

법령, 판례 등 모든 법령정보를 한 번에 검색 OK !

**ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS
NETWORK UTILIZATION AND INFORMATION PROTECTION**

[Enforcement Date 24. Jul, 2024.] [Act No.20069, 23. Jan, 2024., Partial Amendment]

방송통신위원회 (디지털이용자기반과 - 스팸)02-2110-1522, 1524



법제처 국가법령정보센터

www.law.go.kr

2024.06.17

ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND INFORMATION PROTECTION

[Enforcement Date 24. Jul, 2024.] [Act No.20069, 23. Jan, 2024., Partial Amendment]

방송통신위원회 (디지털이용자기반과 - 스팸) 02-2110-1522, 1524
과학기술정보통신부 (통신자원정책과 - 통신과금관련) 044-202-6669
과학기술정보통신부 (사이버침해대응과 - 해킹 등 침해대응 관련) 044-202-6461, 6462
방송통신위원회 (이용자정책총괄과) 02-2110-1514
방송통신위원회 (디지털유해정보대응과 - 불법정보 및 청소년보호 관련) 02-2110-1564, 1549
방송통신위원회 (디지털이용자기반과 - 본인확인제 관련) 02-2110-1521
과학기술정보통신부 (디지털기반안전과- 집적정보통신시설 관련) 044-202-6777, 6778

CHAPTER I GENERAL PROVISIONS

Article 1 (Purpose) The purpose of this Act is to contribute to improving citizens' lives and enhancing public welfare by facilitating utilization of information and communications networks, protecting people using information and communications services, and developing an environment in which people can utilize information and communications networks in a healthier and safer way. <Amended on Feb. 4, 2020>

[This Article Wholly Amended on Jun. 13, 2008]

Article 2 (Definitions) (1) The terms used in this Act are defined as follows: <Amended on Jan. 29, 2004; Jan. 26, 2007; Dec. 21, 2007; Jun. 13, 2008; Mar. 22, 2010; May 28, 2014; Jun. 9, 2020>

1. The term "information and communications network" means an information and communications system for collecting, processing, storing, searching, transmitting, or receiving information by using telecommunications equipment defined in subparagraph 2 of Article 2 of the Telecommunications Business Act or computers and applied computer technology;
2. The term "information and communications services" means telecommunications services defined in subparagraph 6 of Article 2 of the Telecommunications Business Act and services providing information or intermediating the provision of information by using such telecommunications services;

3. The term "provider of information and communications services" means a telecommunications business entity defined in subparagraph 8 of Article 2 of the Telecommunications Business Act and any other person who provides information or intermediates to provide information commercially by utilizing services provided by a telecommunications business entity;
4. The term "user" means a person who uses information and communications services rendered by providers of information and communications services;
5. The term "electronic document" means data prepared and transmitted, received, or stored electronically in a standardized document by a device capable of processing information, such as a computer;
6. Deleted; <Feb. 4, 2020>
7. The term "computer security incident" means an event resulting from an attack on an information and communications network or an information system related to such network by any of the following:
 - (a) Means of hacking, computer virus, logic bomb, electronic mail bomb, denial of service, high-power electromagnetic wave, etc.;
 - (b) Means of installing, in an information and communications network or an information system related thereto, a program, technical device, etc. that enables to bypass the normal protection and authentication processes of the information and communications network and makes access thereto possible;
8. Deleted; <Jun. 22, 2015>
9. The term "message board" means, regardless of its name, a computer program or a technical device with which users can publish information in the form of a code, letters, voice, sound, image, motion picture, or any other form purposely to disclose the information to the public by using an information and communications network;
10. The term "telecommunications billing services" means information and communications services to perform the following business activities:
 - (a) Business activities charging and collecting prices for goods or services sold or provided by a third person (hereinafter referred to as "goods or services") together with charges for the telecommunications services provided;
 - (b) Business activities transmitting and receiving information on transactions electronically so that prices for goods or services sold or provided by a third person can be billed or

collected together with charges for the telecommunications services provided by under item (a), or settling, on behalf of another person, or intermediating payments for such prices;

11. The term "provider of telecommunications billing services" means a person who provides telecommunications billing services after being registered under Article 53;

12. The term "user of telecommunications billing services" means a person who purchases or uses goods or services by using telecommunications billing services rendered by a provider of telecommunications billing services;

13. The term "electronic transmission medium" means a medium transmitting codes, letters, voices, images, or motion pictures to addressees in an electronic form, such as an electronic document, via information and communications networks.

(2) Except as provided in paragraph (1), definitions of the terms used in this Act shall be governed by the Framework Act on National Informatization. <Amended on Jun. 13, 2008; Mar. 23, 2013; Jun. 9, 2020>

Article 3 (Responsibilities of Providers and Users of Information and Communications

Services) (1) Every provider of information and communications services shall contribute to protection of rights and interests of users and enhancement of users' abilities to use information by protecting users and providing information and communications services in a healthier and safer way. <Amended on Feb. 4, 2020>

(2) Every user shall make efforts to help to establish a healthier information society.

(3) The Government may provide support organizations composed of providers or users of information and communications services in their activities for protecting information and protecting youths in information and communications networks. <Amended on Feb. 4, 2020>

[This Article Wholly Amended on Jun. 13, 2008]

Article 4 (Formulating Policy on Promotion of Utilization of Information and Communications

Networks and Protection of Information) (1) The Minister of Science and ICT or the Korea Communications Commission shall formulate policies to lay the foundations for an information society through the promotion of utilization of information and communications networks; the stable management and operation of such networks; the protection of users; and other related activities (hereinafter referred to as "promotion of

utilization of information and communications networks, the protection of information, or other related matters"). <Amended on Mar. 29, 2011; Mar. 23, 2013; Jul. 26, 2017; Feb. 4, 2020>

(2) The policies under paragraph (1) shall contain descriptions of the following: <Amended on Dec. 24, 2018; Jun. 9, 2020>

1. Development and dissemination of technology related to information and communications networks;
 2. Standardization of information and communications networks;
 3. Promotion of utilization of information and communications networks, including the development of content of information and applied service for information and communications networks under Article 11;
 4. Facilitation of sharing information through information and communications networks;
 5. Promotion of use of the Internet;
 6. Deleted; <Feb. 4, 2020>
 - 6-2. Deleted; <Feb. 4, 2020>
 7. Protection of youths in information and communications networks;
 - 7-2. Development and dissemination of technologies that identify false sounds, visions, pictorial images, etc., made using artificial intelligence technology, among information circulated through information and communications networks;
 8. Enhancement of safety and reliability of information and communications networks;
 9. Other matters necessary for the promotion of utilization of information and communications networks, the protection of information, or other related matters.
- (3) When preparing the policies under paragraph (1), the Minister of Science and ICT or the Korea Communications Commission shall ensure that the policies conform to the basic plan for national informatization under Article 6 of the Framework Act on National Informatization. <Amended on Mar. 29, 2011; Mar. 23, 2013; Jul. 26, 2017; Jun. 9, 2020>
[This Article Wholly Amended on Jun. 13, 2008]

Article 5 (Relationship to Other Statutes) Except as otherwise provided in any other statute, the promotion of utilization of information and communications networks, the protection of information, or other related matters shall be governed by this Act: Provided, That, in the event of a conflict between this Act and the Electronic Financial Transactions Act with respect to telecommunications billing services under Chapter VII, this Act shall prevail.

<Amended on Jun. 12, 2018; Feb. 4, 2020>

[This Article Wholly Amended on Jun. 13, 2008]

Article 5-2 (Application to Acts Done Overseas) This Act shall apply to any act done overseas if such conduct affects the domestic market or users in the market.

[This Article Newly Inserted on Jun. 9, 2020]

CHAPTER II PROMOTION OF UTILIZATION OF INFORMATION AND COMMUNICATIONS NETWORKS

Article 6 (Development of Technology) (1) The Minister of Science and ICT may engage the relevant research institute, as prescribed by Presidential Decree, to implement a project for research and development, technical cooperation, transfer of technology, technical guidance, or similar, in order to effectively promote the development of technology and equipment related to information and communications networks. <Amended on Mar. 23, 2013; Jul. 26, 2017>

(2) The Government may provide financial support to a research institute that implements a project for research and development or similar in accordance with paragraph (1) for all or part of the cost and expenses incurred in such project.

(3) Matters necessary for the disbursement and management of cost and expenses under paragraph (2) shall be prescribed by Presidential Decree.

[This Article Wholly Amended on Jun. 13, 2008]

Article 7 (Management and Dissemination of Technology-Related Information) (1) The Minister of Science and ICT shall manage, systematically and comprehensively, the information pertaining to technology and equipment related to information and communications networks (hereafter in this Article referred to as "technology-related information"). <Amended on Mar. 23, 2013; Jul. 26, 2017>

(2) If necessary for managing technology-related information systematically and comprehensively, the Minister of Science and ICT may request data relevant to technology-related information from the relevant administrative agency and a national or public research institute. Upon such request, the head of such agency or institute shall comply therewith, unless there is a compelling reason not to do so. <Amended on Mar. 23, 2013; Jul. 26, 2017>

(3) The Minister of Science and ICT shall perform projects for dissemination of technology-related information, so that technology-related information can be used promptly and easily. <Amended on Mar. 23, 2013; Jul. 26, 2017>

(4) Matters necessary for the scope of technology and equipment related to information and communications networks which are to be disseminated pursuant to paragraph (3), shall be prescribed by Presidential Decree.

[This Article Wholly Amended on Jun. 13, 2008]

Article 8 (Standardization and Certification of Information and Communications Networks) (1)

The Minister of Science and ICT shall establish and give public notice of the standards for information and communications networks in order to promote the utilization of information and communications networks, and may recommend providers of information and communications services or persons who manufacture or supply products related to information and communications networks to comply with the standards: Provided, That the matters for which the Korean Industrial Standards under Article 12 of the Industrial Standardization Act have already been established shall comply with such standards.

<Amended on Mar. 23, 2013; Jul. 26, 2017>

(2) A person who manufactures or supplies a product related to information communications in conformity with the standards publicly notified pursuant to paragraph (1) may put on the product a mark stating that the product conforms to the standards, subject to the prior certification of the certification body under Article 9 (1).

(3) Where a product falls under the proviso of paragraph (1) and the certification under Article 15 of the Industrial Standardization Act has been already given to the product, the product shall be deemed to have been certified pursuant to paragraph (2).

(4) No person other than a person who holds the certification under paragraph (2) may put a mark verifying that his or her product conforms to the standards or put any similar mark, nor may he or she sell a product with any similar mark or display such product for the purpose of sale.

(5) The Minister of Science and ICT may order a person who sells a product or displays such product for the purpose of sale in violation of paragraph (4), to collect and recall the product or to obtain certification to put such mark; or may take any other corrective measure as necessary. <Amended on Mar. 23, 2013; Jul. 26, 2017>

(6) Matters regarding the subject matters of the standardization, the methods and procedures for such standardization, and a mark of certification under paragraphs (1) through (3), and the collection, recall, corrective measures, etc. under paragraph (5) shall be prescribed by Ordinance of the Ministry of Science and ICT. <Amended on Mar. 23, 2013; Jul. 26, 2017>

[This Article Wholly Amended on Jun. 13, 2008]

Article 9 (Designation of Quality Certifying Institutions) (1) The Minister of Science and ICT may designate an institution to certify that products related to information and communications networks (hereinafter referred to as "certification body"), which are manufactured or supplied by a person, conform to the standards publicly notified pursuant to the main clause of Article 8 (1). <Amended on Mar. 23, 2013; Jul. 26, 2017>

(2) If a certification body falls under any of the following, the Minister of Science and ICT may revoke the designation of such body or give an order of business suspension for a prescribed period not exceeding six months: Provided, That the Minister of Science and ICT shall revoke such designation, if it falls under subparagraph 1: <Amended on Mar. 23, 2013; Jul. 26, 2017>

1. If the body is designated by fraud or other improper means;
2. If the body has not continued its certification services for at least one year without good cause;
3. If the body fails to meet the standards for designation under paragraph (3).

(3) Matters regarding the standards and procedures for designation under paragraph (1), and the criteria for revocation of designation and for business suspension of a certification body under paragraph (2), and other related matters shall be prescribed by Ordinance of the Ministry of Science and ICT. <Amended on Mar. 23, 2013; Jul. 26, 2017>

[This Article Wholly Amended on Jun. 13, 2008]

Article 10 (Support for Development of Content of Information) With an aim of securing national competitiveness and enhancing the public interest, the Government may provide financial and technical support, or otherwise, to persons who develop relevant contents of information that can be distributed through information and communications networks.

[This Article Wholly Amended on Jun. 13, 2008]

Article 11 (Acceleration of Development of Applied Services for Information and

Communications Networks) (1) The Government may provide financial and technical support or other necessary support to any State agency, local government, or public institution that develops and operates applied services for improving efficiency in processing its business affairs or automatizing or upgrading its business process by utilizing information and communications network (hereinafter referred to as "applied services for information and communications networks").

(2) The Government may provide financial and technical support or other necessary support to the private sector with an aim of facilitating the development of applied services for information and communications networks by the private sector; and shall take the following measures for nurturing technical human resources necessary to develop applied services for information and communications networks:

1. Support for Internet education conducted by schools at different levels and other educational institutions;
2. Extension of Internet education for citizens;
3. Support for projects to cultivate technical human resources specializing in information and communications networks;
4. Establishment of and support for institutions to cultivate technical human resources specializing in information and communications networks;
5. Support for development and dissemination of educational programs for utilizing information and communications networks;
6. Support for establishment of the technical qualification system related to information and communications networks and support for supply of technical human resources specializing in information and communications networks on demand;
7. Other matters necessary to cultivate technical human resources related to information and communications networks.

[This Article Wholly Amended on Jun. 13, 2008]

Article 12 (Establishment of System for Sharing Information) (1) The Government may encourage the development of a system for sharing information through linked operation and standardization of information and communications networks or in any other way so that the networks can be made efficient use of.

(2) The Government may provide financial and technical support or other necessary support to any person who develops a system for sharing information under paragraph (1).

(3) Matters necessary for the encouragement and support under paragraphs (1) and (2) shall be prescribed by Presidential Decree.

[This Article Wholly Amended on Jun. 13, 2008]

Article 13 (Projects for Promoting Utilization of Information and Communications Networks)

(1) The Minister of Science and ICT may implement projects designed to promote efficient utilization and dissemination of technology, equipment, and applied services related to information and communications networks, as prescribed by Presidential Decree, in order to promote the utilization of information and communications networks in various areas of public service, local communities, industry, life, and social welfare and to eliminate gaps in accessibility to information. <Amended on Mar. 23, 2013; Jul. 26, 2017>

(2) The Government may provide financial and technical support or other necessary support to persons who participate in the projects under paragraph (1).

[This Article Wholly Amended on Jun. 13, 2008]

Article 14 (Proliferation of the Internet) The Government shall formulate and implement policies to induce the public and private sectors to use Internet facilities available in the public and private sectors so that the Internet can be widely used; to form the basis for using the Internet through education and public relations activities on the Internet; and to eliminate gaps in accessibility to the Internet between localities, genders, and ages.

[This Article Wholly Amended on Jun. 13, 2008]

Article 15 (Improvement of Quality of Internet Services) (1) The Minister of Science and ICT shall formulate and implement policies to protect rights and interests of users of Internet services and to ensure improvement of quality of Internet services and stable availability of Internet services. <Amended on Mar. 23, 2013; Jul. 26, 2017>

(2) If deemed necessary for implementing the policies under paragraph (1), the Minister of Science and ICT may prescribe and give public notice of the standards for measuring and assessing the quality of Internet services, hearing opinions of organizations of providers and users of information and communications services and others. <Amended on Mar. 23, 2013; Jul. 26, 2017>

(3) Every provider of information and communications services may voluntarily assess the current status of quality of his or her own Internet services in accordance with the standards under paragraph (2) and may notify the results thereof to users.

[This Article Wholly Amended on Jun. 13, 2008]

Article 16 Deleted. <Jan. 29, 2004>

Article 17 Deleted. <Jan. 29, 2004>

CHAPTER III Deleted.

