent of the addressee of advertisement information;
 2. Measures to automatically generate the contact points of addressee i.e., by combining numbers, codes or letters into new telephone numbers or e-mail addresses;
 3. Measures to automatically register e-mail addresses in order to transmit advertisement information made for profit; or
 4. Measures to conceal the identity of the sender of advertisement information or the source of advertisement transmission.
- (7) Anybody, who transmits advertisement information for profit, shall take necessary measures in such a manner as prescribed by the Presidential Decree lest the addressee should be charged the monetary cost incurred when telephoning a message to refuse, or withdraw the consent of, such information.

Article 50-2 (Prohibition of Unauthorized Collection of e-Mail Addresses)

- (1) Nobody shall collect e-mail addresses by using automatic programs extracting e-mail addresses from Internet homepages and other technological devices without prior consent of their system operators or administrators.
- (2) Nobody shall sell or circulate the e-mail addresses collected in violation of Paragraph (1).
- (3) Nobody shall use e-mail addresses while knowing such e-mail addresses are prohibited from collecting, selling and circulating pursuant to Paragraphs (1) and (2).

Article 50-3 (Entrusting Transmission of Advertisement Information Made for Profit)

- (1) Anybody, who entrusts other person with a task to transmit advertisement information made for profit, shall control and supervise him/her lest the trustee should violate Articles 50 and 50-2.
- (2) Anybody, who is entrusted by a person with a task to transmit advertisement information made for profit pursuant to Paragraph (1), shall be deemed an employee of such person in compensating the damage caused by violating the relevant acts related with such task.

Article 50-4 (Restrictions on Information Transmission Services, etc.)

- (1) The information and communications service providers may take measures to refuse to

provide the relevant services in any of the following Subparagraphs:

1. Where obstacles occur or are expected to occur in providing services owing to transmitting or receiving advertisement information;
 2. Where users would not want to receive advertisement information; or
 3. Where the services provided by the information and communications service providers pursuant to an end-user agreement are utilized for transmitting illegal advertisement information.
- (2) The information and communications service providers, which intend to take measures to refuse pursuant to Paragraph (1), shall include such provisions as how to refuse the relevant services in an end-user agreement with the user of such services.
- (3) The information and communications service providers, which intend to take measures to refuse pursuant to Paragraph (1), shall notify such measures to interested parties including the user of such services; *provided, however*, that the prompt notification is required without delay after taking such measures in case of impossibility of prior notice.

Article 50-5 (Installation of Advertisement Programs for Profit, etc.)

The information and communications service providers, which intend to show up advertisement information made for profit or install the programs to collect personal information in the users' computer or other data processing devices as prescribed by the Presidential Decree, shall obtain the consent of users. In this case, they shall notify the usage of such programs and the method how to delete.

Article 50-6 (Distribution of Softwares to Block the Transmission of Advertisement Programs Made for Profit)

- (1) The Broadcasting and Communications Commission may develop and distribute softwares and computer programs by which the addressee can conveniently block or report the advertisement information made for profit transmitted in violation of Article 50.
- (2) The Broadcasting and Communications Commission may provide necessary support to the relevant public institutions, corporations, associations, etc. in order to promote the development and distribution of softwares and computer programs to block and report pursuant to Paragraph (1).
- (3) The Broadcasting and Communications Commission may advise the information and communications service providers to take such necessary measures as development of

technologies, education, public relations, etc. for the protection of addressees when the services of the information and communications service providers are used to transmit the advertisement information made for profit in violation of Article 50.

- (4) Necessary matters for the development and distribution pursuant to Paragraph (1) and the support pursuant to Paragraph (2) shall be prescribed by the Presidential Decree.

Article 50-7 (Restrictions on Posting Advertisement Information Made for Profit)

- (1) Nobody shall post any advertisement information made for profit on the Internet homepage contrary to the explicit refusal of its system operator or administrator.
- (2) A system operator or administrator of the Internet homepage may take such measures as deleting the advertisement information made for profit which is posted in violation of Paragraph (1).

Article 50-8 (Prohibition of Transmission of Advertisement Information for Illegal Act)

Nobody shall transmit advertisement information regarding goods or services prohibited by this Act or other acts via the information and communications networks.

Article 51 (Restrictions on Outflow of Material Information into Foreign Countries)

- (1) The government may have each information and communications service provider or the relevant user of information and communications services take measures necessary to prevent material information regarding the domestic industry, economy, science and technology, etc. from being flowed out of Korea into foreign countries via the information and communications networks.
- (2) The scope of material information referred to in Paragraph (1) shall be as follows:
1. Security information related with the national security and major policy information; or
 2. Information regarding state-of-the-art technologies or equipment developed domestically.
- (3) The government may have each information and communications service provider dealing with the information referred to any of the Subparagraphs of Paragraph (2) take the following measures:
1. Establishing systemic and technological devices to prevent improper utilization of the information and communications networks;

2. Taking systemic and technological measures to block the illegal destruction or manipulation of information; or
3. Taking measures to prevent the leakage of material information acquired in the course of handling information by the information and communications service provider.

