ENFORCEMENT DECREE OF THE PROTECTION OF COMMUNICATIONS SECRETS ACT

Wholly Amended by Presidential Decree No. 20660, Feb. 29, 2008
Amended by Presidential Decree No. 22151, May 4, 2010
Presidential Decree No. 22467, Nov. 2, 2010
Presidential Decree No. 22605, Dec. 31, 2010
Presidential Decree No. 24445, Mar. 23, 2013
Presidential Decree No. 25050, Dec. 30, 2013
Presidential Decree No. 25532, Aug. 6, 2014
Presidential Decree No. 27806, Jan. 26, 2017
Presidential Decree No. 28210, Jul. 26, 2017
Presidential Decree No. 28211, Jul. 26, 2017

Article 1 (Purpose)

The purpose of this Decree is to provide for matters delegated by the Protection of Communications Secrets Act and matters necessary for the enforcement thereof.

Article 2 (Basic Principles in Application of the Act)

Where a prosecutor (including a military prosecutor; hereinafter the same shall apply), judicial police officer (including a military judicial police officer; hereinafter the same shall apply) or the head of an intelligence and investigative agency censors mail or wiretaps telecommunications (hereinafter referred to as "measures restricting communications") for criminal investigation or national security or where he/she records or monitors undisclosed conversations between third parties, he/she shall do so only where measures restricting communications or the recording or monitoring of conversations are especially required and where all requirements prescribed by the Protection of Communications Secrets Act (hereinafter referred to as the "Act") are met; and even if he/she takes measures restricting communications or records or monitors conversations upon obtaining a permit or approval in accordance with the Act, he/she shall immediately cease such activities where deemed unnecessary to continue such activities, thereby ensuring infringement on communications secrets of the people is limited to the minimum.

Article 3 (Equipment and Facilities Excluded from Wiretapping Equipment)

Equipment and facilities excluded from wiretapping equipment pursuant to the proviso to subparagraph 8 of Article 2 of the Act are any of the following, which are not appliances or apparatus manufactured for the purpose of wiretapping: *<Amended by Presidential Decree No. 22605, Dec. 31, 2010; Presidential Decree No. 27806, Jan. 26, 2017>*

1. Telecommunications equipment and facilities for business under subparagraph 4 of Article 2 of the Telecommunications Business Act;
2. Telecommunications equipment and facilities for personal use installed pursuant to Article 64 of the Telecommunications Business Act;
3. Deleted; *<by Presidential Decree No. 22605, Dec. 31, 2010>*
4. Radio communication equipment of a radio station established pursuant to Article 19 of the Radio Waves Act;
5. Broadcasting and communication equipment that underwent assessment on appropriateness pursuant to Article 58-2 of the Radio Waves Act;
6. Radio communication equipment used for monitoring of radio waves under Articles 49 and 50 of the Radio Waves Act;
7. Applied radio equipment for communications permitted pursuant to Article 58 of the Radio Waves Act;
8. Audio and video applications (including those using direct current) among electric appliances under subparagraph 1 of Article 2 of the Electrical Appliances and Consumer Products Safety Control Act;
9. Hearing aids or appliances and apparatus similar thereto;
10. Other appliances and apparatus generally used for telecommunications and radio control.

Article 4 (Requests for Permission for Measures Restricting Communications for Criminal Investigation)

(1) In addition to matters under Article 6 (4) of the Act, the following matters shall be mentioned in a request for permission for measures restricting communications for criminal investigation under Article 6 (4) of the Act:

1. The gist of suspicion;
2. Where several permits are requested at the same time, the purport thereof and grounds therefor.

(2) A prosecutor who requests such permission shall sign and seal a request for permission under paragraph (1).

Article 5 (Procedures for Extension of Period of Measures Restricting Communications)

(1) Where a prosecutor, judicial police officer or the head of an intelligence and investigative agency requests permission or applies for approval for extension of the period of measures restricting

communications pursuant to Articles 6 (7) and 7 (2) of the Act, he/she shall make such request or application in writing.

(2) A prosecutor, judicial police officer or the head of an intelligence and investigative agency shall state a reason why an extension of the period is required and the period to be extended in a document referred to in paragraph (1) and attach explanatory materials thereto.

Article 6 (Scope, etc. of Intelligence and Investigative Agencies)

(1) "Intelligence and investigative agencies prescribed by Presidential Decree" in Article 7 (1) of the Act means agencies under subparagraph 6 of Article 2 of the Regulations on Planning and Adjustment of Intelligence and Security Affairs.

(2) Where the head of an intelligence and investigative agency takes measures restricting communications under Article 7 of the Act and a judicial police officer takes measures restricting communications for investigation of an intelligence crime, etc. referred to in subparagraph 5 of Article 2 of the Regulations on Planning and Adjustment of Intelligence and Security Affairs among crimes referred to in the subparagraphs of Article 5 (1) of the Act, the Director of the National Intelligence Service (hereinafter referred to as the "Director of the NIS") may consult the head of the relevant intelligence and investigative agency on the selection of crimes subject to measures restricting communications and adjust the selection only where consultations and adjustment are required to prevent the abuse of measures restricting communications, such as overlapping of crimes subject to measures restricting communications between intelligence and instigative agencies.