Article 18 Deleted. <Jun. 22, 2015>

Article 19 Deleted. <Jun. 22, 2015>

Article 20 Deleted. <Jun. 22, 2015>

Article 21 Deleted. <Jun. 22, 2015>

CHAPTER IV CREATION OF SAFE ENVIRONMENT FOR USE OF INFORMATION AND COMMUNICATIONS

SECTION 1 Deleted

Article 22 Deleted. <Feb. 4, 2020>

Article 22-2 (Consent to Access Authority) (1) Where a provider of information and communications services needs authority to access (hereinafter referred to as "access authority") information stored and functions installed in mobile devices of users in order to provide the relevant services, the provider shall inform users of the following so that users may clearly recognize such matters, and shall obtain consent of users:

1. In the case of access authority certainly necessary to provide the relevant services:
 - (a) Items of the information and functions for which access authority is necessary;
 - (b) Grounds that access authority is necessary;
2. In the case of access authority not certainly necessary to provide the relevant services:
 - (a) Items of the information and functions for which access authority is necessary;

(b) Grounds that access authority is necessary;

(c) Fact that users may give no consent to the permission for access authority.

(2) No provider of information and communications services shall refuse to provide the relevant services to users on the ground that the users give no consent to the establishment of access authority not certainly necessary to provide the relevant services.

(3) Persons manufacturing and providing a basic operating system (referring to an operating environment in which software installed in mobile devices can be run) of mobile devices, manufacturers of mobile devices, and persons manufacturing and providing a software for mobile devices shall take measures necessary for protecting users' information, such as devising methods for users to give or revoke consent to access authority where the provider of information and communications services intends to access the information stored and functions installed in mobile devices.

(4) The Korea Communications Commission may conduct compliance inspections to ascertain that access authority is set for relevant services in accordance with paragraphs (1) through (3). <Newly Inserted on Jun. 12, 2018>

(5) The scope of, and methods for consenting to, access authority referred to in paragraph (1), the measures necessary for protecting users' information referred to in paragraph (3), and other necessary matters shall be prescribed by Presidential Decree. <Amended on Jun. 12, 2018>

[This Article Newly Inserted on Mar. 22, 2016]

Article 23 Deleted. <Feb. 4, 2020>

Article 23-2 (Restrictions on Use of Resident Registration Numbers) (1) Except in any of the following cases, no provider of information and communications services may collect or use users' resident registration numbers: <Amended on Feb. 4, 2020>

1. Where the provider is designated as an identification service agency pursuant to Article 23-3;

2. Deleted; <Feb. 4, 2020>

3. Where a telecommunications business entity, who resells a mobile communications service and the like provided by a facilities-based telecommunications business entity under Article 38 (1) of the Telecommunications Business Act, collects or uses resident

registration numbers of users in relation to performing the identification service of a mobile telecommunications business entity designated as an identification service agency under Article 23-3.

(2) Even where the collection and use of users' resident registration numbers is authorized pursuant to paragraph (1) 3, an identification method without using the users' resident registration numbers (hereinafter referred to as "alternative means") shall be provided.

<Amended on Feb. 4, 2020>

[This Article Wholly Amended on Feb. 17, 2012]

Article 23-3 (Designation of Identification Service Agencies) (1) The Korea Communications Commission may, after reviewing the following, designate a person as an identification service agency who is deemed competent to safely and reliably perform the affairs of development, provision, and administration of the alternative means (hereinafter referred to as "identification service"):

1. A plan for physical, technological, and administrative measures in order to secure safety of the identification service;
2. Technological and financial capability necessary for performing the identification service;
3. Appropriateness of the scale of facilities relevant to the identification service.

(2) When an identification service agency intends to fully or partially suspend the identification service, it shall determine and notify a suspension period to the users not later than 30 days prior to the intended date of suspension and shall report the same to the Korea Communications Commission. In such cases, the suspension period shall not exceed six months.

(3) When an identification service agency intends to discontinue the identification service, it shall notify the intention to the users not later than 60 days prior to the intended date of discontinuation and shall report the same to the Korea Communications Commission.

(4) Matters necessary for the detailed review criteria for each item subject to the review and the designation procedures for identification service agencies under paragraph (1), suspension or discontinuation of the identification service under paragraphs (2) and (3), and other matters shall be prescribed by Presidential Decree.

[This Article Newly Inserted on Apr. 5, 2011]

Article 23-4 (Suspension of Identification Services and Revocation of Designation of

Identification Service Agencies) (1) When an identification service agency falls under any of the following, the Korea Communications Commission may order full or partial suspension of its identification service for a specified period of up to six months or revoke the designation of the identification service agency: Provided, That in cases falling under subparagraph 1 or 2, the Korea Communications Commission shall revoke the designation of the identification service agency:

1. Where the identification service agency is designated by fraud or other improper means;
2. Where a person who has received an order to suspend the identification service fails to suspend such service in violation of the order;
3. Where a person fails to start the identification service within six months from the date of designation, or has suspended the service for at least six consecutive months;
4. Where the identification service agency no longer meets the standards for designation pursuant to Article 23-3 (4).

(2) Standards and procedures for disposition granted under paragraph (1) and other necessary matters shall be prescribed by Presidential Decree.

[This Article Newly Inserted on Apr. 5, 2011]

Article 23-5 (Creation and Processing of Connecting Information) (1) An identification service agency shall not create, provide, use, compare, link irreversibly encrypted form of any user's resident registration number (hereinafter referred to as "connecting information") or perform other similar acts (hereinafter referred to as "processing") for the purpose of interlinking the services of a provider of information and communication services, except in cases falling under any of the following subparagraphs:

1. Where providing services to safely identify and authenticate users using information entered by the users;
2. Where administrative agencies and public institutions (hereinafter referred to as "administrative agencies, etc.") holding uniquely identifiable information under Article 24 of the Personal Information Protection Act (hereinafter in this Article referred to as "uniquely identifiable information") utilize connecting information to provide electronic government service defined in subparagraph 5 of Article 2 of the Electronic Government Act, in any of the following cases:

- (a) Where the head of a central agency responsible for administrative affairs under subparagraph 4 of Article 2 of the Electronic Government Act requests for the creation and processing of connecting information in order to provide integral support to administrative agencies, etc. for the identification of users;
 - (b) Where an administrative agency, etc. inevitably requests the creation and processing of connecting information without obtaining the user's consent within the scope of the purpose of processing uniquely identifiable information;
3. Where a person holding uniquely identifiable information requests the creation and processing of connecting information of a data subject who has requested the transmission of personal information in order to fulfill the obligation to transmit personal information pursuant to Article 35-2 of the Personal Information Protection Act;
4. Where the processing of resident registration numbers is permitted under the subparagraphs of Article 24-2 (1) of the Personal Information Protection Act, and the identification service agency and the relevant provider of information and communications services together have obtained approval from the Korea Communications Commission for providing information and communication services prescribed by the Presidential Decree for which it is inevitable to create and process connecting information without obtaining the consent of the user.
- (2) Where the Korea Communications Commission intends to approve the creation and processing of connecting information under paragraph (1) 4, the Commission shall comprehensively examine the following matters:
- 1. Appropriateness and innovativeness of the realization of services to be provided;
 - 2. Adequacy of procedures for creating and processing connecting information;
 - 3. Plans for physical, technical, and administrative measures to ensure safety in creating and processing connecting information;
 - 4. Adequacy of measures to protect the rights of users;
 - 5. Impacts and effects on relevant markets and user benefits.
- (3) The Korea Communications Commission may revoke approval for the creation and processing of connecting information under paragraph (1) 4 in any of the following: Provided, That in the case of subparagraph 1, the approval shall be revoked:

1. Where they have obtained approval for the creation and processing of connecting information under paragraph (1) 4 by fraud or in any other improper means;
2. Where they fail to comply with the matters examined under each subparagraph of paragraph (2);
3. Where they violate the obligation to take physical, technical, or administrative measures under Article 23-6 (1);
4. Where they violate a statute or regulation related to the protection of personal information and the reason for such violation is material.

(4) A person who is provided with connecting information from an identification service agency (hereinafter referred to as a "entity using connecting information") for the services under the subparagraphs of paragraph (1) may process the connecting information within the scope of purposes for which the person has been provided: Provided, That if the data subject separately consents, the connecting information may be processed within the scope of the consented purpose.

(5) Matters necessary for approval procedures for creating and processing connecting information under paragraphs (1) through (4), detailed examination criteria for each approval, criteria for revoking approval, and other matters shall be prescribed by Presidential Decree.

[This Article Newly Inserted on Jan. 23, 2024]

[\[Effective date has not yet specified\]](#)

Article 23-6 (Obligation to Take Safety Measures for Connecting information) (1) Where an identification service agency creates and processes connecting information, it shall take physical, technical and administrative measures to ensure safety for creating and processing the connecting information in addition to the measures under Article 29 of the Personal Information Protection Act.

(2) Where an entity using connecting information provides services under the subparagraphs of Article 23-5 (1), in addition to measures pursuant to Article 29 of the Personal Information Protection Act, the entity shall store and manage the connecting information separately from resident registration numbers and take measures to ensure that the connecting information is not lost, stolen, leaked, falsified, altered, or damaged (hereinafter referred to as "safety measures").

(3) The Korea Communications Commission may inspect the operation and management of physical, technical and administrative measures taken by an identification service agency that meets the standards prescribed by the Presidential Decree, including the scale and turnover of connecting information created and processed, and safety measures taken by the entity using the connecting information.

(4) The Korea Communications Commission may entrust the affairs regarding inspection under paragraph (3) to a specialized institution prescribed by Presidential Decree.

(5) Matters necessary for the physical, technical and administrative measures under paragraph (1) and the safety measures under paragraph (2) shall be prescribed by Presidential Decree.

[This Article Newly Inserted on Jan. 23, 2024]

Article 24 Deleted. <Feb. 4, 2020>

Article 24-2 Deleted. <Feb. 4, 2020>

Article 25 Deleted. <Feb. 4, 2020>

Article 26 Deleted. <Feb. 4, 2020>

Article 26-2 Deleted. <Feb. 4, 2020>

SECTION 2 Deleted

Article 27 Deleted. <Feb. 4, 2020>

Article 27-2 Deleted. <Feb. 4, 2020>

Article 27-3 Deleted. <Feb. 4, 2020>

Article 28 Deleted. <Feb. 4, 2020>

Article 28-2 Deleted. <Feb. 4, 2020>

Article 29 Deleted. <Feb. 4, 2020>

Article 29-2 Deleted. <Feb. 4, 2020>

SECTION 3 Deleted

Article 30 Deleted. <Feb. 4, 2020>

Article 30-2 Deleted. <Feb. 4, 2020>

Article 31 Deleted. <Feb. 4, 2020>

Article 32 Deleted. <Feb. 4, 2020>

Article 32-2 Deleted. <Feb. 4, 2020>

Article 32-3 Deleted. <Feb. 4, 2020>

Article 32-4 Deleted. <Feb. 4, 2020>

Article 32-5 (Designation of Domestic Agents) (1) A person who meets the criteria prescribed by Presidential Decree, based upon considerations such as the number of users and sales, from among providers of information and communications services or similar with no domicile or place of business in the Republic of Korea, shall designate, in writing, an agent to act on his or her behalf with respect to the following (hereinafter referred to as "domestic agent"):

1. Deleted; <Feb. 4, 2020>
2. Deleted; <Feb. 4, 2020>
3. Submission of related articles, documents, etc. under Article 64 (1).

(2) A domestic agent shall be a person who has a domicile or place of business in the Republic of Korea.

(3) In designating a domestic agent pursuant to paragraph (1), all the following matters shall be disclosed on its website and the like: <Amended on Feb. 4, 2020>

1. The domestic agent's name (if the domestic agent is a corporation, referring to the name of the corporation and the name of its representative);
2. The domestic agent's domicile (if the domestic agent is a corporation, referring to the address of its place of business), and his or her telephone number and electronic mail address.

(4) If a domestic agent violates this Act in relation to the subparagraphs of paragraph (1), such violation shall be deemed to have been committed by the relevant provider of information and communications services or similar.

[This Article Newly Inserted on Sep. 18, 2018]

SECTION 4 Deleted

Article 33 Deleted. <Mar. 29, 2011>

Article 33-2 Deleted. <Mar. 29, 2011>

Article 34 Deleted. <Mar. 29, 2011>

Article 35 Deleted. <Mar. 29, 2011>

Article 36 Deleted. <Mar. 29, 2011>

Article 37 Deleted. <Mar. 29, 2011>

Article 38 Deleted. <Mar. 29, 2011>

Article 39 Deleted. <Mar. 29, 2011>

Article 40 Deleted. <Mar. 29, 2011>

CHAPTER V PROTECTION OF USERS IN INFORMATION AND COMMUNICATIONS NETWORKS

Article 41 (Preparation of Policy on Protection of Youths) (1) The Korea Communications Commission shall prepare a policy on the following measures to protect youths from information harmful to youth, such as information of obscenities and violence, circulated through information and communications networks (hereinafter referred to as "information harmful to youth"):

1. Development and dissemination of content-screening software;
2. Development and dissemination of technology for protection of youths;
3. Education and public relations activities for protection of youths;

4. Other matters prescribed by Presidential Decree for protection of youths.

(2) The Korea Communications Commission may, in an effort to implement the policy under paragraph (1), support activities conducted by the Korea Communications Standards Commission under Article 18 of the Act on the Establishment and Operation of Korea Communications Commission (hereinafter referred to as the "Communications Standards Commission"), organizations of providers or users of information and communications services, and other relevant specialized institutions for protection of youths.

[This Article Wholly Amended on Jun. 13, 2008]

Article 42 (Labeling of Media Products Harmful to Youths) A person who provides information to the general public purposely to make it public through telecommunications services rendered by a telecommunications business entity (hereinafter referred to as "information provider") and who intends to provide any media product harmful to youths defined in subparagraph 3 of Article 2 of the Youth Protection Act among the media products referred to in subparagraph 2 (e) of Article 2 of that Act, shall put a label indicating that the information is a media product harmful to youths by the labeling method prescribed by Presidential Decree. <Amended on Sep. 15, 2011>

[This Article Wholly Amended on Jun. 13, 2008]

Article 42-2 (Prohibition on Advertisement of Media Products Harmful to Youths) No one may transmit, to a youth defined in subparagraph 1 of Article 2 of the Youth Protection Act, any information containing an advertisement of a media product harmful to youths defined in subparagraph 3 of Article 2 of that Act among the media products referred to in subparagraph 2 (e) of Article 2 of that Act in the form of code, letter, voice, sound, image, or motion picture through an information and communications network or display such information to the general public without taking any measure to restrict access by a youth. <Amended on Sep. 15, 2011>

[This Article Wholly Amended on Jun. 13, 2008]

Article 42-3 (Designation of Persons Responsible for Protection of Youths) (1) A provider of information and communications services who meets the criteria prescribed by Presidential Decree, such as the average number of daily users and sales, shall designate a person responsible for protection of youths to keep youths from information harmful to youths in

the information and communication network.

(2) The person responsible for protection of youths shall be chosen from among executive officers of the relevant business entity or the persons in a position equivalent to the head of a department responsible for business affairs related to protection of youths.

(3) The person responsible for protection of youths shall block and control information harmful to youths in the information and communications network and shall perform business affairs for protection of youths, including establishment of a plan for protection of youths from information harmful to youths.

(4) Matters necessary for designating a person responsible for protection of youths under paragraph (1) shall be prescribed by Presidential Decree.

[This Article Wholly Amended on Jun. 13, 2008]

Article 43 (Duty of Providers of Visual or Sound Information to Keep Information) (1) An information provider prescribed by Presidential Decree from among those who engage in business providing media products harmful to youths defined in subparagraph 3 of Article 2 of the Youth Protection Act among the media products referred to in subparagraph 2 (e) of Article 2 of that Act in a way to make it impossible to save or record the harmful media products in a user's computer shall keep relevant information. <Amended on Sep. 15, 2011>

(2) The period during which an information provider under paragraph (1) is obligated to keep relevant information shall be prescribed by Presidential Decree.

[This Article Wholly Amended on Jun. 13, 2008]

Article 44 (Protection of Rights in Information and Communications Networks) (1) No user may circulate any information in violation of other person's rights, including invasion of privacy and defamation, through an information and communications network.

(2) Every provider of information and communications services shall make efforts to prevent any information under paragraph (1) from being circulated through the information and communications network operated and managed by the provider.