Article 52 (Korea Information & Security Agency)

- (1) The government shall establish the Korea Information & Security Agency (hereinafter referred to as “KISA”) to implement efficiently such policies as to enhance the information and communications networks (excluding the establishing, improving and managing such networks), as to promote the safe usage, and as to support the international cooperation and going abroad related with broadcasting and communications.
- (2) KISA shall be a juridical person.
- (3) KISA shall conduct the business referred to in the following Subparagraphs:
 1. To survey and research into legal regimes, policies and systems for the utilization and protection of the information and communications networks, and the international cooperation and going abroad related with broadcasting and communications;
 2. To do research and analysis of statistics related with the utilization and protection of the information and communications networks;
 3. To analyze negative effects of informatization and to research into countermeasures;
 4. To conduct public relations, education and training for the utilization and protection of the information and communications networks;
 5. To secure data protection in the information and communications networks, and to achieve technological development and standardization related with the Internet address resources;
 6. To help establish the policy for the knowledge-based information security industries, and to conduct related technological development and training of human resources;
 7. To implement and support authentication and assessment in respect of data protection including a diagnosis of the safety of data protection, authentication of data protection management system, assessment and authentication of data protection system, etc.;
 8. To do research into effective measures for data protection, and to support the development and distribution of data protection technologies;
 9. To support the operation of the Dispute Mediation Committee and to operate the Reporting Center for Personal Information Infringement;

10. To do counseling and process claims regarding the transmission of advertisement information and the Internet advertisement;
 11. To deal with and analyze causes of the incidents infringing upon the information and communications networks, and to operate the incident response system;
 12. To manage the authentication of electronic signature pursuant to Article 25(1) of the Electronic Signature Act;
 13. To support the efficient operation of the Internet and the promotion of utilization thereof;
 14. To help protect the stored information of the Internet users;
 15. To support the service policy related with the Internet;
 16. To protect users in the Internet, and to help flow and disseminate sound information;
 17. To conduct business regarding the Internet addresses under the Act on the Internet Resources;
 18. To support operation of the Internet Address Dispute Mediation Committee pursuant to Article 16 of the Act on the Internet Resources;
 19. To assist the international cooperation, going abroad and overseas public relations related with broadcasting and communications;
 20. Other activities incidental to the business of Subparagraphs 1 through 19; and
 21. Other tasks prescribed by this Act, and other acts and regulations to be conducted by KISA, or entrusted by the Minister of Administration and Security, the Minister of Knowledge and Economy, the Broadcasting and Communications Commission, or the head of other administrative agencies;
- (4) The government may make contributions to cover expenses necessary for the operation of KISA.
- (5) The provisions regulating the incorporated foundation in the Civil Act shall apply *mutatis mutandis* to the matters not prescribed by this Act with respect to KISA.
- (6) Other person than KISA shall not use the name of the Korea Information & Security Agency.
- (7) Other matters necessary to operate, and conduct business of, KISA shall be prescribed by the Presidential Decree.

CHAPTER VII. COMMUNICATIONS BILLING SERVICES

Articles 53 - 61 *Omitted.*

CHAPTER VIII. INTERNATIONAL COOPERATION

Article 62 (International Cooperation)

In performing the function stated in the following Subparagraphs, the government shall cooperate with other states or international organizations:

1. Cross-border transfer of personal information and data protection;
2. Protection of the youth in the information and communications networks;
3. Prevention of the incidents threatening the safety of information and communications networks; and
4. Other activities to ensure safe and sound utilization of information and communications services.

Article 63 (Protection of Out-bound Personal Information)

- (1) The information and communications service providers, etc. shall not enter into any international contract of which contents violate the provisions of this Act with respect to the personal information of users.
- (2) The information and communications service providers, etc. shall obtain the consent of users when they intend to transfer the personal information of such users to abroad.
- (3) The information and communications service providers, etc. shall, when they intend to obtain the consent pursuant to Paragraph (2), notify the user in advance of the whole matters stated in the following Subparagraphs:
 1. The items of personal information to be transferred;
 2. The state to which personal information will be transferred, the date and time of transfer and the method thereof;
 3. The name (referring to the company name and the contact points of the officer in charge of data protection in case of a juridical person) of a person who will be provided with the personal information; and
 4. The purpose of utilization, and the period of retention and utilization, of personal

- information on the part of a person who will be provided with the personal information.
- (4) The information and communications service providers, etc. shall take the protective measures as prescribed by the Presidential Decree when they transfer the personal information to abroad with the consent pursuant to Paragraph (2).