Article 7 (Permission from Court concerning Measures Restricting Communications for National Security)

(1) A high court under Article 7 (1) 1 of the Act refers to the high court having jurisdiction over the place of domicile or the seat of both parties or one party of Koreans to be subjected to measures restricting communications.

(2) Where it is impracticable for the chief judge of a high court under paragraph (1) to perform his/her duties due to illness, overseas trip, long-term business trip, etc., the president of the relevant high court may appoint an associate judge to conduct affairs related to permission on behalf of the chief judge.

(3) Where the head of an intelligence and investigative agency intends to take measures restricting communications pursuant to Article 7 (1) 1, he/she shall file an application for a request for permission with a prosecutor of a high prosecutors' office equivalent to a high court under paragraph (1).

(4) Where a prosecutor of a high prosecutors' office who has received an application under paragraph (3) requests permission for measures restricting communications, Article 4 shall apply mutatis mutandis thereto.

Article 8 (President's Approval for Measures Restricting Communications for National Security)

(1) Where the head of an intelligence and investigative agency intends to take measures restricting communications pursuant to Article 7 (1) 2 of the Act, he/she shall submit a plan for such measures to the Director of the NIS.

(2) The Director of the NIS shall review whether a plan submitted by the head of an intelligence and investigative agency under paragraph (1) is appropriate, and where he/she judges that the plan is not appropriate, he/she may request the head of the relevant intelligence and investigative agency to withdraw such plan.

(3) Where the head of an intelligence and investigative agency prepares a plan under paragraph (1), Article 6 (4) of the Act and Article 4 of this Decree shall apply mutatis mutandis thereto.

(4) The Director of the NIS shall integrate plans submitted by the head of an intelligence and investigative agency pursuant to paragraph (1), apply for approval to the President, and notify the head of the relevant intelligence and investigative agency of the outcomes thereof in writing.

Article 9 (Parties to Communications in Relation to Measures Restricting Communications for National Security)

(1) In applying Article 7 of the Act, where the name of a party to communications is indicated differently from the name of the relevant real party, such as the assumed name or borrowed name, notwithstanding such different indication, measures restricting communications shall be based on the relevant real party.

(2) Where one party to communications is a person provided for in Article 7 (1) 2 of the Act and the other party is not specified or unclear, such cases shall be deemed communications referred to in Article 7 (1) 2 of the Act.

Article 10 (Procedures for Emergency Measures Restricting Communications)

Where the head of an intelligence and investigative agency intends to take measures restricting communications under Article 8 of the Act for national security (hereinafter referred to as "emergency measures restricting communications") and where a judicial police officer intends to take emergency measures restricting communications for investigation of an intelligence crime, etc. under subparagraph 5 of Article 2 of the Regulations on Planning and Adjustment of Intelligence and Security Affairs, he/she shall receive adjustment from the Director of the NIS beforehand: Provided, That where there is an extraordinary ground that he/she cannot receive adjustment beforehand, he/she shall immediately obtain approval therefor after the fact.

Article 11 (Matters to Be Attended to When Implementing Measures Restricting Communications)

(1) No person who implements measures restricting communications pursuant to Article 9 of the Act (including a person who has been entrusted with the execution thereof pursuant to the latter part of Article 9 (1) of the Act; hereafter the same shall apply in this Article) shall cause interference in the normal

communication of mail and telecommunications and the maintenance, repair, etc. thereof on the ground of the implementation thereof.

(2) No person who implements measures restricting communications shall divulge confidential information of others he/she has learned in the course of implementing such measures or impair the reputation of persons who are subjected to measures restricting communications.

Article 12 (Cooperation in Implementation of Measures Restricting Communications)

Where a prosecutor, judicial police officer or the head of an intelligence and investigative agency (including a public official under his/her jurisdiction delegated by him/her) requests a communications agency or any other related agency to provide cooperation in the implementation of measures restricting communications, he/she shall issue a copy of the cover of a permit for measures restricting communications under Article 9 (2) of the Act (in cases referred to in Article 7 (1) 2 of the Act, referring to a letter of approval from the President; hereafter the same shall apply in Articles 13 (2), 16 (1) and (2) and 17 (1) through (3)) or a permit for emergency wiretapping, and produce a certificate of character that may indicate his/her identity to the head of a communications agency or any other related agency.

Article 13 (Entrustment of Implementation of Measures Restricting Communications)

(1) A prosecutor, judicial police officer or the head of an intelligence and investigative agency may entrust the implementation of measures restricting communications to any of the following agencies having jurisdiction over the place of domicile or the seat of one or both parties to be subjected to measures restricting communications pursuant to Article 9 (1) of the Act, the crime scene or the place of domicile or the seat of a person who is an accomplice to parties to communications:

1. A post office, the head of which is a public official of Grade V or higher;
2. A telecommunications service provider under the Telecommunications Business Act.