(3) The Korea Communications Commission may prepare a policy on technological development, education, public relations activities, and other activities to prevent violation of other persons' rights by information circulated through information and communications

networks, including invasion of privacy and defamation and may recommend providers of information and communications services to adopt the policy. <Amended on Mar. 23, 2013; May 28, 2014>

[This Article Wholly Amended on Jun. 13, 2008]

Article 44-2 (Request for Deletion of Information) (1) Where information provided through an information and communications network purposely to be made public intrudes on other persons' privacy, defames other persons, or violates other persons' right otherwise, the victim of such violation may request the provider of information and communications services who managed the information to delete the information or publish a rebuttable statement (hereinafter referred to as "deletion or rebuttal"), presenting explanatory materials supporting the alleged violation. In such cases, a person who requesting deletion or rebuttal (hereafter in this Article referred to as "applicant") may designate a means to be notified of the progress and results of such processing, such as a text message or e-mail, and a person who has posted the relevant information (hereafter in this Article referred to as "person who posted information") may designate in advance the means to be notified of the fact of taking measures under paragraph (2), such as text messages or e-mails. <Amended on Mar. 22, 2016; Jan. 3, 2023>

(2) Upon receipt of a request for deletion or rebuttal of the information under paragraph (1), a provider of information and communications services shall delete the information or take a temporary or any other necessary measure and shall notify the applicant and the publisher of the information without delay. In such cases, the provider of information and communications services shall make it known to users that he or she has taken necessary measures by posting a public notification on the relevant message board or in any other way.

(3) If there is any media product harmful to youths published in violation of the labeling method under Article 42 in the information and communications network operated and managed by a provider of information and communications services or if a content advertising any media product harmful to youths is displayed in such network without any measures to restrict access by youths under Article 42-2, the provider shall delete such content without delay.

(4) Notwithstanding a request for deletion of the information under paragraph (1), if it is impracticable to judge whether information violates any right or it is anticipated that there will probably be a dispute between interested parties, a provider of information and communications services may take a measure to block access to the information temporarily (hereinafter referred to as "temporary measures"). In such cases, the period for the temporary measure shall not exceed 30 days.

(5) Every provider of information and communications services shall clearly state in advance the details, procedures, and other matters regarding necessary measures in the terms and conditions.

(6) If a provider of information and communications services takes necessary measures under paragraph (2) for the information circulated through the information and communications network operated and managed by himself or herself, the provider may have his or her liability to indemnify loss incurred by such information mitigated or discharged.

[This Article Wholly Amended on Jun. 13, 2008]

Article 44-3 (Discretionary Temporary Measures) (1) If a provider of information and communications services finds that information circulated through the information and communications network which he or she operates and manages, intrudes on someone's privacy, defames someone, or violates someone's rights, the provider may take temporary measures at his or her discretion.

(2) The latter part of Article 44-2 (2), the latter part of Article 44-2 (4), and Article 44-2 (5) shall apply mutatis mutandis to the temporary measures under paragraph (1).

[This Article Wholly Amended on Jun. 13, 2008]

Article 44-4 (Self-Regulation) (1) An organization of providers of information and communications services may establish and implement a code of conduct applicable to providers of information and communications services with an objective to protect users and render information and communications services more safely and reliably. <Amended on Dec. 24, 2018>

(2) An organization of providers of information and communications services may establish and enforce self-regulating guidelines for monitoring, etc. so as to prevent any of the

following information from being circulated in information and communications networks:

<Newly Inserted on Dec. 24, 2018>

1. Information harmful to youth;
2. Unlawful information under Article 44-7.

(3) The Government may support self-regulating activities by organizations of providers of information and communications services under paragraphs (1) and (2). <Newly Inserted on Dec. 24, 2018>

[This Article Wholly Amended on Jun. 13, 2008]

Article 44-5 (Identity Verification of Users of Message Boards) (1) If any of the following persons intends to install and operate a message board, he or she shall take necessary measures, as prescribed by Presidential Decree (hereinafter referred to as "measures for identity verification"), including preparation of methods and procedures for verifying identity of users of the message board:

1. A State agency, local government, public enterprise, or quasi-government agency under Article 5 (3) of the Act on the Management of Public Institutions, or a local government-invested public corporation or a local government public corporation under the Local Public Enterprises Act (hereinafter referred to as "public institution, etc.");

2. Deleted. <May 28, 2014>

(2) Deleted. <May 28, 2014>

(3) The Government shall prepare a policy to develop a safer and more reliable system to verify identity of users under paragraph (1).

(4) A public institution, etc. may have its liability for damages caused by fraudulent use of a user's identity by a third party mitigated or discharged, if it has taken the measures for identity verification under paragraph (1) with care as a good manager. <Amended on May 28, 2014>

[This Article Wholly Amended on Jun. 13, 2008]

[Paragraph (1) 2 of this Article was deleted by Act No. 12681 on May 28, 2014, following the decision of unconstitutionality by the Constitutional Court made on 23.8.2012].

Article 44-6 (Claim to Furnish User's Information) (1) A person who alleges that information published or circulated by a specific user has intruded on his or her privacy, defamed him

or her, or violated his or her rights, may file a claim with the defamation dispute conciliation division under Article 44-10 to demand the relevant provider of information and communications services to furnish the information he or she possesses about the alleged offender (referring to the minimum information prescribed by Presidential Decree, including the name and address, necessary for filing a civil or criminal complaint), along with materials supporting his or her allegation of the violation, in order to file a civil or criminal complaint against the alleged offender.

(2) Upon receipt of a claim under paragraph (1), the defamation dispute conciliation division shall make a decision on whether to furnish information, hearing the opinion of the relevant user, unless it is impossible to contact the relevant user or there is any particular reason otherwise.

(3) A person who receives information about the relevant user under paragraph (1) shall not use the information for any purpose other than the purpose of filing a civil or criminal complaint.

(4) Other necessary matters regarding the content of a claim to furnish information of a user and the procedures therefor shall be prescribed by Presidential Decree.

[This Article Wholly Amended on Jun. 13, 2008]

Article 44-7 (Prohibition on Circulation of Unlawful Information) (1) No one may circulate any of the following information through an information and communications network:

<Amended on Sep. 15, 2011; Mar. 22, 2016; Jun. 12, 2018>

1. Information with obscene content distributed, sold, rented, or displayed openly in the form of code, words, sound, images, or motion picture;
2. Information with content that defames other persons by divulging a fact or false information, openly and with intent to disparage the person's reputation;
3. Information with content that arouses fear or apprehension by reaching other persons repeatedly in the form of code, words, sound, image, or motion picture;
4. Information with content that compromises, destroys, alters, or forges an information and communications system, data, a program, or similar or that interferes with the operation of such system, data, program, or similar without good cause;
5. Information with content that amounts to a media product harmful to youths under the Youth Protection Act and that is provided for profit without fulfilling the duties and

obligations under the relevant statutes and regulations, including the duty to verify the subject's age and the duty of labeling;

6. Information with content that amounts to speculative activities prohibited by statutes and regulations;

6-2. Information with content of transactions of personal information in violation of this Act or any other statute or regulation regarding the protection of personal information;

6-3. Information regarding methods, drawings, etc. for manufacturing guns or explosives (including things with a yield that may expose people to risk of life or bodily injury);

7. Information with content that divulges a secret classified under statutes and regulations or any other State secret;

8. Information with content that violates the National Security Act;

9. Other information with content that attempts to commit, aids, or abets a crime.

(2) The Korea Communications Commission may order a provider of information and communications services or a manager or an operator of a message board to reject, suspend, or restrict management of information under paragraph (1) 1 through 6, 6-2 and 6-3, subject to deliberation by the Communications Standards Commission: Provided, That if the information falls under paragraph (1) 2 or 3, the Commission shall not issue an order to reject, suspend, or restrict such management against the intention specifically manifested by the victim of the relevant information. <Amended on Mar. 22, 2016; Jun. 12, 2018>

(3) The Korea Communications Commission shall order a provider of information and communications services or a manager or an operator of a message board to reject, suspend, or restrict management of information under paragraph (1) 7 through 9, if the information falls under all of the following: <Amended on Mar. 22, 2016; Dec. 24, 2018>

1. A request was made by the head of a related central administrative agency [including requests from the head of an investigative agency for photos or videos or copies thereof (including copies of such copies) under Article 14 of the Act on Special Cases concerning the Punishment of Sexual Crimes out of the information referred to in paragraph (1) 9];

2. A demand for correction was made pursuant to subparagraph 4 of Article 21 of the Act on the Establishment and Operation of Korea Communications Commission after deliberation by the Communications Standards Commission within seven days from the

date the request under subparagraph 1 had been received;

3. The provider of information and communications services or the manager or operator of the message board has not complied with the demand for correction.

(4) The Korea Communications Commission shall provide an opportunity to the provider of information and communications services or the manager, operator, or relevant user of the message board to whom an order is to be issued pursuant to paragraph (2) or (3) to present his or her opinion in advance: Provided, That the Commission need not provide an opportunity to present an opinion in any of the following cases:

1. Where it is necessary to make an urgent disposition for public safety or welfare;
2. Where there is a ground prescribed by Presidential Decree to believe that it is obviously impracticable or evidently unnecessary to hear an opinion;
3. Where a person concerned clearly manifests his or her intent to give up the opportunity to present his or her opinion.

(5) An information and communication service provider that installs and operates a domestic server for temporary storage of data and meets the criteria prescribed by the Presidential Decree for the type and scale of business shall take the following technical and administrative measures to prevent the distribution of information falling under the subparagraphs of paragraph (1): <Newly Inserted on Jan. 23, 2024>

1. Measures to identify whether the information described in each of the subparagraphs of paragraph (1) is stored on the server and to promptly restrict access to it, subject to deliberation by the Communications Standards Commission in accordance with paragraphs 2 and 3;
2. Measures to request the person who posted the information identified under subparagraph 1 to prohibit the distribution of the relevant information;
3. Measures to have the actual status of the operation and management of the measures under subparagraph 1 recorded automatically in the system, and to keep it for the period prescribed by Presidential Decree;
4. Other measures prescribed by Presidential Decree as necessary to prevent the distribution of information falling under the subparagraphs of paragraph (1);

[This Article Wholly Amended on Jun. 13, 2008]

Articles 44-8 (Protection of Children in Interactive Information and Communications Services) When a provider of information and communications services provides children under 14 years of age with information and communications services based on a system that processes information by engaging in a conversation with a human user through text messages or voice chat, it shall endeavor not to provide information containing inappropriate content to such children.

[This Article Newly Inserted on Dec. 24, 2018]

Article 44-9 (Persons Responsible for Preventing Circulation of Illegally Filmed Materials or

the like) (1) A provider of information and communications services who meets the criteria prescribed by Presidential Decree, such as the average number of daily users, sales, and types of business, shall designate a person (hereinafter referred to as a "person responsible for preventing the circulation of illegally filmed materials or the like") responsible for preventing the circulation of the following information (hereinafter referred to as "illegally filmed materials or the like") available to the public through the information and communications network the provider operates or manages:

1. A photograph or video or copies thereof (including copies of such copies) Article 14 of the Act on Special Cases concerning the Punishment of Sexual Crimes;
2. Compiled content, composited content, fictitious content, or copies thereof (including copies of such copy) under Article 14-2 of the Act on Special Cases concerning the Punishment of Sexual Crimes;
3. Child or youth sexual exploitation materials defined in subparagraph 5 of Article 2 of the Act on the Protection of Children and Youth against Sex Offenses.

(2) Persons responsible for preventing the circulation of illegally filmed materials or the like shall take measures necessary to prevent the circulation thereof, such as deleting them and blocking access thereto, pursuant to Article 22-5 (1) of Telecommunications Business Act.

(3) Necessary matters regarding the number of persons responsible for preventing the circulation of illegally filmed materials or the like, qualification requirements, training, and other matters shall be prescribed by Presidential Decree.

[This Article Newly Inserted on Jun. 9, 2020]

Article 44-10 (Defamation Dispute Conciliation Division) (1) The Communications Standards Commission shall have the defamation dispute conciliation division comprised of five members or fewer for efficient conciliation of disputes arising in connection with information that intrudes other persons' privacy, defames other persons, or violates other persons' rights, including a member or more holding the qualification of attorney-at-law.
<Amended on Jun. 9, 2020>

(2) The members of the defamation dispute conciliation division shall be commissioned by the chairperson of the Communications Standards Commission with consent of the Communications Standards Commission.

(3) Articles 33-2 (2) and 35 through 39 shall apply mutatis mutandis to the procedures for conciliation of disputes by the defamation dispute conciliation division. In such cases, "Dispute Mediation Committee" shall be construed as "Communications Standards Commission", and "disputes over personal information" as "disputes arising in connection with information that intrudes other persons' privacy, defames other persons, or violates other persons' rights among information circulated through information and communications networks".

(4) Matters necessary for the installation and operation of the defamation dispute conciliation division and the conciliation of disputes, and other related matters shall be prescribed by Presidential Decree.

[This Article Wholly Amended on Jun. 13, 2008]

CHAPTER VI SECURING OF STABILITY OF INFORMATION AND COMMUNICATIONS NETWORKS

Article 45 (Securing of Stability of Information and Communications Networks) (1) Any of the following persons shall take protective measures to secure the reliability of the information and ensure the stability of the information and communications networks used to provide information and communications services: <Amended on Jun. 9, 2020>

1. A provider of information and communications services;
2. A person who manufactures or imports devices, equipment, and facilities prescribed by Presidential Decree, among devices, equipment, and facilities which can transmit or receive information by being connected to an information and communications network

(hereinafter referred to as "devices and the like connected to an information and communications network").

(2) The Minister of Science and ICT may determine and give public notice of guidelines for protective measures for information (hereinafter referred to as "information protection guidelines"), specifying details of the protective measures under paragraph (1) and may recommend any of the persons falling under paragraph (1) to observe the guidelines. <Amended on Feb. 17, 2012; Mar. 23, 2013; Jul. 26, 2017; Jun. 9, 2020>

(3) The information protection guidelines shall contain descriptions of the following: <Amended on Mar. 22, 2016; Jun. 9, 2020>

1. Technical and physical protective measures, including installation and operation of an information security system, to prevent or counteract access to or invasion upon an information and communications network by a person with no due authorization;
2. Technical protective measures for preventing unlawful leakage, forgery, alteration, or deletion of information;
3. Technical and physical protective measures for securing the state of enabling continuous use of information and communications networks;
4. Administrative protective measures for stabilization of information and communications networks and protection of information, including securing human resources, organization, and expenses and establishing related plans;
5. Technical protective measures for information security of devices and the like connected to an information and communications network.

(4) The Minister of Science and ICT may request the heads of relevant central administrative agencies to reflect the content of the information security guidelines in standards for testing, inspection, certification, etc. related to devices and the like connected to information and communications networks with regard to the substantive areas under their jurisdictions. <Newly Inserted on Jun. 9, 2020>

[This Article Wholly Amended on Jun. 13, 2008]

Article 45-2 (Preliminary Examination on Information Protection) (1) If a provider of information and communications services intends to newly establish an information and communications network or to provide information and communications services, he or she shall take the matters regarding information protection into account in planning or

designing thereof.

(2) The Minister of Science and ICT may recommend a person who intends to operate the information and communications services or the telecommunications business falling under any of the following to take protective measures in accordance with the preliminary examination standards for information protection as prescribed by Presidential Decree: <Amended on Mar. 23, 2013; Jul. 26, 2017>

1. The information and communications services or telecommunications business prescribed by Presidential Decree, for which authorization or permission by the Minister of Science and ICT should be obtained or registration with or report to the Korea Communications Commission should be made pursuant to this Act or other statutes or regulations;
2. The information and communications services or telecommunications business prescribed by Presidential Decree and fully or partially financed by the Minister of Science and ICT for the business expenses thereof.

(3) Standards, methods, procedures, fees for the preliminary examination on information protection pursuant to paragraph (2) and other necessary matters shall be prescribed by Presidential Decree.