CHAPTER IX. SUPPLEMENTARY PROVISIONS

Article 64 (Submission of Materials, etc.)

- (1) The Minister of Administration and Security or the Broadcasting and Communications Commission may request the information and communications service providers, etc. (in this Article, including any person to whom Article 67 applies *mutatis mutandis*) to submit relevant goods, documents, etc. in case any of the following Subparagraphs shall apply:
1. Where the violation of this Act is detected or knowingly suspected;
 2. Where the violation of this Act is reported or any claim thereon is received; or
 3. Where such other cases as prescribed by the Presidential Decree are necessary to protect the users.
- (2) The Broadcasting and Communications Commission may request the information and communications service providers, etc. to have access to, or submit, data with respect to the name, address, residence registration number, period of utilization, etc. of the person who transmitted advertisement information made for profit in violation of this Act in order to take the measures stated in the following Subparagraphs against such transmitter:
1. Corrective measures pursuant to Paragraph (4);
 2. Imposition of fine for negligence pursuant to Article 76; and
 3. Other measures amounting to the above-mentioned Subparagraphs.
- (3) When the information and communications service providers, etc. fail to submit materials pursuant to Paragraphs (1) and (2), or they are deemed to have violated this Act, the Minister of Administration and Security or the Broadcasting and Communications Commission may have its officials enter the business place of the information and communications service providers, etc. to inspect their current business operations and examine ledger and books, or other documents, etc.

- (4) The Minister of Administration and Security or the Broadcasting and Communications Commission may order that the information and communications service providers, etc. in violation of this Act should take necessary corrective measures, and demand such information and communications service providers, etc., who have been ordered to do so, to make such fact public. In this case, such necessary matters as the method how to make it public, the criteria and procedure thereof, etc. shall be prescribed by the Presidential Decree.
- (5) The Minister of Administration and Security or the Broadcasting and Communications Commission may, when it ordered necessary corrective measures pursuant to Paragraph (4), make the fact public. In this case, such necessary matters as the method how to make it public, the criteria and procedure thereof, etc. shall be prescribed by the Presidential Decree.
- (6) The Minister of Administration and Security or the Broadcasting and Communications Commission shall, when it requests the relevant information and communications service providers, etc. to submit or have access to data, etc. pursuant to Paragraphs (2) and (3), notify in writing (including the electronic message) of the reason for request, legal grounds, time limit of submission thereof or the date and time to have access thereto, the content of data to be submitted or accessed in detail.
- (7) In case of inspection pursuant to Paragraphs (3), the inspection plan including the inspection date and time, reasons for inspection, particulars to be inspected shall be notified to the relevant information and communications service providers, etc. at least seven days before the scheduled inspection date; *provided, however*, that the same does not apply in case of emergency or when it deems such prior notification inappropriate to attain the inspection purpose because of probable destruction of evidences.
- (8) The officials, who conduct the inspection pursuant to Paragraph (3), shall carry certificates showing their authority, produce them to persons concerned, and deliver them the document containing officials' names, inspection hours, purposes thereof, etc.
- (9) The Minister of Administration and Security or the Broadcasting and Communications Commission shall, when it received, had access to, or inspected the data, etc. pursuant to Paragraphs (1) and (3), notify in writing the relevant information and communications service providers, etc. of the inspection result (in case of making an order to take corrective measures subsequent to the inspection, including such order).
- (10) The Minister of Administration and Security or the Broadcasting and Communications

Commission shall, for the purpose of request of submission or inspection of data, etc. pursuant to Paragraphs (1) and (4), may ask the head of KISA for technical advices and other necessary support.

- (11) Any request of submission of, access to, or inspection of, data, etc. pursuant to Paragraphs (1) and (4) shall be made within the minimum scope necessary to implement this Act, and shall not be misused for other purposes.

Article 64-2 (Preservation and Destruction of Materials, etc.)