(2) Where a prosecutor, judicial police officer or the head of an intelligence and investigative agency (including a public official delegated by him/her) intends to entrust the implementation of measures restricting communications to an agency under any of the following subparagraphs of paragraph (1) (hereinafter referred to as "communications agency, etc."), he/she shall issue a copy of the cover of a permit for measures restricting communications or a permit for emergency wiretapping, etc. (referring to a permit for emergency censorship or permit for emergency wiretapping; hereinafter the same shall apply) along with a request for entrustment issued by the head of an agency to which he/she belongs and present an identification indicating his/her authority to a communications agency, etc.

(3) In addition to paragraphs (1) and (2), the Minister of Science and ICT or the head of a telecommunications service provider shall determine matters necessary for entrustment, such as the scope of entrusted affairs, etc. in consultation with the head of an agency who has entrusted the implementation of measures restricting communications. *<Amended by Presidential Decree No. 24445, Mar. 23, 2013; Presidential Decree No. 28210, Jul. 26, 2017>*

Article 14 (Measures for Smooth Communication of Mail and Telecommunications)

(1) Where cooperation in the implementation of measures restricting communications pursuant to Article 12 or the implementation of measures restricting communications entrusted pursuant to Article 13 (1) causes interference with normal communication of mail and telecommunications, the head of a communication agency, etc. may request a prosecutor, judicial police officer or the head of an intelligence and investigative agency who has requested such cooperation or entrusted such measures to correct such intereference. In such cases, any person requested to correct such intereference shall immediately correct it.

(2) Where any telecommunications service provider (hereinafter referred to as "telecommunications service provider") under the Telecommunications Business Act judges that the provision of data for confirmation of the fact of communications pursuant to Article 13 of the Act causes considerable intereference with his/her business, he/she may provide data for confirmation of the fact of communications in consultation with or by making adjustments with a prosecutor, judicial police officer or the head of an intelligence and investigative agency who has requested to provide such data so that such interference may be minimized.

Article 15 (Recording and Signing of Fact of Handing over and Taking over of Mail)

Where a prosecutor, judicial police officer or the head of an intelligence and investigative agency takes over mail from a post office for postal censorship and returns mail he/she has taken over, a person who takes over and a person who hands over the relevant mail shall record and sign the fact of the handing over and taking over of the relevant mail in the book of cooperation in the implementation of measures restricting communications.

Article 16 (Suspension of Execution, etc. of Entrusted Affairs)

(1) Where a prosecutor, judicial police officer or the head of an intelligence and investigative agency has entrusted a communications agency, etc. with the implementation of emergency measures restricting communications, he/she shall submit a copy of the cover of a permit for measures restricting communications to a communications agency, etc. within 36 hours from the time it implements entrusted measures restricting communications.

(2) Where a prosecutor, judicial police officer or the head of an intelligence and investigative agency fails to submit a copy of the cover of a permit for measures restricting communications within hours under paragraph (1), a communications agency, etc. shall immediately discontinue the implementation of entrusted affairs.

(3) Where a communications agency, etc. discontinues the implementation of entrusted affairs pursuant to paragraph (2), a prosecutor, judicial police officer or the head of an intelligence and investigative agency shall immediately return mail, if any, which he/she has taken over from the communications agency, etc.

Article 17 (Period, etc. for Preservation of Copy of Cover of Permit, etc. for Measures Restricting Communications)

(1) Types, objects, the scope, the period, the place and method of implementation, etc. of measures restricting communications shall be indicated on a copy of the cover of a permit for measures restricting communications or a permit for emergency wiretapping, etc. to be submitted to a communications agency, etc. pursuant to Articles 12, 13 and 16.

(2) The period for preservation of a copy of the cover of a permit for measures restricting communications or a permit for emergency wiretapping, etc. and the period for keeping the book under Article 9 (3) shall be three years: Provided, That where such permit or book is classified as confidentiality pursuant to the Regulations on Security Affairs, the period for such preservation or keeping shall be the period for protection of such confidentiality.

(3) Any person who has been entrusted with the implementation of measures restricting communications or provided cooperation in the implementation thereof pursuant to Articles 12 through 16 shall take proper measures for preservation, such as restrictions on perusal, in order to protect confidentiality on a copy of the cover of a permit for measures restricting communications or a permit for emergency wiretapping, etc. and the book thereof, and prevent damage to or the falsification of such copy and book.

Article 18 (Measures after Implementing Measures Restricting Communications)

(1) A prosecutor, judicial police officer or the head of an intelligence and investigative agency who has implemented measures restricting communications shall prepare a report on the details of the implementation thereof and the gist of the outcomes obtained therefrom, and take proper measures for preservation, such as seal and restrictions on perusal, in order to protect confidentiality thereon and prevent damage thereto and the falsification thereof, along with the outcomes obtained from the implementation of such measures restricting communications.

(2) Where a judicial police officer closes a case he/she has investigated or investigated internally by implementing measures restricting communications, he/she shall report the outcomes thereof to a prosecutor: Provided, That this shall not apply where he/she sends such case to the prosecution.