[This Article Newly Inserted on Feb. 17, 2012]

Article 45-3 (Designation of Chief Information Security Officers) (1) A provider of information and communications services shall designate an executive officer or employee meeting the standards prescribed by Presidential Decree as a chief information security officer and shall file a report thereon to the Minister of Science and ICT, in order to ensure the security of information and communications systems, etc. and safe management of information: Provided, That a provider of information and communications services whose total assets, turnover, and the like meet the criteria prescribed by Presidential Decree need not file a report on such chief information security officer. <Amended on May 28, 2014; Jul. 26, 2017; Jun. 12, 2018; Jun. 8, 2021>

(2) Methods and procedures for reporting under paragraph (1) and other matters shall be prescribed by Presidential Decree. <Newly Inserted on May 28, 2014>

(3) No chief information security officer designated and reported under the main clause of paragraph (1) (limited to where a provider of information and communications services

whose total assets, turnover, and the like meet the criteria prescribed by Presidential Decree) may hold another office concurrently, other than perform duties referred to in paragraph (4). <Newly Inserted on Jun. 12, 2018>

(4) A chief information security officer shall perform the following duties: <Amended on Jun. 8 2021>

1. The chief information security officer shall be responsible for the following duties:
 - (a) To formulate, implement, and improve information protection plans;
 - (b) To conduct regular audit and improve the actual conditions and practices of information protection;
 - (c) To identify and evaluate risks relating to information protection and develop countermeasures for information protection;
 - (d) To formulate and implement plans for information protection education and simulation training;
2. The chief information security officer may hold another office concurrently to perform the following:
 - (a) Duties of providing information security disclosure under Article 13 of the Act on the Promotion of Information Security Industry;
 - (b) Duties of chief information security officers under Article 5 (5) of the Act on the Protection of Information and Communications Infrastructure;
 - (c) Duties of chief information security officers under Article 21-2 (4) of the Electronic Financial Transactions Act;
 - (d) Duties of privacy officers under Article 31 (2) of the Personal Information Protection Act;
 - (e) Taking other measure necessary for information protection in accordance with this Act or any other relevant statute or regulation.
- (5) A provider of information and communications services may establish and operate a council of chief information security officers comprised of chief information security officers prescribed in paragraph (1) in order to jointly prevent and respond to a computer security incident, share necessary information, and implement other joint programs prescribed by Presidential Decree. <Amended on May 28, 2014; Jun. 12, 2018>

(6) The Government may fully or partially provide support to the Council of Information Security Officers under paragraph (5) for expenses incurred in conducting its activities. <Amended on May 28, 2014; Jun. 22, 2015; Jun. 12, 2018>

(7) Necessary matters regarding qualifications, etc. of chief information security officers shall be prescribed by Presidential Decree. <Newly Inserted on Jun. 12, 2018>
[This Article Newly Inserted on Feb. 17, 2012]

Article 46 (Protection of Data Centers) (1) Among the following information and communications service providers who meet the standards prescribed by Presidential Decree in terms of the scale, etc. of information and communications facilities (hereinafter referred to as "data center operator, etc.") shall take protective measures, as prescribed by Presidential Decree, in order to operate information and communications facilities in a stable manner: <Amended on Jun. 9, 2020; Jan. 3, 2023>

1. A person who operates and manages clustered information and communications facilities to provide information and communications services for others (hereinafter referred to as "data center operator");

2. A person who operates and manages an information and communications facility directly clustered to provide his or her own information and communications services.

(2) Every data center operator shall purchase insurance policies as prescribed by Presidential Decree to cover damages that may be caused by destruction or damage of the data center or any other trouble in operation.

(3) The Minister of Science and ICT may regularly inspect whether protective measures under paragraph (1) have been implemented and may order a data center operator, etc. to take corrective measures with respect to matters requiring supplementation: Provided, That in cases of matters for which inspection under Article 36-2 (2) of the Framework Act on Broadcasting Communications Development has been conducted with respect to a data center operator, such matters shall be excluded from the inspection on whether protective measures under paragraph (1) have been implemented. <Newly Inserted on Jan. 3, 2023>

(4) The Minister of Science and ICT may request providers of information and communications services falling under any subparagraph of paragraph (1), the heads of relevant central administrative agencies, the heads of local governments, and the heads of institutions designated as public institutions pursuant to Article 4 of the Act on the

Management of Public Institutions to submit materials in order to verify whether they fall under the category of data center operators and to conduct an inspection under paragraph (3). Upon receipt of a request for submission of materials in such cases, a person in receipt of such request shall comply therewith, in the absence of good cause, and Article 64 (6) and (9) through (11) shall apply mutatis mutandis to the procedures, methods, etc. for requesting submission of materials. <Newly Inserted on Jan. 3, 2023>

(5) Article 64-2 shall apply mutatis mutandis to the protection and destruction of materials submitted pursuant to paragraph (4). <Newly Inserted on Jan. 3, 2023>

(6) Where the provision of information and communications services has been suspended during the period prescribed by Presidential Decree due to a disaster, calamity, or other physical or functional defects, a data center operator shall report to the Minister of Science and ICT without delay the current status of suspension, causes of such suspension, emergency measures, and recovery measures. In such cases, the Minister of Science and ICT may provide technical support necessary for the recovery and protection of clustered information and communications facilities. <Newly Inserted on Jan. 3, 2023>

(7) A provider of information and communications services who has leased a clustered information and communications facility provided by a data center operator shall actively cooperate with the data center operator in implementing protective measures under paragraph (1), and where the data center operator installs and operates facilities necessary for protective measures under paragraph (1) or exclusively operates and manages rental facilities, such as directly installing and operating facilities necessary for protective measures under paragraph (1) or controlling access to such facilities, he or she shall take measures, such as reporting, etc. when he or she implements protective measures or suspends services due to a disaster, etc., as prescribed by Presidential Decree. <Newly Inserted on Jan. 3, 2023>

(8) The Minister of Science and ICT may entrust affairs regarding the inspection under paragraph (3) and technical support under paragraph (6) to a specialized institution prescribed by Presidential Decree. <Newly Inserted on Jan. 3, 2023>

(9) The frequency and method of inspection under paragraph (3), the method of reporting under paragraph (6), and other necessary matters shall be prescribed by Presidential Decree. <Newly Inserted on Jan. 3, 2023>

[This Article Wholly Amended on Jun. 13, 2008]

Article 46-2 (Emergency Countermeasures of Data Center Operators) (1) In any of the following cases, a data center operator may fully or partially suspend rendering relevant services, as stipulated in the terms and conditions: <Amended on Apr. 22, 2009; Mar. 23, 2013; Jul. 26, 2017>

1. If it is anticipated that an abnormality found in the information system of a person who uses the data center (hereinafter referred to as "user of a data center") will probably cause a serious trouble to the information and communications networks of other users of the data center or of the data center;
2. If it is anticipated that an external computer security incident will probably cause serious trouble to the data center;
3. If there occurs a serious computer security incident and the Minister of Science and ICT or the Korea Internet and Security Agency requests the suspension of the services.

(2) When a data center operator suspends his or her services in accordance with paragraph (1), he or she immediately notify users of the data center the suspension of services, specifically stating the reasons for the suspension, the date, time, period, and details of the suspension, and other related matters.

(3) Once the event that caused suspension of services terminates, a data center operator shall resume his or her services immediately.

[This Article Wholly Amended on Jun. 13, 2008]

Article 46-3 Deleted. <Feb. 17, 2012>

Article 47 (Certification of Information Security Management Systems) (1) With respect to a person who establishes and operates a comprehensive management system, including administrative, technical, and physical protective measures, for ensuring stability and reliability of an information and communications network (hereinafter referred to as "information security management system"), the Minister of Science and ICT may certify as to whether such person meets the standards under paragraph (4). <Amended on Feb. 17, 2012; Mar. 23, 2013; Dec. 1, 2015; Jul. 26, 2017>

(2) A telecommunication business entity under subparagraph 8 of Article 2 of the Telecommunications Business Act, or any of the following persons who provides or

intermediates the provision of information by using telecommunications services of any telecommunication business entity, shall receive the certification under paragraph (1): <Newly Inserted on Feb. 17, 2012; Dec. 1, 2015; Dec. 24, 2018; Jun. 9, 2020; Jan. 23, 2024>

1. A person who renders information and communications services, as prescribed by Presidential Decree, as a person registered pursuant to Article 6 (1) of the Telecommunications Business Act (hereinafter referred to as a "major provider of information and communications services");

2. A data center operator;

3. A person meeting the standards prescribed by Presidential Decree, whose sales, tax revenue, or any similar for the previous year is at least 150 billion won, whose sales in the information and communications service sector for the previous year is at least 10 billion won, or whose average daily users for the previous year is at least one million.

(3) Where a person required to be certified in accordance with paragraph (2) is certified for conformity with international standards for information protection or takes measures for information protection, as prescribed by Ordinance of the Ministry of Science and ICT, the Minister of Science and ICT may omit part of certification examination under paragraph (1). In such cases, the detailed scope of omitted certification examination shall be determined and publicly notified by the Minister of Science and ICT. <Newly Inserted on Dec. 1, 2015; Jul. 26, 2017>

(4) For the purpose of certification of an information security management system under paragraph (1), the Minister of Science and ICT may determine and give public notice of other necessary matters, such as certification standards specifying countermeasures for administrative, technical, and physical protection. <Amended on Feb. 17, 2012; Mar. 23, 2013; Dec. 1, 2015; Jul. 26, 2017>

(5) The period of validity of the certification of an information security management system under paragraph (1) shall be three years: Provided, That upon receipt of any rating for information security management in accordance with Article 47-5 (1), the certification under paragraph (1) shall be deemed effective during the period of validity of such rating. <Newly Inserted on Feb. 17, 2012; Dec. 1, 2015>

(6) The Minister of Science and ICT may have the Korea Internet and Security Agency or any institution designated by the Minister of Science and ICT (hereinafter referred to as

"certification body for information security management systems") perform the following affairs related to the certification under paragraphs (1) and (2): <Newly Inserted on Feb. 17, 2012; Mar. 23. 2013; Dec. 1, 2015; Jul. 26, 2017>

1. Examination to verify whether the information security management system established by an applicant for certification meets the certification standards under paragraph (4) (hereinafter referred to as "examination for certification");
2. Review on the results of examination for certification;
3. Issuance and management of written certifications;
4. Ex post facto management of granted certifications;
5. Fosterage and qualification management of the certification examiners of information security management systems;
6. Other affairs regarding the certification of information security management systems.

(7) If necessary for the efficient conduct of affairs related to certification, the Minister of Science and ICT may designate an institution that performs affairs related to examination for certification (hereinafter referred to as "examination institution for information security management systems"). <Newly Inserted on Dec. 1, 2015; Jul. 26, 2017>

(8) The Korea Internet and Security Agency, a certification body for information security management systems, and an examination institution for information security management systems shall, in order to enhance the efficiency of information security management systems, perform ex post facto management at least once a year and notify the Minister of Science and ICT of the results thereof. <Newly Inserted on Feb. 17, 2012; Mar. 23. 2013; Dec. 1, 2015; Jul. 26, 2017>

(9) A person who has received the certification of an information security management system in accordance with paragraphs (1) and (2) may indicate or publicize the content of the certification, as prescribed by Presidential Decree. <Amended on Feb. 17, 2012; Dec. 1, 2015>

(10) The Minister of Science and ICT may revoke the certification where any of the following grounds is found: Provided, That in cases falling under subparagraph 1, the Minister of Science and ICT shall revoke the certification: <Newly Inserted on Feb. 17, 2012; Mar. 23. 2013; Dec. 1, 2015; Jul. 26, 2017>

1. Having received the certification of an information security management system by fraud or other improper means;
2. Falling short of the certification standards under paragraph (4);
3. Refusing or obstructing the ex post facto management under paragraph (8).

(11) Methods and procedures for, and scope and fees of, certification under paragraphs (1) and (2), methods and procedures for ex post facto management under paragraph (8), methods and procedures for revoking certification under paragraph (10), and other necessary matters shall be prescribed by Presidential Decree. <Amended on Feb. 17, 2012; Dec. 1, 2015>

(12) Standards and procedures for, and period of validity of, the designation of a certification body for information security management systems and an examination institution for information security management systems, and other necessary matters shall be prescribed by Presidential Decree. <Amended on Feb. 17, 2012; Dec. 1, 2015>

[This Article Wholly Amended on Jun. 13, 2008]

Article 47-2 (Revocation of Designation of Certification Body or Examination Institution for Information Security Management Systems)

(1) If a corporation or organization designated as a certification body or an examination institution for information security management systems pursuant to Article 47 falls under any of the following cases, the Minister of Science and ICT may revoke the designation or order it to fully or partially suspend the relevant business for a prescribed period not exceeding one year: Provided, That in cases falling under subparagraph 1 or 2, the Minister of Science and ICT shall revoke the designation: <Amended on Feb. 17, 2012; Mar. 23, 2013; Dec. 1, 2015; Jul. 26, 2017>

1. Where it has obtained the designation of a certification body or an examination institution for information security management systems by fraud or other improper means;
2. Where it has performed certification or examination for certification during a business suspension period;
3. Where it has not performed certification or examination for certification without good cause;
4. Where it has performed certification or examination for certification, in violation of Article 47 (11);

5. Where it no longer meets the standards for designation under Article 47 (12).

(2) Matters necessary for the revocation of designation and suspension of business under paragraph (1) and other related matters shall be prescribed by Presidential Decree.

[This Article Wholly Amended on Jun. 13, 2008]

[Title Amended on Dec. 1, 2015]

Article 47-3 Deleted. <Feb. 4, 2020>

Article 47-4 (Protection of User Information) (1) The Government may prescribe guidelines necessary for protection of information of users to recommend users to observe the guidelines and may take measures necessary for preventing computer security incidents and precluding spread thereof, such as inspection of vulnerabilities and technical support.

(2) The Government may entrust affairs regarding measures taken under paragraph (1) to the Korea Internet and Security Agency or a specialized institution prescribed by Presidential Decree. <Newly Inserted on Jun. 9, 2020>

(3) If a major provider of information and communications services foresees that a serious problem is likely to occur in the information system of a user who uses the services, the information and communications network, or similar provided by such provider because of an occurrence of a serious computer security incident on the information and communications network, the provider may request the user to take necessary protective measures as stipulated by the terms and conditions and may place a temporary restriction on access to the relevant information and communications network if the user does not perform as requested. <Amended on Jun. 9, 2020>

(4) When a software business entity defined in Article 2 of the Software Promotion Act has produced a program that can address security vulnerabilities, he or she shall notify the Korea Internet and Security Agency of such production and shall notify users of the software of the production at least twice within one month from the date of production. <Amended on Apr. 22, 2009; Jun. 9, 2020>

(5) Specific details that shall be stipulated by the terms and conditions with respect to the request for protective measures under paragraph (3) and other related matters shall be prescribed by Presidential Decree. <Amended on Jun. 9, 2020>

[This Article Wholly Amended on Jun. 13, 2008]

[This Article Moved from Article 47-3 <Feb. 17, 2012>]

Article 47-5 (Assignment of Rating for Information Security Management) (1) A person who has obtained the certification of an information security management system pursuant to Article 47 is entitled to receive a rating for information security management from the Minister of Science and ICT in order to enhance the level of a corporate's management of its comprehensive information security and to secure users' reliability on information security services. <Amended on Mar. 23, 2013; Jul. 26, 2017>

(2) The Minister of Science and ICT may authorize the Korea Internet and Security Agency to perform the affairs of assigning ratings under paragraph (1). <Amended on Mar. 23, 2013; Jul. 26, 2017>

(3) A person who has obtained a rating for information security management pursuant to paragraph (1) may indicate the obtained rating or advertise the details of such rating as prescribed by Presidential Decree.

(4) Where the Minister of Science and ICT finds any of the following cases, he or she may revoke the granted rating: Provided, That in the cases falling under subparagraph 1, the Minister of Science and ICT shall revoke the granted rating: <Amended on Mar. 23, 2013; Dec. 1, 2015; Jul. 26, 2017>

1. Where a person has obtained a rating for information security management by fraud or other improper means;

2. Where a person falls short of the standards for rating pursuant to paragraph (5).

(5) Standards for review in assigning ratings pursuant to paragraph (1); the methods and procedures for and fees of assigning ratings; the effective term of ratings; the methods and procedures for revocation of ratings pursuant to paragraph (4); and other necessary matters shall be prescribed by Presidential Decree.

[This Article Newly Inserted on Feb. 17, 2012]

Article 47-6 (Giving Monetary Award to Person Reporting Information Security Vulnerability)

(1) The Government may pay a monetary award, within the budget, to a person who has reported any information security vulnerability relating to information communications services, devices and the like connected to information and communications networks, or

software (hereinafter referred to as "information security vulnerability") to prevent computer security incidents and stop damage from spreading.

(2) Persons eligible for monetary awards under paragraph (1), the standards and procedures for the payment of such monetary awards, and other relevant matters shall be prescribed by Presidential Decree.

(3) The Government may entrust affairs regarding the payment of monetary awards under paragraph (1) to the Korea Internet and Security Agency.

[This Article Newly Inserted on Jun. 10, 2022]

Article 47-7 (Special Cases concerning Certification of Information Security Management

System) (1) The Minister of Science and ICT may relax and apply the certification standards and procedures pursuant to Article 47 (1) and (2) to persons who fall under any of the following subparagraphs among persons seeking certification pursuant to Article 47 (1) and (2):

1. A small enterprise under Article 2 (2) of the Framework Act on Small and Medium Enterprises;
2. Any other person who meets the criteria prescribed by the Presidential Decree according to the scale and characteristics of information and communication services.