- (1) The Minister of Administration and Security or the Broadcasting and Communications Commission shall not provide to a third party the documents, materials, etc. submitted or collected pursuant to Article 64 nor make them public, if and when it is requested by the relevant information and communications service providers, etc. to preserve such materials.
- (2) In case the Minister of Administration and Security or the Broadcasting and Communications Commission received the materials submitted via the information and communications networks, or made them digitalized, it shall take systemic and technological security measures lest the personal information, trade secrets etc. should be leaked out.
- (3) The Minister of Administration and Security or the Broadcasting and Communications Commission shall destroy immediately the documents, materials, etc. submitted or collected pursuant to Article 64, if there occurs a case applicable to any of the following Subparagraphs except otherwise specifically provided in other acts. The same shall apply to the person to whom the Minister of Administration and Security, the Minister of Knowledge and Economy or the Broadcasting and Communications Commission delegates or entrusts the whole or part of its authority pursuant to Article 65:
1. Where the purpose for which the request for submission of materials, visit and inspection, order to take corrective measures, etc. take place pursuant to Article 64 has been attained;
 2. Where an administrative judgment is filed in disobedience of the order to take corrective measures pursuant to Article 64(4), or, in case of the administrative lawsuit, the relevant administrative dispute settlement proceedings have been closed;
 3. Where the fine for negligence is levied pursuant to Article 76(4) and there is no objection thereto until the period of objection is over pursuant to Article 76(5);

4. Where any objection is raised against the imposition of fine for negligence pursuant to Article 76(4) and the non-litigation proceedings of the competent court with jurisdiction are over.

Article 64-3 (Imposition of Surcharge, etc.)

- (1) In case an action is in violation of any of the following Subparagraphs, the Broadcasting and Communications Commission may impose the surcharge amounting to not more than one percent(1/100) of total sales related with such violation on the wrong-doing electricity and communications operator; *provided, however*, that the surcharge of not more than 100 million won may be imposed to the violator of Subparagraph 6:
 1. To collect personal information without obtaining the consent of a user in violation of Article 22(1);
 2. To collect personal information which is most likely to infringe upon the right and interest, or the privacy, of an individual without obtaining the consent of the subject in violation of Article 23(1);
 3. To utilize personal information in violation of Article 24;
 4. To provide personal information to a third party in violation of Article 24-2;
 5. To entrust handling of personal information without obtaining the consent of a user in violation of Article 25(1);
 6. To leave the personal information of a user lost, stolen, leaked, altered or damaged owing to failure to take measures required by Articles 28(1) 2 through 5; or
 7. To collect the personal information of a minor of age below 14 without obtaining the consent of his/her legal representative in violation of Article 31(1).
- (2) In case the surcharge is imposed pursuant to Paragraph (1), if such electricity and communications operator denies to submit data for the calculation of sales or submits false data, its sales amount may be estimated on the basis of financial statements and other accounting information of the electricity and communications operator with a similar size, and the business data including the number of subscribers, tariff table of users, etc. *provided, however*, that, in such a case of no sales report at all or the difficulty to calculate the amount of sales as prescribed by the Presidential Decree, the surcharge of not more than 400 million won may be imposed to such operator.
- (3) When imposing the surcharge pursuant to Paragraph (10), the Broadcasting and Communications Commission shall take the particulars stated in the following

Subparagraphs into consideration:

1. The substance and status of violations;
 2. The duration and times of violations; and
 3. The size of profit acquired out of violations.
- (4) The surcharge pursuant to Paragraph (1) shall be assessed with the provision of Paragraph (3) taken into consideration, but the detailed criteria and procedure for the assessment of surcharge shall be prescribed by the Presidential Decree.
- (5) When the person, who is required to pay the surcharge pursuant to Paragraph (1), fails to pay the surcharge until the due date, the Broadcasting and Communications Commission shall collect the additional charge amounting to six percent per annum (6% p.a.) of such surcharge for the period from the following day of the due date.
- (6) When the person, who is required to pay the surcharge pursuant to Paragraph (1), fails to pay the surcharge until the due date, the Broadcasting and Communications Commission shall press for the payment by designating the extended period. If and when the person fails to pay the surcharge and the additional charge for the extended period pursuant to Paragraph (5), the Broadcasting and Communications Commission finally shall collect the surcharge and the additional charge likewise by the disposition for recovery of the National Tax arrears.
- (7) In case the surcharge imposed pursuant to Paragraph (1) is refunded owing to the court judgment, etc., the additional fee in the amount of six percent per annum (6% p.a.) of such surcharge to be refunded shall be paid for the period from the payment date of surcharge to the refund date.

Article 65 (Delegation and Entrustment of Authority)

- (1) The authority of the Minister of Administration and Security, the Minister of Knowledge and Economy or the Broadcasting and Communications Commission under this Act may be delegated or entrusted in part to the head of its administrative agency under its control or the head of the Regional Communication Office in such a manner as prescribed by the Presidential Decree.
- (2) The Minister of Knowledge and Economy may entrust the project to promote the utilization of the information and communications networks, etc. pursuant to Article 13 to the National Information Society Agency (NISA) established pursuant to Article 10 of the Framework Act on Informatization Promotion in such a manner as prescribed by the

Presidential Decree.