(3) Where the head of an intelligence and investigative agency has gathered information by implementing measures restricting communications under Article 7 of the Act or a judicial police officer has closed a case he/she investigated or investigated internally by implementing measures restricting communications on an intelligence crime, etc. under subparagraph 5 of Article 2 of the Regulations on Planning and Adjustment of Intelligence and Security Affairs, he/she shall prepare a written report on the details of the implementation thereof and the gist of the outcomes obtained therefrom and submit it to the Director of the NIS.

(4) In cases of the outcomes obtained from measures restricting communications for criminal investigation, the period for preservation in the implementation of measures for preservation under

paragraph (1) shall be the period the same as the period for preservation of the record of a criminal case related thereto, and in cases of the outcomes obtained from measures restricting communications for national security, the period for preservation in the implementation of measures for preservation under paragraph (1) shall be the period for protection of confidentiality classified pursuant to the Regulations on Security Affairs.

Article 19 (Postponement of Notice on Implementation of Measures Restricting Communications)

(1) Where a prosecutor or judicial police officer intends to obtain approval from the director of the competent district prosecutors' office (including the senior prosecutor of the competent ordinary prosecution department) in order to postpone notice on the implementation of measures restricting communications pursuant to Article 9-2 (5) of the Act, he/she shall file a written application for approval stating types, objects, the scope and the period of implemented measures restricting communications, the date he/she dealt with a case for which measures restricting communications were implemented and the outcomes thereof, grounds that he/she intends to postpone notice, etc. In such cases, the judicial police officer shall submit a document applying for approval from the director of the competent district prosecutors' office to the competent district prosecutors' office or its branch office (including the competent ordinary prosecution department).

(2) The director of the competent district prosecutors' office who has received an application under paragraph (1) shall review grounds for postponement of notice, etc. and notify a prosecutor or judicial police officer of the outcomes thereof.

Article 20 (Designation of Persons in Charge of Dealing with Entrusted Affairs)

(1) Where the head of a communications agency, etc. is entrusted with the implementation of measures restricting communications, he/she shall designate persons in charge of dealing with such entrusted affairs.

(2) Among persons in charge of dealing with entrusted affairs under paragraph (1), persons in charge of dealing with entrusted affairs of measures restricting communications for national security under Article 7 of the Act shall be only persons granted access to Class II classified information, and the number of persons designated shall be kept to the minimum necessary.

Article 21 (Bearing Expenses and Providing Equipment and Facilities Following Entrustment of Affairs, etc.)

(1) The head of a communications agency, etc. entrusted with the implementation of measures restricting communications or requested to provide cooperation in the implementation thereof and the head of a communications agency, etc. requested to provide cooperation in the implementation of requests for providing data for confirmation of the fact of communications may request the head of an agency to which a prosecutor or judicial police officer who has entrusted the execution thereof or requested the provision of such data belongs or the head of an intelligence and investigative agency (hereafter in this Article referred

to as "head of an entrusting agency") to pay expenses incurred in conducting such affairs.

(2) The head of an entrusting agency and the head of an entrusted agency shall consult about methods, etc. of the calculation of expenses under paragraph (1) and the payment thereof and determine such methods, etc.

(3) A prosecutor, judicial police officer or the head of an intelligence and investigative agency who has entrusted the implementation of measures restricting communications shall provide the head of a communications agency, etc. with equipment necessary for the implementation thereof.

Article 22 (Approval for Manufacture, etc. of Wiretapping Equipment)

(1) Any person who intends to obtain approval for the manufacture, importation, sale, distribution, possession, use and advertising of wiretapping equipment (hereinafter referred to as "approval for wiretapping equipment") pursuant to Article 10 of the Act shall submit an application for approval for wiretapping equipment and a schematic diagram of the relevant wiretapping equipment to the Minister of Science and ICT along with data on the purpose of an application for approval, specifications and performance of such equipment. <*Amended by Presidential Decree No. 24445, Mar. 23, 2013; Presidential Decree No. 28210, Jul. 26, 2017*>

(2) The Minister of Science and ICT, upon receiving an application for approval under paragraph (1), shall review such application and approve it only where the purpose thereof is deemed by him/her to be appropriate and wiretapping equipment is deemed by him/her not to cause damage to other telecommunications equipment and facilities. In such case, the Minister of Science and ICT may fix the period for validity of approval in consideration of the type, purpose, etc. of such approval. <*Amended by Presidential Decree No. 24445, Mar. 23, 2013; Presidential Decree No. 28210, Jul. 26, 2017*>

(3) Where the Minister of Science and ICT has granted approval for wiretapping equipment under paragraph (2), he/she shall issue a letter of approval for wiretapping equipment to an applicant. <*Amended by Presidential Decree No. 24445, Mar. 23, 2013; Presidential Decree No. 28210, Jul. 26, 2017*>

(4) Where the Minister of Science and ICT has not approved an application for approval under paragraph (1), he/she shall issue a document specifying grounds therefor in detail to the relevant applicant. <*Amended by Presidential Decree No. 24445, Mar. 23, 2013; Presidential Decree No. 28210, Jul. 26, 2017*>

Article 23 (Book of Management of Wiretapping Equipment)

Any person who has obtained approval for wiretapping equipment pursuant to Article 22 (2) shall keep the book of management of wiretapping equipment and record the conditions of the management thereof pursuant to Article 10 (4) of the Act.