(2) The Minister of Science and ICT may provide necessary support, including costs and technology related to paragraph (1), to ensure the stability and reliability of the information and communication network.

(3) The Minister of Science and ICT may determine and publicly notify the certification standards and procedures under paragraph (1) and other necessary matters.

[This Article Newly Inserted on Jan. 23, 2024]

Article 48 (Prohibition on Intrusive Acts on Information and Communications Networks) (1)

No one shall intrude on an information and communications network without a rightful authority for access or beyond a permitted authority for access.

(2) No one shall mutilate, destroy, alter, or forge an information and communications system, data, program, or similar without good cause, nor shall he or she convey or spread a program that is likely to interrupt operation of such system, data, program, or similar (hereinafter referred to as "malicious program").

(3) No one shall cause a trouble to an information and communications network to interfere with stable operation of the information and communications network by sending a large amount of signals or data, letting the network process an illegitimate order, or doing the similar actions.

(b) No person shall install a program or technical device that enables access to the information and communication network bypassing the normal protection and authentication procedures of the information and communication network without good cause on the information and communication network or the information system related to the information and communication network, or deliver or distribute it.

<Newly Inserted on Jan. 23, 2024>

[This Article Wholly Amended on Jun. 13, 2008]

Article 48-2 (Countermeasures against Computer Security Incidents) (1) The Minister of Science and ICT shall perform the following business affairs to take proper countermeasures against computer security incidents and may have the Korea Internet and Security Agency fully or partially perform the business affairs, if necessary to do so:

<Amended on Apr. 22, 2009; Mar. 23, 2013; Jul. 26, 2017>

1. Collection and spread of information about computer security incidents;
2. Precaution and warning of computer security incidents;
3. Emergency measures against computer security incidents;
4. Other countermeasures against computer security incidents prescribed by Presidential Decree.

(2) Any of the following persons shall furnish the Minister of Science and ICT or the Korea Internet and Security Agency with the information related to computer security incidents, including statistics by type of computer security incidents, statistics of traffic of the relevant information and communications network, and statistics of use by access channel, as prescribed by Presidential Decree: <Amended on Apr. 22, 2009; Mar. 23, 2013; Jul. 26, 2017>

1. A major provider of information and communications services;
2. A data center operator;
3. Other persons prescribed by Presidential Decree from among those who operate an information and communications network.

(3) The Korea Internet and Security Agency shall analyze the information under paragraph (2) and report it to the Minister of Science and ICT. <Amended on Apr. 22, 2009; Mar. 23, 2013; Jul. 26, 2017; Jul. 26, 2017>

(4) If a business entity obligated to furnish the information in accordance with paragraph (2) refuses to do so without good cause or furnishes false information, the Minister of Science and ICT may order the business entity to make a correction within a reasonable period. <Amended on Mar. 23, 2013; Jul. 26, 2017>

(5) The Minister of Science and ICT or the Korea Internet and Security Agency shall use the information furnished in accordance with paragraph (2) properly within the extent necessary for taking countermeasures against a computer security incident. <Amended on Apr. 22, 2009; Mar. 23, 2013; Jul. 26, 2017>

(6) If necessary to take countermeasures against a computer security incident, the Minister of Science and ICT or the Korea Internet and Security Agency may request a person falling under any subparagraph of paragraph (2) to provide human resources for assistance. <Amended on Apr. 22, 2009; Mar. 23, 2013; Jul. 26, 2017>

[This Article Wholly Amended on Jun. 13, 2008]

Article 48-3 (Report on Computer Security Incidents) (1) If a computer security incident occurs, a provider of information and communications services shall immediately report it to the Minister of Science and ICT or the Korea Internet and Security Agency; in such cases, if a provider of information and communications services has already notified or reported a computer security incident in accordance with another statute, such report mandated under the former part shall be deemed to have been made: <Amended on Apr. 22, 2009; Mar. 23, 2013; Jul. 26, 2017; Jun. 10, 2022>

1. Deleted; <Jun. 10, 2022>

2. Deleted. <Jun. 10, 2022>

(2) Upon receipt of a report on a computer security incident under paragraph (1) or becoming aware of a computer security incident, the Minister of Science and ICT or the Korea Internet and Security Agency shall take necessary measures under the subparagraphs of Article 48-2 (1). <Amended on Apr. 22, 2009; Mar. 23, 2013; Jul. 26, 2017>

(3) Upon receipt of a notice of or report on a computer security incident under the latter part of paragraph (1), the head of a related agency shall share relevant information with the Minister of Science and ICT or the Korea Internet and Security Agency without delay.

<Newly Inserted on Jun. 10, 2022>

[This Article Wholly Amended on Jun. 13, 2008]

Article 48-4 (Analysis of Causes of Computer Security Incidents) (1) If a computer security incident occurs, a person who operates an information and communications network, including a provider of information and communications services, shall analyze the causes of the computer security incident; respond thereto, based on the results of analysis, for stopping damage from spreading; and take measures necessary to recover from the damage and prevent a recurrence of such computer security incident. <Amended on Jun. 10, 2022>

(2) If a computer security incident occurs in an information and communications network operated by a provider of information and communications services, the Minister of Science and ICT may analyze the causes of the computer security incident and develop countermeasures to stop damage from spreading, to respond to such incident, to recover from damage, and to prevent a recurrence of such incident; and may recommend the provider of information and communications services to take necessary measures. <Newly Inserted on Jun. 10, 2022>

(3) Where a serious computer security incident occurs in an information and communications network operated by a provider of information and communications services, the Minister of Science and ICT may organize a private-public joint investigation team having expertise in the protection of information and analyze the causes of such computer security incident if necessary for analyzing such causes and developing countermeasures pursuant to paragraph (2). <Amended on Mar. 23, 2013; Jul. 26, 2017; Jun. 10, 2022>

(4) If deemed necessary for analyzing the causes of a computer security incident and developing countermeasures pursuant to paragraph (2), the Minister of Science and ICT may order the relevant provider of information and communications services to preserve relevant data, such as records on access to the relevant information and communications network. <Amended on Mar. 23, 2013; Jul. 26, 2017; Jun. 10, 2022>

(5) The Minister of Science and ICT may demand a provider of information and communications services to submit data related to a computer security incident, if deemed necessary for analyzing the causes of such computer security incident and developing countermeasures pursuant to paragraph (2); and in the case of a serious computer security incident, the Minister may require public officials under his or her jurisdiction or a private-public joint investigation team under paragraph (3) to enter the place of business of the relevant person and to investigate the causes of the incident: Provided, That data corresponding to the communication confirmation data defined in subparagraph 11 of Article 2 of the Protection of Communications Secrets Act shall be submitted in the manner prescribed by that Act. <Amended on Mar. 23, 2013; Jul. 26, 2017; Jun. 10, 2022>

(6) The Minister of Science and ICT or the private-public joint investigation team shall not use the information learned through the data submitted and the investigation conducted in accordance with paragraph (5) for any purpose other than the analysis of the causes of the computer security incident and development of countermeasures and shall destroy it immediately after the analysis of the causes is completed. <Amended on Mar. 23, 2013; Jul. 26, 2017; Jun. 10, 2022>

(7) Matters necessary for the organization and operation of a private-public joint investigation team under paragraph (3), the protection of data submitted pursuant to paragraph (5), the methods and procedures for investigation thereunder, etc. shall be prescribed by Presidential Decree. <Amended on Jun. 10, 2022>

[This Article Wholly Amended on Jun. 13, 2008]

Article 48-5 (Countermeasures against Computer Security Incidents Related to Devices and

the like Connected to Information and Communications Networks) (1) Where a computer security incident related to devices and the like connected to an information and communications network occurs, the Minister of Science and ICT may analyze the cause of the relevant computer security incident in cooperation with the heads of relevant central administrative agencies.

(2) Where there occurs a computer security incident related to devices and the like connected to an information and communications network, which is likely to cause any danger to the lives, bodies, or property of citizens, the Minister of Science and ICT may request the heads of relevant central administrative agencies to take the following

measures:

1. Measures, such as the inspection of vulnerabilities and technical support under Article 47-4 (1);
2. Measures necessary for precluding the spread of damage;
3. Improvement of other systems for the information security of devices and the like connected to an information and communications network.

(3) Where there occurs a computer security incident related to devices and the like connected to an information and communications network, the Minister of Science and ICT may recommend a person who manufactures or imports the relevant devices and the like connected to an information and communications network to take measures, such as improving vulnerabilities thereof, for preventing an expansion or recurrence of the computer security incident.

(4) The Minister of Science and ICT may subsidize a specialized institution prescribed by Presidential Decree for expenses incurred in conducting the following business activities:

1. Research to formulate guidelines for information security related to devices and the like connected to information and communications networks;
2. Research for improving standards for testing, inspection, authentication, etc. related to devices or the like connected to information and communications networks.

[This Article Newly Inserted on Jun. 9, 2020]

Article 48-6 (Certification of Devices and the like Connected to Information and Communications Networks)

(1) Where devices and the like connected to an information and communications network meet the certification standards under paragraph (2) as a result of an examination conducted by a testing agency for certification under paragraph (4), the Minister of Science and ICT may grant information security certification.

(2) The Minister of Science and ICT may determine and publicly notify certification standards for ensuring the stability of information and communications networks and securing the reliability of information, with regard to the information security certification under paragraph (1) (hereinafter referred to as "information security certification").

(3) Where a person who has obtained information security certification falls under any of the following subparagraphs, the Minister of Science and ICT may revoke such certification: Provided, That in cases falling under subparagraph 1, such certification shall be revoked:

1. Where he or she has obtained information security certification by fraud or other improper means;
 2. Where he or she fails to meet the certification standards provided for in paragraph (2).
- (4) In order to efficiently conduct tests verifying whether devices and the like connected to an information and communications network meet the certification standards referred to in paragraph (2), the Minister of Science and ICT may, if necessary, designate, as a testing agency for certification, an institution satisfying the designation standards prescribed by Presidential Decree.
- (5) Where a testing agency for certification designated pursuant to paragraph (4) (hereinafter referred to as a "testing agency for certification") falls under any of the following cases, the Minister of Science and ICT may revoke such designation: Provided, That in cases falling under subparagraph 1, such certification shall be revoked:
1. Where it has obtained the designation by fraud or other improper means;
 2. If it fails to meet the criteria for designation under paragraph (4).
- (6) The Minister of Science and ICT may entrust affairs related to information security certification and the revocation thereof to the Korea Internet and Security Agency.
- (7) Necessary matters regarding procedures, etc. for information security certification and cancellation of such certification and procedures, etc. for designation of testing agencies for certification and cancellation of such designation shall be prescribed by Presidential Decree.

[This Article Newly Inserted on Jun. 9, 2020]

Article 49 (Protection of Secrets) No one shall mutilate another person's information processed, stored, or transmitted through an information and communications network, nor shall he or she infringe, misappropriate, or divulge another person's secret.

[This Article Wholly Amended on Jun. 13, 2008]

Article 49-2 (Prohibition on Collection of Information by Deception) (1) No one shall collect another person's information or entice another person to furnish information through an information and communications network by deception.

(2) Whenever a provider of information and communications services discovers a violation of paragraph (1), he or she immediately report it to the Minister of Science and ICT or the

Korea Internet and Security Agency. <Amended on Apr. 22, 2009; Mar. 22, 2016; Jul. 26, 2017; Feb. 4, 2020>

(3) Upon receipt of a report under paragraph (2) or becoming aware of a violation of paragraph (1), the Minister of Science and ICT or the Korea Internet and Security Agency shall take the following measures as necessary: <Amended on Apr. 22, 2009; Mar. 22, 2016; Jul. 26, 2017; Feb. 4, 2020; Jun. 10, 2022>

1. Collection and diffusion of the information related to the violation;
2. Precaution and warning of similar damage;
3. Emergency measures for preventing damage and spread thereof, including requesting a provider of information and communications services to conduct all or some of the following:
 - (a) Blockage of access paths;
 - (b) Suspension of the provision of information and communications services for telephone numbers used for a violation described in paragraph (1);
 - (c) Notification to relevant users of the fact that they have been exposed to a violation described in paragraph (1).

(4) To take measures referred to in paragraph (3) 3, the Minister of Science and ICT may order providers of information and communications services to take necessary measures, such as sharing among themselves information regarding deception through information and communications networks. <Newly Inserted on Mar. 22, 2016; Jul. 26, 2017; Feb. 4, 2020>

(5) Upon receipt of a request made under paragraph (3) 3, a provider of information and communications services may take the relevant measures in the manner prescribed by relevant terms and conditions of use. <Newly Inserted on Jun. 10, 2022>

(6) Details to be stipulated by the terms and conditions of use under paragraph (5) shall be prescribed by Presidential Decree. <Newly Inserted on Jun. 10, 2022>

[This Article Wholly Amended on Jun. 13, 2008]

[Title Amended on Feb. 4, 2020]

Article 49-3 (Suspension of Provision of Telecommunications Services for Telephone Numbers Used as Means of Deception) (1) When a person prescribed by Presidential Decree, including the Commissioner General of the National Police Agency, the Prosecutor General,

and the Governor of the Financial Supervisory Service, has verified telephone numbers used as means of deception described in Article 49-2 (1), the person may request the Minister of Science and ICT to suspend the provision of telecommunications services for the relevant telephone numbers.

(2) A user whose telecommunication services have been suspended due to a request made paragraph (1) may file an objection with the agency that has requested the suspension.

(3) Matters necessary for procedures, etc. for filing an objection under paragraph (2) shall be prescribed by Presidential Decree.

[This Article Newly Inserted on Jun. 10, 2022]

Article 50 (Restrictions on Transmission of Advertising Information for Profit) (1) If any person intends to transmit advertising information for profit by using an electronic transmission medium, he or she shall obtain express prior consent from an addressee of such information: Provided, That he or she need not obtain prior consent in any of the following cases: <Amended on Mar. 22, 2016; Jun. 9, 2020>

1. Where a person who has directly collected contact details from the addressee in his or her dealings of goods, etc. intends to transmit advertising information for profit on the same kinds of goods, etc. as those he or she manages and has dealt with the addressee within a period prescribed by Presidential Decree;

2. Where a telemarketer under the Act on Door-to-Door Sales informs prospective customers of the collection source of their personal information by voice, and solicits them to buy products or services by means of a telephone call.

(2) Notwithstanding paragraph (1), where an addressee expresses his or her intention to refuse to receive information or revokes his or her prior consent, no person who intends to transmit advertising information for profit by using an electronic transmission medium shall transmit advertising information for profit.

(3) Notwithstanding paragraph (1), a person who intends to transmit advertising information for profit by using an electronic transmission medium during the time between 9:00 pm and 8:00 am of the following day shall obtain express prior consent from the addressee of such information: Provided, That the forgoing shall not apply to media prescribed by Presidential Decree.

(4) A person who transmits advertising information for profit by using an electronic transmission medium shall specify the following matters in advertising information, as prescribed by Presidential Decree:

1. The name and contact details of a sender;
2. Matters regarding measures and methods by which an addressee can readily express his or her intention to refuse to receive information or to revoke his or her consent to receive information.

(5) A person who transmits advertising information for profit by using an electronic transmission medium shall not engage in any of the following acts: <Amended on Jan. 23, 2024>

1. Act of evading or preventing addressees from opting out or withdrawing their consent to receive advertising information;
2. Act of automatically generating an addressee's contact information, such as a telephone number and e-mail address, using a combination of numbers, symbols, or letters;
3. Act of automatically registering a telephone number or e-mail address for the purpose of transmitting advertising information for profit;
4. Various acts to conceal the identity of the sender of advertising information or the source of the transmission of the advertisement;
5. Various acts to deceive an addressee into responding for the purpose of transmitting advertising information for profit.

(6) A person who transmits advertising information for profit by using an electronic transmission medium shall take necessary measures so that an addressee does not incur any cost, such as telephone charges, when the addressee refuses to receive or revokes his or her consent to receive such information, as prescribed by Presidential Decree.

(7) A person who intends to transmit advertising information for profit using an electronic transmission medium shall, when an addressee expresses his or her intention to consent to the receipt of such information under paragraphs (1) and (3) refuse to receive, or revoke his or her consent to receive, advertising information under paragraph (2), inform the relevant addressee of the outcomes of measures taken in relation to consent to receive, refusal to receive, or revocation of consent to receive, advertising information, as prescribed by Presidential Decree. <Amended on Jan. 23, 2024>

(8) A person who obtains consent to receive advertising information pursuant to paragraph (1) or (3) shall regularly verify whether an addressee of advertising information consents to receive such information, as prescribed by Presidential Decree.