- (3) The Minister of Administration and Security or the Broadcasting and Communications Commission may entrust doing job to request the submission of, and inspect, the materials pursuant to Articles 64(1) and (2) to KISA in such a manner as prescribed by the Presidential Decree.
- (4) The provision of Article 64(8) shall apply *mutatis mutandis* to the employees of KISA who are subject to Paragraph (3).

Article 65-2 Deleted.

Article 66 (Confidentiality, etc.)

Any person who is or was engaged in the business stated in the following Subparagraphs shall not leak secrets acquired while performing his/her duties to any other person, or use such secrets for other purposes than the initial duties; *provided, however*, that the same shall not apply where other acts specifically prescribe otherwise:

1. Mediating any dispute conducted by the Dispute Mediation Committee under Article 33;
2. Authenticating the data protection and management system under Article 47;
3. Assessing the data protection system under Article 52(3)4;
4. Diagnosis of the safety of data protection under Article 46-3; and
5. Mediating any dispute conducted by the Defamation Dispute Mediation Panel under Article 44-10.

Article 67 (Application to Other Persons than Information and Communications Service Providers)

- (1) The provisions of Articles 22, 23-2, 24, 24-2, 25, 26, 26-2, 27, 27-2, 28, 28-2 and Articles 29 through 32 shall apply *mutatis mutandis* to the persons prescribed by the Presidential Decree, from among other persons than the information and communications service providers, who provide goods or services, collects, utilizes or provides the personal information of customers of their goods or services. In this case, the “information and communications service provider” and the “information and communications service providers, etc.” shall be deemed the “providers of goods or services,” and the “user” shall be deemed the “customer of goods or services,” respectively.
- Further, the persons, to whom the provisions of Articles 22, 23-2, 24, 24-2, 25, 26, 26-2, 27,

27-2, 28 and 28-2 and Articles 29 through 32 apply *mutatis mutandis*, shall be regulated in respect of the criteria and method pursuant to Articles 27-2(1),(3) and 28(1), and other details by the Ordinance of the Ministry of Administration and Security.

- (2) The provisions of Articles 22, 23, 23-2, 24, 24-2, 26, 26-2, 27, 27-2, 28 and 28-2 and Articles 29 through 31 shall apply *mutatis mutandis* to the trustee as prescribed in Article 25(1).

Article 59 *Omitted.*

Article 68 (Establishment of Korea Association of Information and Telecommunication)

Deleted as of September 23, 2010

Article 68-2 (Establishment of Korea Information Security Industry Association)

- (1) Any person, who is doing business related with information security, may establish the Korea Information Security Industry Association (KISIA) subject to the authorization of the Minister of Knowledge and Economy for the sound development of the information security industry and enhancement of overall industrial standard of information security.
- (2) KISIA shall be a juridical person.
- (3) Other matters necessary for the authorization procedure, operation and supervision of KISIA shall be prescribed by the Presidential Decree.
- (4) The provisions regulating the incorporated association in the Civil Act shall apply *mutatis mutandis* to KISIA except otherwise provided for in this Act.

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

The officers and employees of NISA and KISA, who are conducting the job entrusted by the Minister of Administration and Security, the Minister of Knowledge and Economy or the Broadcasting and Communications Commission pursuant to Articles 65(2) and (3), shall be deemed government officials in the application of Articles 129 through 132 of the Criminal Act.

CHAPTER X. PENAL PROVISIONS

Article 70 (Penal Provisions)

- (1) Any person who has defamed other person by alleging openly facts via the information and communications networks with the purpose of slandering him/her shall be subject to imprisonment with or without prison labor for not more than 3 years or by a fine not exceeding 20 million won.
- (2) Any person who has defamed other person by alleging openly false facts via the information and communications networks with the purpose of slandering him/her shall be subject to imprisonment with prison labor for not more than 7 years or the suspension of qualification for not more than 10 years, or by a fine not exceeding 50 million won.
- (3) The offense stated in Paragraphs (1) and (2) shall not be indicted against the will expressed by the victim.