Article 24 (Revocation, etc. of Approval)

(1) Where any person who has obtained approval under Article 22 falls under any of the following, the Minister of Science and ICT shall revoke such approval and notify him/her of his/her decision in writing:

<Amended by Presidential Decree No. 24445, Mar. 23, 2013; Presidential Decree No. 28210, Jul. 26, 2017>

1. Where it is proved that he/she has obtained approval by fraud or other improper means;
2. Where he/she has violated Article 10 (4) of the Act.

(2) Any person in whose case approval has been revoked pursuant to paragraph (1) shall, without delay, return a letter of approval to the Minister of Science and ICT. *<Amended by Presidential Decree No. 24445, Mar. 23, 2013; Presidential Decree No. 28210, Jul. 26, 2017>*

Article 25 (Disposal of Illegal Wiretapping Equipment)

Where any approval for wiretapping equipment is revoked pursuant to Article 24 or the validity period of approval under the latter part of Article 22 (2) expires, any person who has obtained approval for wiretapping equipment shall discontinue the manufacture, sale, use, etc. of such wiretapping equipment, dispose of such wiretapping equipment or take other necessary measures, and report the outcomes thereof to the Minister of Science and ICT. *<Amended by Presidential Decree No. 24445, Mar. 23, 2013; Presidential Decree No. 28210, Jul. 26, 2017>*

Article 26 (Hearings)

Where the Minister of Science and ICT intends to revoke approval pursuant to Article 24 (1) or revoke the registration of illegal wiretapping equipment detection service pursuant to Article 10-5 of the Act, he/she shall hold a hearing. *<Amended by Presidential Decree No. 24445, Mar. 23, 2013; Presidential Decree No. 28210, Jul. 26, 2017>*

Article 27 (Reporting, etc. of Wiretapping Equipment by State Agencies)

(1) "Matters prescribed by Presidential Decree" in Article 10-2 (1) and (2) of the Act means any of the following matters:

1. Types and names of wiretapping equipment;
2. Quantity;
3. Operating voltage;
4. Methods of use;
5. Wiretapping capability;
6. Timing for introduction.

(2) Where a State agency (excluding an intelligence and investigative agency) introduces wiretapping equipment, it shall report matters referred to in any of the following subparagraphs of paragraph (1) to the Minister of Science and ICT within 15 days after each half year expires. *<Amended by Presidential Decree No. 24445, Mar. 23, 2013; Presidential Decree No. 28210, Jul. 26, 2017>*

(3) Where a State agency makes a report under paragraph (2), it shall attach documents stating matters referred to in any of the following subparagraphs of paragraph (1) for each wiretapping equipment.

(4) Where an intelligence and investigative agency introduces wiretapping equipment, it shall notify the Intelligence Committee of the National Assembly of matters referred to in paragraph (1) within 15 days after each half year expires.

Article 28 (Application for Registering Illegal Wiretapping Equipment Detection Service)

(1) Any person who intends to register illegal wiretapping equipment detection service (hereinafter referred to as "illegal wiretapping equipment detection service") under Article 10-3 (1) of the Act shall submit an application for registration of illegal wiretapping equipment detection service (including electronic documents) to the Minister of Science and ICT along with the following documents (including electronic documents): *<Amended by Presidential Decree No. 24445, Mar. 23, 2013; Presidential Decree No. 28210, Jul. 26, 2017>*

1. A plan to protect users and a business plan;
2. The current status of technical human resources and certificates of work experience of the relevant technical human resources (to attach only in cases of technical human resources who do not have national technical qualifications under the National Technical Qualifications Act);
3. The current status of detection equipment in possession.

(2) The Minister of Science and ICT, upon receipt of an application for registration pursuant to paragraph (1), shall confirm a corporation registration certificate and national technical qualifications of the relevant technical human resources through the sharing of administrative information under Article 36 (1) of the Electronic Government Act: Provided, That where the relevant technical human resources do not consent to the confirmation of national technical qualifications, the Minister of Science and ICT shall require them to attach a copy of the relevant national technical qualifications. *<Amended by Presidential Decree No. 22151, May 4, 2010; Presidential Decree No. 22467, Nov. 2, 2010; Presidential Decree No. 24445, Mar. 23, 2013; Presidential Decree No. 28210, Jul. 26, 2017>*

Article 29 (Issuance, etc, of Certificates of Registration)

(1) Upon receipt of an application for registration pursuant to Article 28, where such application is deemed by the Minister of Science and ICT to meet requirements for registration referred to in Article 30, he/she shall record the following matters in the book of registration of illegal wiretapping equipment detection service and issue a certificate of registration of illegal wiretapping equipment detection service (hereinafter referred to as "certificate of registration") to the relevant applicant within 20 days from the date he/she receives such application: *<Amended by Presidential Decree No. 24445, Mar. 23, 2013; Presidential Decree No. 28210, Jul. 26, 2017>*