[This Article Wholly Amended on May 28, 2014]

Article 50-2 Deleted. <May 28, 2014>

Article 50-3 (Commissioned Transmission of Advertising Information for Profit) (1) A person who has entrusted the transmission of advertising information for profit to a third party shall control and oversee the third party to ensure that the third party does not violate Article 50. <Amended on May 28, 2014>

(2) A person entrusted with the transmission of advertising information for profit under paragraph (1) shall be deemed an employee of a person who has entrusted the transmission of information in determining liability for damages caused by a violation of a statute related to such business affair. <Amended on Jun. 9, 2020>

[This Article Wholly Amended on Jun. 13, 2008]

Article 50-4 (Restrictions on Rendering Information Transmission Services) (1) A provider of information and communications services may take measures to refuse rendering corresponding services in any of the following cases:

1. If transmission or reception of advertising information hinders or is likely to hinder rendering the services;
2. If a user does not want to receive advertising information;
3. Deleted. <May 28, 2014>

(2) If a provider of information and communications services intends to take any measure for refusal under paragraph (1) or (4), he or she shall include matters regarding the refusal of the relevant services in the terms and conditions of a contract for use of information and communications services for which he or she concludes with the user of such services. <Amended on May 28, 2014>

(3) A provider of information and communications services shall inform interested persons, such as users to whom such services are provided, of the fact that he or she has taken measures for refusal under paragraph (1) or (4): Provided, That where it is impracticable to inform them of the fact in advance, he or she shall inform them of the fact without delay

after he or she has taken measures for refusal. <Amended on May 28, 2014>

(4) Where services which a provider of information and communications services provides to users under a contract for use are used for transmitting advertising information for profits, in violation of Article 50 or 50-8, the relevant provider of information and communications services shall formulate necessary measures, such as refusal to provide the relevant services or redressing problems of information and communications networks or services. <Newly Inserted on May 28, 2014>

[This Article Wholly Amended on Jun. 13, 2008]

Article 50-5 (Installation of Advertising Programs for Profit) When a provider of information and communications services intends to install a program designed to display advertising information or collect personal information in a user's computer or any other information processing device prescribed by Presidential Decree, he or she shall obtain consent from the user. In such cases, the provider shall notify the purpose of use of the program and the method of deletion.

[This Article Wholly Amended on Jun. 13, 2008]

Article 50-6 (Distribution of Software Designed to Block Transmission of Advertising

Information for Profit) (1) The Korea Communications Commission may develop and distribute software or computer programs designed for addressees to conveniently block or report any advertising information for profit when it is transmitted in violation of Article 50.

(2) The Korea Communications Commission may provide necessary support to related public agencies, corporations, organizations, or similar for facilitating the development and distribution of software or computer programs for blocking or reporting transmission under paragraph (1).

(3) If telecommunications services rendered by a provider of information and communications services are used in transmitting advertising information for profit in violation of Article 50, the Korea Communications Commission may recommend the provider of information and communications services to take necessary measures, such as development of technology, education, and public relations activities to protect addressees.

(4) The method of the development and distribution under paragraph (1) and the matters necessary for the support under paragraph (2) shall be prescribed by Presidential Decree.
[This Article Wholly Amended on Jun. 13, 2008]

Article 50-7 (Restrictions on Posting of Advertising Information for Profit) (1) Where any person intends to post advertising information for profit on a website, he or she shall obtain prior consent from the operator or the manager of a website: Provided, That in cases of a message board to which any person can have easy access without special authority and on which any person can post his or her message, he or she need not obtain prior consent.

(2) Notwithstanding paragraph (1), where the operator or the manager of a website explicitly expresses his or her intention to refuse to post a notice or to revoke his or her prior consent, no person who intends to post advertising information for profit shall post advertising information for profit.

(3) The operator or the manager of a website may take measures, such as deletion of advertising information for profit posted in violation of paragraph (1) or (2).

[This Article Wholly Amended on May 28, 2014]

Article 50-8 (Prohibition on Transmission of Advertising Information for Unlawful Acts) No person shall use a telecommunications network to transmit any advertising information about any goods or services whose use, sale, offering, distribution, or other similar conduct is prohibited by this Act or any other statute. <Amended on Jan. 23, 2024>

[This Article Wholly Amended on Jun. 13, 2008]

Article 51 (Restrictions on Outflow of Important Information Abroad) (1) The Government may authorize providers or users of information and communications services to take necessary measures to prevent outflow abroad of any important information about industry, economy, science, technology, etc. of this country through information and communications networks.

(2) The scope of the important information under paragraph (1) shall be as follows:

1. Information related to the national security and major policies;
2. Information about details of cutting-edge science and technology or equipment developed within this country.

(3) The Government may authorize the providers of information and communications services that manage the information under the subparagraphs of paragraph (2) to take the following measures: <Amended on Mar. 22, 2016>

1. Installation of a systematic or technical device for preventing unlawful use of information and communications networks;
2. Systematic and technical measures for preventing unlawful destruction or manipulation of information;
3. Measures for preventing leakage of important information that providers of information and communications services have learned while managing the information.

[This Article Wholly Amended on Jun. 13, 2008]

Article 52 (Korea Internet and Security Agency) (1) The Government shall establish the Korea Internet and Security Agency (hereinafter referred to as the "Internet and Security Agency") to upgrade information and communications networks (excluding matters regarding establishment, improvement, and management of information and telecommunications networks), encourage the safe use thereof, and promote the international cooperation and advancement into the overseas market in relation to broadcasting and communications. <Amended on Apr. 22, 2009; Jun. 9, 2020>

(2) The Internet and Security Agency shall be a corporation. <Amended on Apr. 22, 2009>

(3) The Internet and Security Agency shall perform the following business affairs:<Amended on Apr. 22, 2009; Feb. 17, 2012; Mar. 23, 2013; Nov. 19, 2014; Jun. 22, 2015; Jul. 26, 2017; Feb. 4, 2020; Jun. 9, 2020; Jun. 8, 2021; Jun. 10, 2022; Jan. 23, 2024>

1. Survey and research of laws, policies, and systems for the use and protection of information and telecommunications networks, promotion of the international cooperation and advancement into the overseas market in relation to broadcasting and communications, etc.;
2. Survey and analysis of statistics regarding the use and protection of information and telecommunications networks;
3. Analysis of negative effects arising from the use of information and telecommunications networks and research on countermeasures;
4. Public relations activities, education, and training for using and protecting information and telecommunications networks;

5. Information protection for information and telecommunications networks, development of technologies regarding the Internet address resources and standardization thereof;
6. Support for policies for the information security industry, development of relevant technology, and fostering of human resources;
7. Implementation of certification and evaluation of information security, such as certification of information security management systems, certification and evaluation of information security systems, certification of information security of devices and the like connected to information and communications networks, and software development security assessment; and the provision of support therefor;
8. Research of countermeasures for protecting personal information, and support for development and dissemination of protective technologies under the Personal Information Protection Act;
9. Operation of a personal information infringement call center under the Personal Information Protection Act;
10. Consultation on and processing of complaints related to transmission of advertising information and online advertisements;
11. Management of computer security incidents in information and communications networks, analysis of causes thereof, operation of systems for responding thereto; and promotion of chief information security officers' activities to prevent and respond to such incidents and to cooperate each other;
12. Support for policies on electronic signature certification under Article 21 of the Electronic Signature Act;
13. Support for an efficient operation of the Internet and encouragement of wider use thereof;
14. Support for the protection of stored information of the Internet users;
15. Support for service policies pertaining to the Internet;
16. Protection of users and support for the dissemination of sound information on the Internet;
17. Affairs related to the management of Internet address resources under the Internet Address Resources Act;

18. Support for the operation of the Internet Address Dispute Resolution Committee under Article 16 of the Internet Address Resources Act;
19. Support for operation of the conciliation committee under Article 25 (7) of the Act on the Promotion of Information Security Industry;
20. Support for such international cooperation, overseas expansion, and overseas publicity activities as are regarding broadcasting and communications;
21. Support for identification service and policies related to creation and processing of connecting information;
22. Any other business incidental to the business referred to in subparagraphs 1 through 21;
23. Other business determined to fall under the affairs of, or entrusted to, the Internet and Security Agency in accordance with this Act, or any other statute or regulation, or other business entrusted by the Minister of Science and ICT, the Minister of the Interior and Safety, the Korea Communications Commission, or the head of any other administrative agency.

(4) Expenses necessary for the business affairs of the Internet and Security Agency shall be funded by the following financial resources: <Amended on Mar. 22, 2016>

1. Government's contributions;
2. Revenues accrued from the business referred to in each subparagraph of paragraph (3);
3. Other revenues accrued from operating the Internet and Security Agency.

(5) Except as provided in this Act, the provisions governing incorporated foundations under the Civil Act shall apply mutatis mutandis to matters regarding the Internet and Security Agency. <Amended on Apr. 22, 2009>

(6) No person, other than the Internet and Security Agency, shall use the name "Korea Internet and Security Agency". <Amended on Apr. 22, 2009>

(7) Matters necessary for the operation of the Internet and Security Agency and performance of its business affairs shall be prescribed by Presidential Decree. <Amended on Apr. 22, 2009>

[This Article Wholly Amended on Jun. 13, 2008]

[Title Amended on Apr. 22, 2009]

CHAPTER VII TELECOMMUNICATIONS BILLING SERVICES

Article 53 (Registration of Providers of Telecommunications Billing Services) (1) A person who intends to render telecommunications billing services shall meet the following requirements and file for registration with the Minister of Science and ICT, as prescribed by Presidential Decree: <Amended on Feb. 29, 2008; Mar. 23, 2013; Jul. 26, 2017>

1. Financial soundness;
2. A plan for protection of users of telecommunications billing services;
3. Human resources and physical facilities required for conducting the business;
4. A business plan.

(2) A person eligible for the registration under paragraph (1) shall be either a company under Article 170 of the Commercial Act or a corporation under Article 32 of the Civil Act; and the total amount of its capital, contributions, or fundamental property shall be at least the amount prescribed by Presidential Decree, not less than 500 million won.

(3) Notwithstanding Article 22 of the Telecommunications Business Act, a provider of telecommunications billing services need not file a report of a value-added telecommunications business entity. <Amended on Mar. 22, 2010>

(4) Articles 23 through 26 of the Telecommunications Business Act shall apply mutatis mutandis to the modification of registered matters of a provider of telecommunications billing services, the transfer of business or acquisition by transfer of business, or the merger or inheritance of business, the succession to business, and the temporary closure, permanent closure, dissolution, or similar of business of a provider of telecommunications billing services. In such cases, "special telecommunications business entity" shall be construed as "provider of telecommunications billing services", and "special telecommunications business" as "telecommunications billing services". <Amended on Mar. 22, 2010; Jun. 9, 2020>

(5) Detailed requirements and procedures for the registration under paragraph (1) and other necessary matters shall be prescribed by Presidential Decree.

[This Article Newly Inserted on Dec. 21, 2007]

[Previous Article 53 moved to Article 62 <Dec. 21, 2007>]

Article 54 (Disqualification from Filing for Registration) Any of the following persons shall be disqualified from filing for registration under Article 53: <Amended on Feb. 29, 2008; Mar. 23, 2013; Jul. 26, 2017; Jun. 9, 2020>

1. A corporation for which one year has not elapsed since its business was permanently closed pursuant to Article 53 (4) or a person who was a majority shareholder (referring to an investor prescribed by Presidential Decree; hereinafter the same shall apply) of such corporation as at the time its business was permanently closed, if one year has not elapsed since the date of permanent closure of its business;
2. A corporation for which three years have not elapsed since its registration was revoked pursuant to Article 55 (1) or a person who was a majority shareholder of such corporation as at the time its registration was revoked, if three years have not elapsed since the date of revocation;
3. A corporation that is still under rehabilitation proceedings under the Debtor Rehabilitation and Bankruptcy Act or a majority shareholder of such corporation;
4. A person who did not perform his or her obligations within an agreed time limit in conducting a banking transaction or any other commercial transaction and who is prescribed by the Minister of Science and ICT;
5. A corporation any of whose majority shareholders falls under subparagraphs 1 through 4.

[This Article Newly Inserted on Dec. 21, 2007]

[Previous Article 54 Moved to Article 63 <Dec. 21, 2007>]

Article 55 (Orders to Revoke Registration) (1) Where a provider of telecommunications billing services files for registration by fraud or other improper means, the Minister of Science and ICT shall revoke the registration. <Amended on Jun. 22, 2015; Jul. 26, 2017>

(2) The procedures for the disposition under paragraph (1) and other necessary matters shall be prescribed by Presidential Decree. <Amended on Jun. 22, 2015>

[This Article Newly Inserted on Dec. 21, 2007]

[Title Amended on Jun. 22, 2015]

[Previous Article 55 moved to Article 64 <Dec. 21, 2007>]

Article 56 (Reporting on Terms and Conditions) (1) Every provider of telecommunications billing services shall prepare terms and conditions on telecommunications billing services and report it to the Minister of Science and ICT (including reporting on a revision thereto). <Amended on Feb. 29, 2008; Mar. 23, 2013; Jul. 26, 2017>

(2) If it is found that the terms and conditions under paragraph (1) are likely to undermine interests of users of telecommunications billing services, the Minister of Science and ICT may recommend the relevant provider of telecommunications billing services to revise the terms and conditions. <Amended on Feb. 29, 2008; Mar. 23, 2013; Jul. 26, 2017>

[This Article Newly Inserted on Dec. 21, 2007]
[Previous Article 56 moved to Article 65 <Dec. 21, 2007>]

Article 57 (Securing Safety in Telecommunications Billing Services) (1) Every provider of telecommunications billing services shall perform his or her duty to pay attention as a good manager so that telecommunications billing services may be provided in a safe manner. <Amended on May 28, 2014>

(2) Every provider of telecommunications billing services shall take administrative measures, including formulation of guidelines for work process and classification of accounts, and technical measures, including establishment of an information security system, to secure safety and reliability of transactions through telecommunications billing services, as prescribed by Presidential Decree.

[This Article Newly Inserted on Dec. 21, 2007]
[Previous Article 57 moved to Article 66 <Dec. 21, 2007>]

Article 58 (Rights of Users of Telecommunications Billing Services) (1) When the price for goods, etc. sold or provided must be paid, or a provider of telecommunications billing services charges the price therefor; such provider shall notify the users of telecommunications billing services of the following: <Amended on Apr. 5, 2011; May 28, 2014>

1. Date and time telecommunications billing services are used;
2. Trade name and contact information of the other party with respect to purchasing or using any good or service through telecommunications billing services (referring to a person who sells or provides any good or service in a transaction through

telecommunications billing services; hereinafter referred to as "other party to a transaction");

3. Amount purchased or used through telecommunications billing services and details thereof;

4. Methods for raising an objection and contact information.

(2) A provider of telecommunications billing services shall provide users of telecommunications billing services with a method by which users can verify the details of purchase and use and shall also furnish a user, upon request, with a written statement on the details of purchase and use (including an electronic document; hereinafter the same shall apply) within two weeks from the date of the request.

(3) A user of telecommunications billing services discovers that the telecommunications billing services have been rendered against his or her will, the user may request the provider of telecommunications billing services to make corrections (excluding where there is an intentional act or negligence on the part of the user of the telecommunications billing services), and where the provider of telecommunications billing services finds that the user's request for correction is reasonable, the provider shall withhold the payment of the price for use to a seller and shall notify the user of the results thereof within two weeks from the date of the request for correction. <Amended on May 28, 2014>

(4) Every provider of telecommunications billing services shall preserve records of telecommunications billing services during the period, within five years, prescribed by Presidential Decree.