Article 71 (Penal Provisions)

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

1. A person who has collected the personal information of users without the consent of users in violation of Article 22(1) (including the case to which the provisions are applied *mutatis mutandis* in Article 67);
2. A person who has collected the personal information likely to excessively infringe upon the right, interest and privacy of the individual without the consent of users in violation of Article 23(1) (including the case to which the provisions are applied *mutatis mutandis* in Article 67);
3. A person who has utilized the personal information of users, provided such personal information to a third party, or received such personal information knowingly for profit or unjust purposes in violation of Articles 24, 24-2(1) and (2) or 26(3) (including the case to which the provisions are applied *mutatis mutandis* in Article 67);
4. A person who has entrusted handling of the personal information without the consent of users in violation of Article 25(1) (including the case to which the provisions are applied *mutatis mutandis* in Article 67);
5. A person who has damaged, infringed upon or leaked the personal information of users in violation of Article 28-2(1) (including the case to which the provisions are applied *mutatis*

mutandis in Article 67);

6. A person who has received the personal information for profit or unjust purposes knowing such information leaked out in violation of Article 28-2(2);
7. A person who has provided or utilized the personal information without taking necessary measures in violation of Article 30(5) (including the case to which the provisions are applied *mutatis mutandis* in Articles 30(7), 31(3) and 67);
8. A person who has collected the personal information of a minor below 14 without the consent of his/her legal representative in violation of Article 31(1) (including the case to which the provisions are applied *mutatis mutandis* in Article 67);
9. A person who has conveyed or distributed malicious programs in violation of Article 48(2);
10. A person who has caused troubles in the information and communications networks in violation of Article 48(3); and
11. A person who has damaged the information of other person, or infringed upon, stolen or leaked the secrets of other person in violation of Article 49.

Article 72 (Penal Provisions)

- (1) Any person referred to in the following Subparagraphs shall be subject to imprisonment with prison labor for not more than 3 years or by a fine not exceeding 30 million won:
 1. A person who has infiltrated the information and communications networks in violation of Article 48(1);
 2. A person who has collected the personal information of other person in violation of Article 49-2(1);
 3. A person who has done business without registration required by Article 53(1);
 4. A person who has lent money or arranged for it by conducting action applicable to any of the following Items:
 - a. To do transactions of communications billing services by pretending to sell or provide the goods or services, or exceeding the real sales, or to let others do so on his/her behalf; or
 - b. To purchase the goods or services at a discount which were bought or used by the user of communications billing services just after such user was induced to buy or use such goods or services by means of the communications billing services.
 5. A person who has leaked the secrets to other person acquired while performing his/her

duties, or utilized such secrets for other purpose than the initial duties in violation of Article 66.

(2) A person stated in Paragraph (1)1 who attempted to commit the crime shall be punished.

Article 73 (Penal Provisions)

Any person referred to in the following Subparagraphs shall be subject to imprisonment with prison labor for not more than 2 years or by a fine not exceeding 10 million won:

1. A person who has lost, stolen, leaked, altered or damaged the personal information of users by failing to take such technological and managerial measures as prescribed in Articles 28(1) 2 through 5 (including the case to which the provisions are applied *mutatis mutandis* in Article 67);
2. A person who has provided media materials harmful to the youth for profit without indicating the harmful nature in violation of Article 42;
3. A person who has transmitted to the youth, or exhibit publicly without taking any measure off-limits to the youth the information to advertize the media materials harmful to the youth in violation of Article 42-2;
4. A person who has used the information of users for other purposes than filing civil or criminal lawsuits;
5. A person who has not observed the order of the Broadcasting and Communications Commission pursuant to Articles 44-7(2) and (3);
6. A person who has not preserved the relevant materials in violation of the order pursuant to Article 48-4(3);
7. A person who has enticed other person to provide with personal information in violation of Article 49-2(1); or
8. A person who has not observed the order pursuant to Article 61.

Article 74 (Penal Provisions)

- (1) Any person referred to in the following Subparagraphs shall be subject to imprisonment with prison labor for not more than 1 year or by a fine not exceeding 10 million won:
1. A person who has put any label on goods, or sold such goods bearing such label or displayed such goods for the purpose of selling them in violation of Article 8(4);
 2. A person who has distributed, sold, rented, or openly displayed lascivious codes, letters, sounds, images or video clips in violation of Article 44-7(1)1;

3. A person who has repeatedly sent codes, letters, sounds, images or video clips inciting fears and uneasiness to other person in violation of Article 44-7(1)3;
 4. A person who has taken technological measures in violation of Article 50(6);
 5. A person who has collected, sold and circulated the e-mail addresses or use them for transmission in violation of Article 50-2;
 6. A person who has transmitted advertisement information in violation of Article 50-8; or
 7. A person who has not registered the change of the registry nor reported business transfer, or the merger and succession of business in violation of Article 53(4).
- (2) The offense stated in Paragraph (1)3 shall not be indicted against the will expressed by the victim.

Article 75 (Joint Penal Provisions)

If a representative of a corporation, or the agent, manager or other employee of a corporation or an individual violated the provisions of Articles 71 through 73 or 74(1) with respect to the business of such corporation or individual, the actor shall be punished, but also the corporation or individual shall be subject to a fine prescribed in the relevant Article; *provided, however*, that the same shall not apply where such corporation or individual was not negligent in taking due care and supervisory duty to do the relevant business.