1. Registration number and the date of registration;
2. The name of the corporation;
3. Its representative;

4. The seat of the principal office;

5. Capital.

(2) Where the Minister of Science and ICT deems supplementation to an application for registration under Article 28 is needed, he/she may request an applicant to supplement such application for a fixed period of not more than seven days. In such case, the period required for supplementation shall not be included in the period of processing referred to in paragraph (1). *<Amended by Presidential Decree No. 24445, Mar. 23, 2013; Presidential Decree No. 28210, Jul. 26, 2017>*

(3) Where any person who has registered illegal wiretapping equipment detection service (hereinafter referred to as "business entity responsible for detecting illegal wiretapping equipment") loses a certificate of registration issued pursuant to paragraph (1) or the certificate of registration is worn out, he/she may request the Minister of Science and ICT to reissue a certificate of registration. *<Amended by Presidential Decree No. 24445, Mar. 23, 2013; Presidential Decree No. 28210, Jul. 26, 2017>*

Article 30 (Requirements for Registration of Illegal Wiretapping Equipment Detection Service)

Requirements for registration of illegal wiretapping equipment detection service under Article 10-3 (3) of the Act shall be as specified in attached Table 1.

Article 31 (Registration of Changes in Illegal Wiretapping Equipment Detection Service)

(1) Where a business entity responsible for detecting illegal wiretapping equipment intends to change any of the following matters, he/she shall register such changes with the Minister of Science and ICT: *<Amended by Presidential Decree No. 24445, Mar. 23, 2013; Presidential Decree No. 28210, Jul. 26, 2017>*

1. Trade name;

2. Representative;

3. The seat of the principal office;

4. A plan to protect users;

5. A business plan;

6. Capital;

7. Technical human resources.

(2) Any person who intends to register changes in illegal wiretapping equipment detection service pursuant to paragraph (1) shall submit an application for registration of changes to illegal wiretapping equipment detection service (including an application in an electronic document) to the Minister of Science and ICT along with documents (including electronic documents) according to the following classification: *<Amended by Presidential Decree No. 24445, Mar. 23, 2013; Presidential Decree No. 28210, Jul. 26, 2017>*

1. Where he/she intends to change the name of a corporation, the representative thereof or the seat of the principal office: A certificate of registration;

2. Where he/she intends to change a plan to protect users or a business plan: Terms and conditions for use to be changed or related documents;

3. Where he/she intends to change technical human resources: Certificates of work experience of technical human resources to be changed (to attach only in case of technical human resources who do not have national technical qualifications under the National Technical Qualifications Act).

(3) The Minister of Science and ICT, upon receipt of an application for registration of changes in the name of a corporation, the representative thereof, the seat of the principal office or capital pursuant to paragraph (2) shall verify a corporation registration certificate and national technical qualifications of the relevant technical human resources through the sharing of administrative information under Article 36 (1) of the Electronic Government Act: Provided, That where the relevant technical human resources do not consent to the verification of national technical qualifications, the Minister of Science and ICT shall require them to attach a copy of the relevant national technical qualifications. *<Amended by Presidential Decree No. 22151, May 4, 2010; Presidential Decree No. 22467, Nov. 2, 2010; Presidential Decree No. 24445, Mar. 23, 2013; Presidential Decree No. 28210, Jul. 26, 2017>*

(4) Where the Minister of Science and ICT accepts the registration of changes (only applicable to the registration of changes referred to in paragraph (1) 1 through 3), he/she shall enter changed matters into a certificate of registration and issue such certificate of registration to the relevant applicant. *<Amended by Presidential Decree No. 24445, Mar. 23, 2013; Presidential Decree No. 28210, Jul. 26, 2017>*

Article 32 (Transfer, etc. of Illegal Wiretapping Equipment Detection Service)

Where a business entity responsible for detecting illegal wiretapping equipment intends to transfer illegal wiretapping equipment detection service or to merge a corporation (excluding any case in which a corporation that is a business entity responsible for detecting illegal wiretapping equipment intends to merge a corporation that is not a business entity responsible for detecting illegal wiretapping equipment), he/she shall submit a report on the transfer and merger of illegal wiretapping equipment detection service (including a report prepared in an electronic document) to the Minister of Science and ICT along with the following documents (including electronic documents): *<Amended by Presidential Decree No. 24445, Mar. 23, 2013; Presidential Decree No. 28210, Jul. 26, 2017>*

1. A copy of a transfer contract or merger contract;
2. A certificate of registration.

Article 33 (Succession to Illegal Wiretapping Equipment Detection Service)

Where a business entity responsible for detecting illegal wiretapping equipment reports on transfer or merger under Article 32, a person who obtains illegal wiretapping equipment detection service by transfer shall succeed to the status of a person who transfers illegal wiretapping equipment detection service as a business entity responsible for detecting illegal wiretapping equipment, and a corporation that is incorporated or continues to exist by the merger of the corporation shall succeed to the status of the

corporation that disappears by the merger as a business entity responsible for detecting illegal wiretapping equipment.