(5) Where a provider of telecommunications billing services (referring to a person who provides services under Article 2 (1) 10 (a)) provides telecommunications billing services or increases the upper limits of use, he or she shall obtain consent from a user of the relevant telecommunications billing services in advance. <Newly Inserted on May 28, 2014>

(6) When a provider of telecommunications billing services (referring to a person who provides services under Article 2 (1) 10 (a)) amends the terms and conditions, he or she shall notify users of the amendment thereof one month prior to the effective date of the amended terms and conditions. In such cases, a user who has an objection to the amended terms and conditions may terminate the contract for telecommunications billing services. <Newly Inserted on May 28, 2014>

(7) The period, types, and scope of the details of purchase and use that a provider of telecommunications billing services should provide pursuant to paragraph (2); the types of records that a provider of telecommunications billing services should preserve pursuant to paragraph (4) and the methods for preserving such records; the methods for notifying amendment to the terms and conditions pursuant to paragraph (6); and matters necessary for terminating the contract, such as the period and procedures for raising an objection; shall be prescribed by Presidential Decree. <Amended on May 28, 2014>

(8) The Minister of Science and ICT shall prescribe and provide public notice of matters necessary for methods for giving consent, etc. under paragraph (5). <Newly Inserted on May 28, 2014; Jul. 26, 2017>

(9) The Minister of Science and ICT may prescribe and provide public notice of detailed matters regarding the methods for settling accounts, etc. so that telecommunications billing services are not provided against the will of users of telecommunications billing services. <Newly Inserted on May 28, 2014; Jul. 26, 2017>

[This Article Newly Inserted on Dec. 21, 2007]

[Previous Article 58 Moved to Article 67 <Dec. 21, 2007>]

- Article 58-2 (Request for Providing Information about Purchasers)** (1) Any user of telecommunications billing services may request the counter-party to a transaction to provide information about the name and date of birth of a person who purchased or used goods, etc. (hereinafter referred to as "purchaser information") if necessary to ascertain that telecommunications billing services have been provided according to his or her intention. In such cases, the counter-party so requested to provide purchaser information shall provide such information within three days from the date of the request without good cause.
- (2) A user of telecommunications billing services shall use the purchaser information provided pursuant to paragraph (1) only for the purpose of identifying the relevant purchaser or submitting such information to an investigative agency in filing a criminal complaint or report.
- (3) Other matters necessary relating to the content of, and the procedures for, requests for purchaser information shall be prescribed by Presidential Decree.

[This Article Newly Inserted on Jun. 12, 2018]

Article 59 (Mediation in and Resolution of Disputes) (1) Any provider of telecommunications billing services may establish and operate an institution or organization to autonomously mediate, resolve, or otherwise address disputes to protect rights and interests of users of telecommunications billing services. <Amended on Jun. 12, 2018; Jun. 9, 2020>

(2) If deemed necessary for mediating, resolving, or otherwise addressing disputes, an organization or institution authorized to mediate and resolve disputes under paragraph (1) may request purchaser information on behalf of a user of telecommunications billing services with consent of the user. In such cases, Article 58-2 shall apply mutatis mutandis to the request for purchaser information, etc. <Newly Inserted on Jun. 12, 2018>

(3) Every provider of telecommunications billing services shall prepare a procedure for raising an objection by users of telecommunications billing services in connection with the services and redressing damages to their rights, as prescribed by Presidential Decree, and where the provider enters into a contract for telecommunications billing services, the provider shall stipulate such procedure in the terms and conditions of use. <Amended on May 28, 2014; Jun. 12, 2018>

[This Article Newly Inserted on Dec. 21, 2007]

[Title Amended on Jul. 12, 2018]

[Previous Article 59 Moved to Article 68 <Dec. 21, 2007>]

Article 60 (Liability for Damages) (1) A provider of telecommunications billing services shall be liable for damages caused to a user of the telecommunications billing services while rendering the services: Provided, That the same shall not apply where the damages were caused by intention or gross negligence on the part of the user of the telecommunications billing services. <Amended on Jun. 9, 2020>

(2) A provider of telecommunications billing services shall negotiate with the claimant to damages for agreement on compensation for the damages under paragraph (1). <Amended on Jun. 9, 2020>

(3) If parties fail to or are unable to reach an agreement on compensation for damages under paragraph (2), either party may file an application for decision with the Korea Communications Commission. <Amended on Feb. 29, 2008>

[This Article Newly Inserted on Dec. 21, 2007]

[Previous Article 60 moved to Article 69 <Dec. 21, 2007>]

Article 61 (Restrictions on Use of Telecommunications Billing Services) The Minister of Science and ICT may order a provider of telecommunications billing services to deny, suspend, or place a restriction on, the services against any of the following persons:
<Amended on Feb. 29, 2008; Sep. 15, 2011; Mar. 23, 2013; Jul. 26, 2017>

1. A person who sells, lends, or provides any media product harmful to youths to a youth in violation of Article 16 of the Youth Protection Act;
2. A person who undermines interests of users of telecommunications billing services seriously by enticing the users to purchase or use goods or services in any of the following means:
 - (a) Transmitting any advertising information for profit in violation of Article 50;
 - (b) Deceiving or enticing users of telecommunications billing services wrongfully;
3. A person who sells or renders goods or services prohibited by this Act or any other statute.

[This Article Newly Inserted on Dec. 21, 2007]

[Previous Article 61 Moved to Article 70 <Dec. 21, 2007>]

CHAPTER VIII INTERNATIONAL COOPERATION

Article 62 (International Cooperation) The Government shall cooperate reciprocally with other nations or international organizations in performing the following affairs:

1. Deleted; <Feb. 4, 2020>
2. Affairs for the protection of youths in information and communications networks;
3. Affairs for the prevention of acts that undermine safety of information and communications networks;
4. Other affairs for the facilitation of sounder and safer use of information and communications services.

[This Article Wholly Amended on Jun. 13, 2008]

Article 63 Deleted. <Feb. 4, 2020>

Article 63-2 Deleted. <Feb. 4, 2020>

CHAPTER IX SUPPLEMENTARY PROVISIONS

- Article 64 (Submission of Data)** (1) The Minister of Science and ICT or the Korea Communications Commission may require a provider of information and communications services (including a domestic agent; hereafter in this Article the same shall apply) to submit related articles, documents, and others in any of the following cases: <Amended on Mar. 29, 2011; Feb. 17, 2012; Mar. 23, 2013; Jul. 26, 2017; Sep. 18, 2018; Feb. 4, 2020>
1. Where the Minister or the Commission becomes aware of a violation or suspected violation of this Act;
 2. Where the Minister or the Commission receives a report or petition on a violation of this Act;
 - 2-2. Where an event, accident, or similar occurs or is likely to occur that noticeably damages safety and reliability of users' information;
 3. Where there is any other ground prescribed by Presidential Decree to believe that it is necessary for the protection of users.
- (2) When the Korea Communications Commission intends to take the following measures against a person who transmitted any advertising information for profit in violation of this Act, it may request a provider of information and communications services to let it peruse or to submit data of the person who transmitted the advertising information, such as the name, address, and resident registration number of the person and the period for access: <Amended on Feb. 4, 2020>
1. Corrective measures under paragraph (4);
 2. Imposition of administrative fines under Article 76;
 3. Any similar measures.
- (3) If a provider of information and communications services fails to submit data under paragraph (1) or (2) or if it is found that a provider of information and communications services has violated this Act, the Minister of Science and ICT or the Korea Communications Commission may assign public officials under his, her, or its control to enter the place of business of the person concerned related to such violation of this Act, including the provider of information and communications services, for inspecting the

current status of business, account books, documents, and others. <Amended on Mar. 29, 2011; Mar. 23, 2013; Mar. 22, 2016; Jul. 26, 2017; Feb. 4, 2020>

(4) The Minister of Science and ICT or the Korea Communications Commission may order a provider of information and communications services who has violated this Act to take corrective measures as necessary to stop or correct the violation and may also require a provider of information and communications services who has been ordered to take corrective measures to announce to the public the fact that he or she received the order to take such corrective measures. In such cases, the matters necessary for the methods, guidelines, and procedures for the public announcement and other related matters shall be prescribed by Presidential Decree. <Amended on Mar. 29, 2011; Mar. 23, 2013; Jul. 26, 2017; Feb. 4, 2020>

(5) In cases of issuing an order to take corrective measures as necessary pursuant to paragraph (4), the Minister of Science and ICT or the Korea Communications Commission may disclose to the public the issuance of the order to take corrective measures. In such cases, the matters necessary for the methods, guidelines, and procedures for the public disclosure and other related matters shall be prescribed by Presidential Decree. <Amended on Mar. 29, 2011; Mar. 23, 2013; Jul. 26, 2017>

(6) When demanding submission or perusal of data or other materials pursuant to paragraph (1) or (2), the Minister of Science and ICT or the Korea Communications Commission shall give a written notice (including an electronic document), specifically stating the reasons and legal authority for such demand, the time limit for submission or the date and time for perusal, the details of data subject to the submission or perusal, and other related matters. <Amended on Mar. 29, 2011; Mar. 23, 2013; Jul. 26, 2017>

(7) When an inspection under paragraph (3) is to be conducted, the plan for the inspection, including the date and time of, and the reasons for and details of, the inspection, shall be notified to the relevant provider of information and communications services not later than seven days before the commencement of the inspection: Provided, That the plan for such inspection shall not be notified in an emergency case or if it is deemed impossible to accomplish the purposes of the inspection because of anticipated destruction of evidence or any other factor if a prior notice is given. <Amended on Feb. 4, 2020>

(8) The public officials who conduct an inspection pursuant to paragraph (3) shall carry an identification indicating their authority with them to present it to people concerned, and shall deliver to the people concerned a document stating their names, the time and purposes of access, and other related matters, whenever they access to a place of business.

(9) In cases of receiving, perusing, or inspecting data or any other material submitted pursuant to paragraphs (1) through (3), the Minister of Science and ICT or the Korea Communications Commission shall notify the relevant provider of information and communications services of the results thereof (including the details of disposition, in cases of intending to make a disposition, such as an order to take corrective measures, as a result of the inspection) in writing. <Amended on Mar. 29, 2011; Mar. 23, 2013; Jul. 26, 2017; Feb. 4, 2020>

(10) The Minister of Science and ICT or the Korea Communications Commission may ask technical advice or any other support of the head of the Internet and Security Agency as necessary in demanding submission of data or conducting an inspection pursuant to paragraphs (1) through (4). <Amended on Apr. 22, 2009; Mar. 29, 2011; Mar. 23, 2013; Jul. 26, 2017>

(11) Demand for submission of data or any other material, and perusal and inspection thereof under paragraphs (1) through (3) shall be limited to the least extent necessary for the enforcement of this Act and shall be not abused for any other purpose.

[This Article Wholly Amended on Jun. 13, 2008]

Article 64-2 (Protection and Destruction of Data) (1) If asked by a provider of information and communications services to protect documents, data, or any other material submitted or collected pursuant to Article 64, the Minister of Science and ICT or the Korea Communications Commission shall not furnish them to a third party or disclose them to the general public. <Amended on Mar. 29, 2011; Mar. 23, 2013; Jul. 26, 2017; Feb. 4, 2020>

(2) In cases of receiving data submitted through an information and communications network or converting collected data or any other material into an electronic format, the Minister of Science and ICT or the Korea Communications Commission shall take systematic and technical measures for security to protect personal information, trade secret, or similar from being leaked. <Amended on Mar 29, 2011; Mar. 23, 2013; Jul. 26, 2017>

(3) If any of the following events occurs, the Minister of Science and ICT or the Korea Communications Commission shall immediately destroy documents, data, or any other material submitted or collected pursuant to Article 64, except as otherwise provided in any other statute. The same shall apply to a person to whom the authority of the Minister of Science and ICT or the Korea Communications Commission has been fully or partially delegated or entrusted under Article 65: <Amended on Mar. 29, 2011; Mar. 23, 2013; Jul. 26, 2017>

1. If the objectives of demanding submission of data, conducting a field inspection, or issuing an order to take corrective measures pursuant to Article 64 have been achieved;
2. If an administrative trial or administrative litigation is filed against an order issued to take corrective measures pursuant to Article 64 (4), when proceedings of such administrative trial are completed;
3. If a disposition is made to impose an administrative fine under Article 76 (4) and there is no objection to it, when the period to raise an objection under paragraph (5) of that Article ends;
4. If there is an objection filed against disposition of an administrative fine under Article 76 (4), when the non-contentious case procedures are closed at the competent court.

[This Article Wholly Amended on Jun. 13, 2008]

Article 64-3 Deleted. <Feb. 4, 2020>

Article 64-4 (Hearings) The Minister of Science and ICT or the Korea Communications Commission shall hold a hearing in any of the following cases: <Amended on Jul. 26, 2017; Feb. 4, 2020; Jun. 9, 2020>

1. Where intending to revoke the designation of a certification body in accordance with Article 9 (2);
2. Where intending to revoke the designation of an identification service agency in accordance with Article 23-4 (1);
3. Where intending to revoke certification of an information security management system in accordance with Article 47 (10);
4. Where intending to revoke the designation of a certification body for information security management systems in accordance with Article 47-2 (1);

5. Where intending to revoke any rating of information security management system in accordance with Article 47-5 (4);
 - 5-2. Where intending to revoke information security certification under Article 48-6 (3);
 - 5-3. Where intending to revoke the designation of a testing agency for certification under Article 48-6 (5);
 6. Where intending to revoke the registration in accordance with Article 55 (1).
- [This Article Newly Inserted on Dec. 1, 2015]

- Article 64-5 (Obligation to Submit Transparency Reports)** (1) A provider of information and communications services who meet the criteria prescribed Presidential Decree, such as the average number of daily users, sales, and types of business, shall prepare an annual report stating the following (hereinafter referred to as "transparency report") with regard to the disposition of illegally filmed materials or the like circulated through information and communications services rendered by the provider and shall submit the report to the Korea Communications Commission by January 31 of the following year:
1. Matters concerning the general efforts made by the provider of information and communications services to prevent the circulation of illegally filmed materials or the like;
 2. Matters concerning the number, details, criteria for processing, results of examination, and results of processing of reports on illegally filmed materials or the like and requests for deletion, etc. of such materials under Article 22-5 (1) of the Telecommunications Business Act;
 3. Matters concerning the preparation and operation of procedures necessary for preventing circulation, such as deleting illegally filmed materials or the like and blocking access thereto, under Article 22-5 (1) of the Telecommunications Business Act;
 4. Matters concerning the placement of persons responsible for preventing the circulation of illegally filmed materials or the like;
 5. Matters concerning the provision of internal training and support for preventing the circulation of illegally filmed materials or the like;
- (2) The Korea Communications Commission shall disclose transparency reports through the information and communications network operated and managed by it.
- (3) The Korea Communications Commission may request a provider of information and communications services to submit data to ascertain the facts of a transparency report or

ascertain the authenticity of the submitted data.

[This Article Newly Inserted on Jun. 9, 2020]

- Article 65 (Delegation and Entrustment of Authority)** (1) The Minister of Science and ICT or the Korea Communications Commission may delegate or entrust part of his or her authority under this Act to the heads of affiliated agencies or the presidents of the regional Korea posts, as prescribed by Presidential Decree. <Amended on Mar. 29, 2011; Mar. 23, 2013; Jul. 26, 2017; Feb. 4, 2020>
- (2) The Minister of Science and ICT may entrust projects under Article 13 for facilitating the use of information and communications networks to the National Information Society Agency under Article 14 of the Framework Act on National Informatization, as prescribed by Presidential Decree. <Amended on Mar. 23, 2013; Jul. 26, 2017; Jun. 9, 2020>
- (3) The Minister of Science and ICT or the Korea Communications Commission may entrust the Internet and Security Agency with business affairs related to demanding submission of data and conducting inspections pursuant to Article 64 (1) and (2), as prescribed by Presidential Decree. <Amended on Apr. 22, 2009; Mar. 29, 2011; Mar. 23, 2013; Jul. 26, 2017>
- (4) Article 64 (8) shall apply mutatis mutandis to employees of the Internet and Security Agency under paragraph (3). <Amended on Apr. 22, 2009>
- [This Article Wholly Amended on Jun. 13, 2008]

Article 65-2 Deleted. <Dec. 30, 2005>

Article 66 (Confidentiality) A person who is or was engaged in a job related to any of the following business affairs shall not divulge to another person any secret that he or she has learned while performing his or her duties, nor does he or she use it for any purpose other than performance of his or her duties: Provided, That the same shall not apply if any other statute provides otherwise: <Amended on Feb. 17, 2012; Jun. 9, 2020>

1. Deleted; <Mar. 29, 2011>
2. Certification of an information security management system under Article 47;
- 2-2. Deleted; <Feb. 4, 2020>
3. Evaluation of information security systems under Article 52 (3) 4;

4. Deleted; <Feb. 17, 2012>

5. Conciliation of disputes by the defamation dispute conciliation division under Article 44-10.

[This Article Wholly Amended on Jun. 13, 2008]

Article 67 Deleted. <Feb. 4, 2020>

Article 68 Deleted. <Mar. 22, 2010>

Article 68-2 Deleted. <Jun. 22, 2015>

Article 69 (Legal Fiction as Public Officials in Application of Penalty Provisions) Executive officers and employees of the National Information Society Agency and the Internet and Security Agency who engage in the business affairs entrusted by the Minister of Science and ICT or the Korea Communications Commission pursuant to Article 65 (2) or (3) shall be deemed public officials in applying Articles 129 through 132 of the Criminal Act.