Article 76 (Fine for Negligence)

- (1) A person who is referred to in the following Subparagraphs and abets other person to do the action applicable to Items 7 through 11 shall be subject to a fine for negligence not exceeding 30 million won:
1. A person who has denied services in violation of Article 23(2) (including the case to which the provisions are applied *mutatis mutandis* in Article 67);
 2. A person who fails to take necessary measures in violation of Article 23-2;
 3. A person who fails to take technological and managerial measures as prescribed in Articles 28(1)1 and 6 (including the case to which the provisions are applied *mutatis mutandis* in Article 67);
 4. A person who fails to destroy personal information in violation of the main sentence of Article 29 (including the case to which the provisions are applied *mutatis mutandis* in Article 67);
 5. A person who fails to take necessary measures in violation of Articles 30(3), (4) and (6)

- (including the case to which the provisions are applied *mutatis mutandis* in Articles 30(7), 31(3) and 67);
6. A person who has not observed the order of the Broadcasting and Communications Commission pursuant to Article 44-5(2);
 7. A person who has transmitted advertisement information made for profit in violation of Articles 50(1) through (3);
 8. A person who has failed to indicate advertisement information or indicated fraudulently in violation of Articles 50(4) or (5);
 9. A person who has got the addressee charged the cost in violation of Article 50(7);
 10. A person who has installed the programs without obtaining the consent of users in violation of Article 50-5;
 11. A person who has posted advertisement information made for profit on the Internet homepage in violation of Article 50-7(1); or
 12. A person who has not observed the order to take corrective measures delivered by the Minister of Administration and Security or the Broadcasting and Communications Commission pursuant to Article 64(4) in violation of Articles 71 through 74, Subparagraphs 1 through 11 and Paragraph (2).
- (2) A person referred to in the following Subparagraphs shall be subject to a fine for negligence not exceeding 20 million won:
1. A person who has failed to make public or notify the users of entrusting the handling of personal information in violation of Article 25(2) (including the case to which the provisions are applied *mutatis mutandis* in Article 67);
 2. A person who has failed to notify the users of transferring the personal information in violation of Articles 26(1) and (2) (including the case to which the provisions are applied *mutatis mutandis* in Article 67);
 3. A person who has failed to designate the officer in charge of data protection in violation of Article 27(1) (including the case to which the provisions are applied *mutatis mutandis* in Article 67);
 4. A person who has failed to make public the personal information policy statement in violation of Article 27-2(1) (including the case to which the provisions are applied *mutatis mutandis* in Article 67);
- (3) A person referred to in the following Subparagraphs shall be subject to a fine for negligence not exceeding 10 million won:

1. A person who has failed to keep electronic messages in custody in violation of Article 20(2);
2. A person who has made public electronic messages in violation of Article 21;
3. A person who has failed to designate the officer in charge of youth protection in violation of Article 42-3(1);
4. A person who has failed to keep information in custody in violation of Article 43;
5. A person who has failed to insure the information and communications facilities in violation of Article 46(2);
6. A person who has failed to undergo the diagnosis of the safety of data protection in violation of Article 46-3(1);
7. A person who has failed to submit the result of the diagnosis of the safety of data protection or submitted the fraudulent report in violation of Article 46-3(2);
8. A person who has fraudulently notified the recommendation or the result pursuant to Article 46-3(5);
9. A person who has failed to observe the order to make improvement pursuant to Article 46-3(6);
10. A person who has failed to inform the user of software in violation of Article 47-3(3);
11. A person who has not observed the order of correction pursuant to Article 48-2(4);
12. A person who has obstructed, rejected or dodged the entry and inspection of business pursuant to Article 48-4(4);
13. A person who has used the name of KISA in violation of Article 52(6);
14. A person who has failed to report the recess, closure or dissolution of business in violation of Article 53(4);
15. A person who has failed to report the general terms and conditions of business in violation of Article 56(1);
16. A person who has failed to take managerial and technological measures in violation of Article 57(2);
- 17 through 21. *Related with communications billing services and omitted*
22. A person who has failed to submit related goods and documents, etc. pursuant to Article 64(1) or submitted false goods and documents, etc.;
23. A person who has denied the access to data and request of data production pursuant to Article 64(2); or
24. A person who has rejected, obstructed or dodged the entry and inspection of business

pursuant to Article 64(3).