Article 34 (Suspension and Closure of Illegal Wiretapping Equipment Detection Service)

(1) Where a business entity responsible for detecting illegal wiretapping equipment intends to suspend illegal wiretapping equipment detection service for at least one month or close such service, he/she shall submit a report on suspension or closure of illegal wiretapping equipment detection service to the Minister of Science and ICT along with a certificate of registration (only where he/she closes illegal wiretapping equipment detection service). *<Amended by Presidential Decree No. 24445, Mar. 23, 2013; Presidential Decree No. 28210, Jul. 26, 2017>*

(2) The period for suspension of illegal wiretapping equipment detection service shall not exceed one year.

Article 35 (Delegation of Authority)

The Minister of Science and ICT shall delegate his/her authority over the following matters to the Director General of the Central Radio Management Office pursuant to Article 10-3 (4) of the Act: *<Amended by Presidential Decree No. 24445, Mar. 23, 2013; Presidential Decree No. 28210, Jul. 26, 2017>*

1. Registration of illegal wiretapping equipment detection service under Article 10-3 of the Act and registration of changes therein under Article 31 of this Decree;
2. Revocation of registration and suspension of business of illegal wiretapping equipment detection service under Article 10-5 of the Act;
3. Hearings on the revocation of registration of illegal wiretapping equipment detection service under Article 26;
4. Reporting of the transfer or merger of illegal wiretapping equipment detection service under Article 32;
5. Reporting of the suspension or closure of illegal wiretapping equipment detection service under Article 34.

Article 36 (Guidelines for Administrative Disposition)

Guidelines for disposition of the revocation of registration and the suspension of business of illegal wiretapping equipment detection service under Article 10-5 of the Act shall be as specified in attached Table 2.

Article 37 (Requests, etc. for Providing Data for Confirmation of Fact of Communications)

(1) The term "competent district court or branch court" in the main body of and proviso to Article 13 (2) of the Act means a district court or branch court having jurisdiction over the place of domicile, the seat or the crime scene of a suspect or a person under investigation, or the place of domicile or the seat of the relevant subscriber.

(2) Where a prosecutor or judicial police officer needs to request a telecommunications service provider to provide data for confirmation of the fact of communications not on a suspect or a person who is investigated but on many subscribers for investigation of the same crime or the execution of a sentence on the same person, he/she may request the provision of such data with one request for permission.

(3) Articles 11 through 13 and 17 through 21 shall apply mutatis mutandis to requests for providing data for confirmation of the fact of communications for criminal investigation or internal investigation and the notification thereof: Provided, That this shall not apply to the main body of Article 17 (2).

(4) Articles 5 through 13, 16 through 18, 20 and 21 shall apply mutatis mutandis to requests for providing data for confirmation of the fact of communications for national security and the notification thereof: Provided, That this shall not apply to the main body of Article 17 (2).

(5) Where a prosecutor, judicial police officer or the head of an intelligence and investigative agency (including a public official under his/her jurisdiction delegated by him/her) issues a copy of the cover of a permit to request the provision of data for confirmation of the fact of communications or a request for providing data for emergency confirmation of the fact of communications, or produce a certificate of character indicating his/her identity to a telecommunications service provider pursuant to Article 12, he/she may issue such copy or produce such certificate of character by fax.

Article 38 (Book on Provision of Data for Confirmation of Fact of Communications)

Where any telecommunication business entity provides data for confirmation of the fact of communications pursuant to Articles 13 (1), 13-2 and 13-4 (1) of the Act, he/she shall record the fact of providing such data in the book of the provision of data for confirmation of the fact of communications.

Article 39 (Reporting on Current Status of Provision of Data for Confirmation of Fact of Communications)

Any telecommunications service provider shall report the current status of the provision of data, etc. to the Minister of Science and ICT within 30 days after each half year expires pursuant to Article 13 (7) of the Act. *<Amended by Presidential Decree No. 24445, Mar. 23, 2013; Presidential Decree No. 28210, Jul. 26, 2017>*

Article 40 (Matters to be Entered in Reports on Measures Restricting Communications)

(1) A report on measures restricting communications submitted to the National Assembly by the head of a central administrative agency of an agency which has implemented measures restricting communications pursuant to Article 15 (4) of the Act shall include the current status of statistics, such as the number of cases in which measures restricting communications were permitted or approved, the number of cases in which measures restricting communications were implemented, and the number of notifications regarding implementation of measures restricting communications.

(2) A report on measures restricting communications submitted to the National Assembly by the head of a central administrative agency of an agency which has been entrusted with the implementation of measures

restricting communications or has provided cooperation in the implementation thereof pursuant to Article 15 (4) of the Act shall include the current status of statistics, such as the number of cases in which he/she has been entrusted with the implementation of measures restricting communications or the number of cases in which he/she has provided cooperation in the implementation thereof.