<Amended on Apr. 22, 2009; Mar. 29, 2011; Mar. 23, 2013; Jul. 26, 2017>

[This Article Wholly Amended on Jun. 13, 2008]

Article 69-2 Deleted. <Feb. 4, 2020>

CHAPTER X PENALTY PROVISIONS

Article 70 (Penalty Provisions) (1) A person who commits defamation of another person by disclosing a fact to the public through an information and communications network purposely to disparage the reputation of such person, shall be punished by imprisonment with labor for up to three years or by a fine not exceeding 30 million won. <Amended on May 28, 2014>

(2) A person who commits defamation of another person by disclosing a false fact to the public through an information and communications network purposely to disparage the reputation of such person, shall be punished by imprisonment with labor for up to seven years, by suspension of qualification for up to 10 years, or by a fine not exceeding 50 million won.

(3) The prosecution may not prosecute a person who committed a crime under paragraph (1) or (2) against the victim's will explicitly manifested.

[This Article Wholly Amended on Jun. 13, 2008]

Article 70-2 (Penalty Provisions) A person who conveys or spread a malicious program in violation of Article 48 (2) shall be punished by imprisonment with labor for up to seven years or by a fine not exceeding 70 million won.

[This Article Newly Inserted on Mar. 22, 2016]

Article 71 (Penalty Provisions) (1) Any of the following persons shall be punished by imprisonment with labor for up to five years or by a fine not exceeding 50 million won:
<Amended on Mar. 22, 2016; Dec. 24, 2018; Jan. 23, 2024>

1. Deleted; <Feb. 4, 2020>
2. Deleted; <Feb. 4, 2020>
3. Deleted; <Feb. 4, 2020>
4. Deleted; <Feb. 4, 2020>
5. Deleted. <Feb. 4, 2020>
6. Deleted; <Feb. 4, 2020>
7. Deleted; <Feb. 4, 2020>
8. Deleted; <Feb. 4, 2020>
9. A person who creates and processes connecting information, in violation of Article 23-5 (1);
10. A person who processes connecting information beyond the scope of purposes under Article 23-5 (4);
11. A person who intrudes into the information and communication network, in violation of Article 48 (1);
12. A person who causes a trouble to the information and communication network, in violation of Article 48 (3);
13. A person who installs a program, technical device, etc. in the information and communications network or an information system related thereto, or transmits or disseminates it, in violation of Article 48 (4);
14. A person damages the information of others or infringes, steals, or discloses the secrets of others, in violation of Article 49;

(2) Any attempt referred to in paragraph (1) 11 shall be punished. <Newly Inserted on Mar. 22, 2016>

[This Article Wholly Amended on Jun. 13, 2008]

[Enforcement Date: Jul. 24, 2024]

Article 72 (Penalty Provisions) (1) Any of the following persons shall be punished by imprisonment with labor for up to three years or by a fine not exceeding 30 million won: <Amended on Jan. 20, 2015; Mar. 27, 2015; Feb. 4, 2020; Jan. 23, 2024>

1. Deleted; <Mar. 22, 2016>

1-2. A person who transmits to a youth any information containing advertisement of a media product harmful to youths or displays such information openly without taking any measures to restrict access by youths, in violation of Article 42-2;

2. A person who collects another person's information in violation of Article 49-2 (1);

2-2. A person who transmits any advertising information, in violation of Article 50-8;

3. A person who conducts affairs without filing for registration under Article 53 (1);

4. A person who lends a loan to someone, or offers, intermediates, recommends, or advertise such loan by committing any of the following acts:

(a) Conducting, or engaging someone to conduct vicariously, a transaction through telecommunications billing services by pretending sale or supply of goods or services or billing more than an actual selling price;

(b) Engaging a user of telecommunications billing services to purchase or use certain goods or services through telecommunications billing services and then purchasing, at a discount, the goods or services purchased or used by the user of telecommunications billing services;

5. A person who divulges to another person any secret known to him or her while performing his or her duties or uses such secret for any purpose other than performance of his or her duties in violation of Article 66.

(3) Deleted. <Feb. 22, 2016>

[This Article Wholly Amended on Jun. 13, 2008]

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

won: <Amended on May 28, 2014; Mar. 22, 2016; Jun. 12, 2018; Feb. 4, 2020; Jun. 10, 2022>

1. Deleted; <Feb. 4, 2020>

1-2. Deleted; <Feb. 4, 2020>

2. A person who provides a media product harmful to youths for profit without labeling it as such in violation of Article 42;

3. Deleted; <Jan. 23, 2024>

4. A person who uses user's information for any purpose other than filing a civil or criminal lawsuit, in violation of Article 44-6 (3);

5. A person who fails to comply with an order issued by the Korea Communications Commission under Article 44-7 (2) or (3);

6. A person who fails to preserve relevant data, in violation of an order issued pursuant to Article 48-4 (4);

7. A person who entices another person to provide him or her with information in violation of Article 49-2 (1);

7-2. A person who uses provided information for any purpose other than identifying a purchaser or submitting the information to an investigative agency in filing a criminal complaint or report, in violation of Article 58-2 (including where that Article shall apply mutatis mutandis under Article 59 (2));

8. A person who fails to comply with an order issued pursuant to Article 61.

[This Article Wholly Amended on Jun. 13, 2008]

Article 74 (Penalty Provisions) (1) Any of the following persons shall be punished by imprisonment with labor for up to one year or by a fine not exceeding 10 million won: <Amended on Feb. 17, 2012; May 28, 2014>

1. A person who puts any similar label on a product or sells a product bearing any similar label, or who displays such product with intent to sell it, in violation of Article 8 (4);

2. A person who distributes, sells, lends, or openly displays any obscene codes, letters, sound, images, or motion pictures in violation of Article 44-7 (1) 1;

3. A person who makes any codes, letters, sound, images, or motion pictures arousing fear or apprehension reach another person repeatedly in violation of Article 44-7 (1) 3;

4. A person who takes measures, in violation of Article 50 (5);
 5. Deleted; <May 28, 2014>
 6. Deleted; <Jan. 23, 2024>
 7. A person who fails to file for any modification of registered matters, or who fails to file a report on transfer, acquisition by transfer, merger, or inheritance of business, in violation of Article 53 (4).
- (2) The prosecution may not prosecute a person who committed a crime under paragraph (1) 3 against the victim's will explicitly manifested.
- [This Article Wholly Amended on Jun. 13, 2008]

Article 75 (Joint Penalty Provisions) If the representative of a corporation, or an agent or employee of, or any other person employed by, a corporation or individual commits any violation referred to in Articles 71 through 73 or Article 74 (1) in conducting the business affairs of the corporation or individual, the corporation or the individual shall, in addition to punishing the violator accordingly, be punished by a fine prescribed in the relevant Article: Provided, That this shall not apply where such corporation or individual has not been negligent in giving due attention and supervision regarding the relevant business affairs to prevent such violation.

[This Article Wholly Amended on Mar. 17, 2010]

Article 75-2 (Confiscation and Punitive Collection) Money and goods or other profits received by a person committing any crime referred to in Article 72 (1) 2 and subparagraph 7 of Article 73 with respect to the relevant violation may be confiscated, and if it is impossible to confiscate such money and goods or other profits, the value thereof may be punitively collected. In such cases, the penalty of confiscation or punitive collection may be imposed in addition to any other penalty. <Amended on Feb. 4, 2020>

[This Article Newly Inserted on Mar. 22, 2016]

Article 76 (Administrative Fines) (1) Any of the following persons and any of the following persons who commit an act falling under any of subparagraphs 7 through 11 shall be subject to an administrative fine not exceeding 30 million won:<Amended on Mar. 29, 2011; Feb. 17, 2012; Mar. 23, 2013; May 28, 2014; Jun. 22, 2015; Dec. 1, 2015; Mar. 22, 2016; Jul. 26, 2017; Sep. 18, 2018; Feb. 4, 2020; Jun. 8, 2021; Jan. 3, 2023; Jan. 23, 2024>

1. A person who refuses to provide services, in violation of Article 22-2 (2);
- 1-2. A person who fails to take measures necessary to protect users' information such as devising methods for users to give or revoke consent to access authority, in violation of Article 22-2 (3);
2. A person who collects or uses resident registration numbers in violation of Article 23-2 (1) or fails to take necessary measures in violation of Article 23-2 (2);
- 2-2. Deleted; <Feb. 4, 2020>
- 2-3. Deleted; <Feb. 4, 2020>
- 2-4. Deleted; <Feb. 4, 2020>
- 2-5. A person who fails to take physical, technical or administrative measures under Article 23-6 (1);
- 2-6. A person who fails to take safety measures in accordance with Article 23-6 (2);
3. Deleted; <Feb. 4, 2020>
4. Deleted; <Feb. 4, 2020>
5. Deleted. <Feb. 4, 2020>
- 5-2. Deleted; <Feb. 4, 2020>
6. Deleted; <May 28, 2014>
- 6-2. A person who fails to designate an executive officer or employee meeting the standards prescribed by Presidential Decree as a chief information security officer, or fails to report the designation of a chief information security officer, in violation of Article 45-3 (1);
- 6-3. A person who requires a chief information security officer to hold another office concurrently other than to perform duties prescribed in Article 45-3 (4), in violation of paragraph (3) of that Article;
- 6-4. A person who fails to comply with a corrective order issued under Article 46 (3);
- 6-5. A person who fails to have an information security management system certified, in violation of Article 47 (2);
7. A person who transmits any advertising information for profit, in violation of Article 50 (1) through (3);
8. A person who fails to state the matters required to be stated, or who states false information on such matters, when transmitting any advertising information, in violation

of Article 50 (4);

9. A person who imposes the burden of any expense on an addressee, in violation of Article 50 (6);

9-2. A person who fails to verify whether an addressee consents to receiving advertising information, in violation of Article 50 (8);

9-3. A person who fails to take necessary measures, in violation of Article 50-4 (4);

10. A person who installs a program without consent of the relevant user, in violation of Article 50-5;

11. A person who posts any advertising information for profit on a website, in violation of Article 50-7 (1) or (2);

11-2. Deleted; <Feb. 4, 2020>

12. A person who fails to comply with an order issued, for violation of this Act, by the Minister of Science and ICT or the Korea Communications Commission pursuant to Article 64 (4).

(2) Any of the following persons shall be subject to an administrative fine not exceeding 20 million won: <Amended on Mar. 22, 2016; Jun 12, 2018; Sep. 18, 2018; Feb. 4, 2020; Jun. 9, 2020>

1. Deleted; <Feb. 4, 2020>

1-2. Deleted; <Feb. 4, 2020>

2. Deleted; <Feb. 4, 2020>

3. Deleted; <Feb. 4, 2020>

4. Deleted; <Feb. 4, 2020>

4-2. A person who fails to take out insurance, in violation of Article 46 (2);

4-3. A person who fails to designate a domestic agent, in violation of Article 32-5 (1);

4-4. A person who fails to designate a person responsible for preventing the circulation of illegally filmed materials or the like, in violation of Article 44-9 (1);

5. Deleted. <Feb. 4, 2020>

(3) Any of the following persons shall be subject to an administrative fine not exceeding 10 million won: <Amended on Apr. 22, 2009; Apr. 5, 2011; Feb. 17, 2012; May 28, 2014; Jun. 22, 2015; Dec. 1, 2015; Mar. 22, 2016; Jul. 26, 2017; Jun. 12, 2018; Jun. 12, 2018; Feb. 4, 2020; Jun. 9, 2020; Jun. 10, 2022; Jan. 3, 2023; Jan. 23, 2024>

1. Deleted; <Jun. 22, 2015>
2. Deleted; <Jun. 22, 2015>
- 2-2. A person who engages in the identification service without being designated as an identification service agency, in violation of Article 23-3 (1);
- 2-3. A person who fails to notify as to suspension of the identification service under Article 23-3 (2) or as to discontinuation of the identification service under Article 23-3 (3) to users or who fails to report the same to the Korea Communications Commission;
- 2-4. A person who continuously engages in the identification service notwithstanding a disposition for suspension of the identification service and revocation of the designation as an identification service agency under Article 23-4 (1);
- 2-5. Deleted; <Feb. 4, 2020>
3. A person who fails to designate a person responsible for protection of youths in violation of Article 42-3 (1);
4. A person who fails to preserve information, in violation of Article 43;
- 4-2. A person who fails to take technical and administrative measures, in violation of Article 44-7 (5);
- 4-3. A person who fails to comply without good cause with a request to submit data under Article 46 (4) of the Act: Provided, That the foregoing shall not apply to the heads of relevant central administrative agencies (including their affiliated agencies) shall be excluded;
- 4-4. A person who fails to file a report or files a false report, in violation of Article 46 (6);
5. Deleted; <Jun. 12, 2018>
6. Deleted; <Dec. 1, 2015>
7. A person who advertises false details of the certification he or she has obtained, in violation of Articles 47 (9);
8. Deleted; <Feb. 17, 2012>
9. Deleted; <Feb. 17, 2012>
10. A person who fails to give notice to users of software, in violation of Article 47-4 (4);
11. A person who fails to comply with an order issued pursuant to Article 48-2 (4) to take corrective measures;

- 11-2. A person who fails to report a computer security incident, in violation of Article 48-3 (1);
- 11-3. A person who fails to submit data demanded under Article 48-4 (5) or submits false data;
- 12. A person who obstructs, refuses, or evades access to a place of business to conduct an investigation under Article 48-4 (5);
- 12-2. A person who fails to comply with an order issued by the Minister of Science and ICT or the Korea Communications Commission, in violation of Article 49-2 (4);
- 12-3. A person who fails to inform the results of handling consent to receive, refusal to receive, or revocation of consent to receive, advertising information, in violation of Article 50 (7);
- 12-4. Deleted; <Jan. 23, 2024>
- 13. A person who uses the name of the Korea Internet and Security Agency, in violation of Article 52 (6);
- 14. A person who fails to file a report on temporary closure, permanent closure, or dissolution of business, in violation of Article 53 (4);
- 15. A person who fails to report terms and conditions, in violation of Article 56 (1);
- 16. A person who fails to take administrative or technical measures, in violation of Article 57 (2);
- 17. A person who fails to notify a user of telecommunications billing services of the date and time of using the aforementioned services and other necessary matters, in violation of Article 58 (1);
- 18. A person who fails to provide a user of telecommunications billing services with the method by which the user can verify the details of purchase or use, or who fails to respond to a request by a user of telecommunications billing services for the provision of such method, in violation of Article 58 (2);
- 19. A person who fails to withhold payment of the price though a request to correct a telecommunications bill he or she has received from a user of telecommunications billing services is reasonable or who fails to notify the user of telecommunications billing services of the results of the measures taken in response to a request of the user, in violation of Article 58 (3);

20. A person who fails to preserve records of telecommunications billing services, in violation of Article 58 (4);
- 20-2. A person who provides telecommunications billing services or increases the maximum use without obtaining consent from a user of telecommunications billing services, in violation of Article 58 (5);
- 20-3. A person who fails to give notice regarding amendment to the terms and conditions of telecommunications billing services, in violation of Article 58 (6);
- 20-4. A person who fails to comply with a request by a user of telecommunications billing services for information, in violation of Article 58-2 (including where that Article shall apply mutatis mutandis under Article 59 (2));
21. A person who fails to prepare the procedures for raising an objection by users of telecommunications billing services and redressing their infringed rights or who fails to stipulate such procedures when he or she enters into a contract for telecommunications billing services, in violation of Article 59 (3);
22. A person who fails to submit, or who falsely submitted, goods, documents, or any other material under Article 64 (1);
23. A person who fails to respond to a request for perusal or submission of data under Article 64 (2);
24. A person who refuses, obstructs or evades access and inspection under Article 64 (3);
25. A person who fails to submit rules, etc. in violation of Article 64-5 (1).
- (4) The administrative fines prescribed in paragraphs (1) through (3) shall be imposed and collected by the Minister of Science and ICT or the Korea Communications Commission, as prescribed by Presidential Decree. <Amended on Mar. 29, 2011; Mar. 23, 2013; Jul. 26, 2017>
- (5) Deleted. <Mar. 14, 2017>
- (6) Deleted. <Mar. 14, 2017>
- (7) Deleted. <Mar. 14, 2017>
- [This Article Wholly Amended on Jun. 13, 2008]