- (4) The fine for negligence stated in Paragraphs (1) through (3) shall be imposed and collected by the Minister of Administration and Security or the Broadcasting and Communications Commission as prescribed by the Presidential Decree.
- (5) Any person who is dissatisfied with a fine for negligence imposed pursuant to Paragraph (4) may file an objection with the Minister of Administration and Security or the Broadcasting and Communications Commission within 30 days from the day of notification of such disposition.
- (6) If any person who has been subject to a fine for negligence pursuant to Paragraph (4) filed an objection pursuant to Paragraph (5), the Minister of Administration and Security or the Broadcasting and Communications Commission shall promptly notify the competent court of the fact, and the competent court shall, upon receiving the notification thereof, put the case on trial in accordance with the Non-Contentious Litigation Procedure Act.
- (7) If any person fails to file an objection within the period under Paragraph (5) and would not pay the fine for negligence, the fine for negligence in question shall be collected likewise by the disposition for recovery of the national taxes in arrears.

ADDENDA

Article 1 (Enforcement Date)

This Act shall enter into force on July 1, 2001.

Articles 2 - 3 *Omitted.*

Article 4 (Transitional Measures Regarding Application of Penal Provisions)

The application of the penal provisions to any act committed prior to the enforcement of this Act shall be governed by the previous provisions.

Article 5 *Omitted.*

Article 6 (Relations to Other Acts and Regulations)

If other acts and regulations cite the former “Act on the Promotion, etc. of Utilization of

Information System” or its provisions at the time of enforcement of this Act and if there exist corresponding provisions thereto in this Act, this Act or the corresponding provisions in this Act shall be regarded as being cited.

ADDENDA

Omitted for the period from December 2001 to December 2003.

ADDENDA

Article 1 (Enforcement Date)

This Act shall enter into force on the day of promulgation (dated of January 29, 2004); *provided, however,* that the revised provisions of Articles 28, 45(4), 46-3, 47-2(4) and 48-4(6) shall enter into force on the day when 6 months elapse after the promulgation.

Article 2 (Transitional Measures Regarding Application of Fine for Negligence)

The application of the fine for negligence to any act committed prior to the enforcement of this Act shall be governed by the previous provisions.

ADDENDUM

This Act shall enter into force on the day when 3 months elapse after its promulgation (dated of December 30, 2004).

ADDENDUM

This Act shall enter into force on the day when 3 months elapse after its promulgation (dated of December 30, 2005).

ADDENDA

Article 1 (Enforcement Date)

This Act shall enter into force on the day of promulgation (dated of February 29, 2008) *for the establishment of the Broadcasting and Communications Commission.*

Articles 2 through 6 *Omitted.*

Article 7 (Amendment to Other Acts)

15. The part of the Act on Promotion of Information and Communications Network Utilization and Data Protection, etc. shall be amended as follows: *Omitted*

Articles 8 through 12 *Omitted.*

ADDENDA

Article 1 (Enforcement Date)

This Act shall enter into force on the day when 6 months elapse after its promulgation (dated of June 13, 2008)

Article 2 (Transitional Measures Regarding Application of Penal Provisions and Fine for Negligence)

The application of the penal provisions and the fine for negligence to any act committed prior to the enforcement of this Act shall be governed by the previous provisions.

ADDENDA

Article 1 (Enforcement Date)

This Act shall enter into force on the day when 3 months elapse after its promulgation (dated of April 22, 2009) *for the establishment of the Korea Internet & Security Agency.*

Articles 2 and 3 *Omitted.*

Article 4 (Amendment to Other Acts) *Omitted.*

Article 5 (Relations to Other Acts and Regulations)

If other acts and regulations cite the former “Act on Promotion of Information and Communications Network Utilization and Data Protection, etc.” or its provisions at the time of enforcement of this Act and if there exist corresponding provisions thereto in this Act, this Act or the corresponding provisions in this Act shall be regarded as being cited.

ADDENDUM

This Act shall enter into force on the day of promulgation (dated of March 17, 2010).

ADDENDA

Article 1 (Enforcement Date)

This Act shall enter into force on the day when 6 months elapse after its promulgation (dated of March 22, 2010).

Articles 2 through 5 *Omitted.*

Article 6 (Amendment to Other Acts)

9. The part of the Act on Promotion of Information and Communications Network Utilization and Data Protection, etc. shall be amended as follows: Article 68 shall be deleted.

Article 7 *Omitted.*

ADDENDA

Article 1 (Enforcement Date)

This Act shall enter into force on the day when 6 months elapse after its promulgation (dated of March 22, 2010).

Articles 2 through 6 *Omitted.*

Article 7 (Amendment to Other Acts)

7. The part of the Act on Promotion of Information and Communications Network Utilization and Data Protection, etc. shall be amended as follows: [. . .] the Framework Act on Electricity and Communications shall read the Electric and Communication Services Act.

Articles 8 and 9 *Omitted.*