(3) Where the Minister of Science and ICT deems it necessary to prepare a report on measures restricting communications under Article 15 (4) of the Act, he/she may request the head of an agency who has been entrusted with the implementation of measures restricting communications or has provided cooperation in the implementation thereof to submit a report on the current status of statistics under paragraph (2) every half year. In such case, the head of an agency which received the request shall comply therewith unless any special ground exists otherwise. *<Amended by Presidential Decree No. 24445, Mar. 23, 2013; Presidential Decree No. 28210, Jul. 26, 2017>*

Article 41 (Telecommunications Service Providers' Duty to Provide Cooperation, etc.)

(1) Where the imminent risk of the life or health of an individual, such as murder and robbery with hostages, exists, any telecommunications service provider shall provide cooperation so that a request for measures restricting communications or for providing data for confirmation of the fact of communications is completed without delay pursuant to Article 15-2 of the Act.

(2) The period for preservation of data for confirmation of the fact of communications of a telecommunications service provider under Article 15-2 (2) of the Act shall be at least the period in the following classification:

1. Data for confirmation of the fact of communications under subparagraph 11 (a) through (d) and (f) of Article 2 of the Act: 12 months: Provided, That in cases of data related to long-distance call and local call services, the period shall be six months;
2. Data for confirmation of the fact of communications under subparagraph 11 (e) and (g) of Article 2 of the Act: three months.

Article 41-2 (Management of Personally Identifiable Information)

When it is inevitable for performing affairs concerning the confirmation of grounds for disqualifying a business entity responsible for detecting illegal wiretapping equipment under Article 10-4 of the Act, the Minister of Science and ICT (including a person to whom the authority of the Minister has been delegated under Article 35) may manage data containing resident registration numbers under subparagraph 1 of Article 19 of the Enforcement Decree of the Personal Information Protection Act. *<Amended by Presidential Decree No. 28210, Jul. 26, 2017>*

Article 41-3 (Re-examination of Regulation)

The Minister of Science and ICT shall examine the appropriateness of the following matters every three years counting from each base date specified in the following (referring to the period that ends on the day

before the base date of every third year) and shall take measures for improvement, etc.: <*Amended by Presidential Decree No. 28210, Jul. 26, 2017*>

1. Requirements for registration of illegal wiretapping equipment detection service under Article 30: January 1, 2014;
2. Guidelines for administrative disposition under Article 36: January 1, 2014.

Article 42 (Application Mutatis Mutandis of the Criminal Procedure Act, etc.)

Except as otherwise provided for in the Act and this Decree, the provisions on seizure and search in the Criminal Procedure Act or the Regulations on Criminal Procedure shall apply mutatis mutandis to requests for measures restricting communications and for providing data for confirmation of the fact of communications within the limits not contrary to the nature thereof.

ADDENDA

Article 1 (Enforcement Decree)

This Decree shall enter into force on the date of its promulgation.

Article 2 (Relationship to other Statutes)

Where the previous Enforcement Decree of the Protection of Communications Secrets Act, the previous Enforcement Rule of the Protection of Communications Secrets Act, or the provision thereof is cited by other statutes at the time this Decree enters into force, if the provision corresponding thereto exists in this Decree, this Decree or the relevant provision of this Decree shall be deemed cited in lieu of the former provision.

ADDENDA <*Presidential Decree No. 22151, May 4, 2010*>

Article 1 (Enforcement date)

This Decree shall enter into force on May 5, 2010.

Articles 2 through 4 Omitted.

ADDENDUM <*Presidential Decree No. 22467, Nov. 2, 2010*>

This Decree shall enter into force on the date of its promulgation.

ADDENDA <*Presidential Decree No. 22605, Dec. 31, 2010*>

Article 1 (Enforcement date)

This Decree shall enter into force on January 24, 2011. (Proviso Omitted.)

Articles 2 through 13 Omitted.

ADDENDA <*Presidential Decree No. 24445, Mar. 23, 2013*>

Article 1 (Enforcement date)

This Decree shall enter into force on the date of its promulgation.

Articles 2 through 4 Omitted.

ADDENDUM <*Presidential Decree No. 25050, Dec. 30, 2013*>

This Decree shall enter into force on the date of its promulgation. (Proviso Omitted.)

ADDENDUM <*Presidential Decree No. 25532, Aug. 6, 2014*>

This Decree shall enter into force on August 7, 2014.

ADDENDA <*Presidential Decree No. 27806, Jan. 26, 2017*>

Article 1 (Enforcement date)

This Decree shall enter into force on January 28, 2017.

Articles 2 through 4 Omitted.

ADDENDA <*Presidential Decree No. 28210, Jul. 26, 2017*>

Article 1 (Enforcement date)

This Decree shall enter into force on the date of its promulgation.

Articles 2 through 6 Omitted.

ADDENDA <*Presidential Decree No. 28211, Jul. 26, 2017*>

Article 1 (Enforcement Date)

This Decree shall enter into force on the date of its promulgation: Provided, That among Presidential Decrees amended pursuant to Article 8 of the Addenda, the amended parts of the Presidential Decrees promulgated before this Decree enters into force, but the enforcement dates of which have not arrived, shall enter into force on the dates the relevant Presidential Decrees enter into force, respectively.

Articles 2 through 8 Omitted.

Last updated : 2018-03-12