PROTECTION OF COMMUNICATIONS SECRETS ACT

Act No. 4650, Dec. 27, 1993
Amended by Act No. 5454, Dec. 13, 1997
Act No. 5681, Jan. 21, 1999
Act No. 6146, Jan. 12, 2000
Act No. 6305, Dec. 29, 2000
Act No. 6346, Jan. 8, 2001
Act No. 6546, Dec. 29, 2001
Act No. 6626, Jan. 26, 2002
Act No. 7138, Jan. 29, 2004
Act No. 7371, Jan. 27, 2005
Act No. 7428, Mar. 31, 2005
Act No. 7503, May 26, 2005
Act No. 8733, Dec. 21, 2007
Act No. 8728, Dec. 21, 2007
Act No. 8867, Feb. 29, 2008
Act No. 9752, May 28, 2009
Act No. 9819, Nov. 2, 2009
Act No. 11690, Mar. 23, 2013
Act No. 11731, Apr. 5, 2013
Act No. 12229, Jan. 14, 2014
Act No. 12764, Oct. 15, 2014
Act No. 12960, Jan. 6, 2015
Act No. 13591, Dec. 22, 2015
Act No. 13717, Jan. 6, 2016
Act No. 13719, Jan. 6, 2016
Act No. 13722, Jan. 6, 2016
Act No. 14071, Mar. 3, 2016
Act No. 14839, Jul. 26, 2017
Act No. 15493, Mar. 20, 2018
Act No. 16849, Dec. 31, 2019
Act No. 17090, Mar. 24, 2020

Act No. 17125, Mar. 24, 2020
Act No. 17347, jun. 9, 2020

Article 1 (Purpose)

The purpose of this Act is to protect communications secrets and further enhance the freedom of communications by limiting the scope of restrictions with respect to the secrecy and freedom of communications and conversations and making due process of law mandatory.

Article 2 (Definitions)

The definitions of the terms used in this Act are as follows: *<Amended by Act No. 6546, Dec. 29, 2001; Act No. 7196, Jan. 29, 2004; Act No. 7371, Jan. 27, 2005>*

1. The term "communication" means mail and electronic telecommunications;
2. The term "mail" means ordinary mail and parcel post under the Postal Service Act;
3. The term "telecommunications" means transmission or reception of all kinds of sounds, words, symbols or images by wire, wireless, fiber cable or other electromagnetic system, including telephone, e-mail, membership information service, facsimile and radio paging;
4. The term "party concerned" means any sender and addressee of mail, or any transmitter and receiver of telecommunications;
5. The term "nationals" means the people of the Republic of Korea who have their addressees or residences in areas where the sovereignty of the Republic of Korea is exercised;
6. The term "censorship" means opening mail without the consent of the party concerned or acquiring knowledge of, recording or withholding its contents through other means;
7. The term "wiretapping" means acquiring or recording the contents of telecommunications by listening to or communally reading the sounds, words, symbols or images of the communications through electronic and mechanical devices without the consent of the party concerned or interfering with their transmission and reception;
8. The term "wiretapping equipment" means electronic, mechanical or other devices that can be used in wiretapping conversations or telecommunications: Provided, That those prescribed by Presidential Decree, among telecommunications apparatuses and instruments or their parts that are generally used and hearing aids designed to correct auditory sense or others used for similar purposes shall be excluded;
8-2. The term "illegal wiretapping equipment detection" means detecting an equipment used for wiretapping or listening to conversations conducted except as provided in this Act;
9. The term "e-mail" means the transmission of any message or any message transmitted through the computer network;

10. The term "membership information service" means the information service provided to any specific member or contractor, or the network of such information service;

11. The term "communication confirmation data" means any of the following data on the records of telecommunications:

(a) The date of telecommunications by subscribers;

(b) The time that the telecommunications commence and end;

(c) The communications number of outgoing and incoming call, etc. and the subscriber number of the other party;

(d) The frequency of use;

(e) The computer communications or Internet log records relating to facts that the users of computer communications or the Internet have used the telecommunications services;

(f) The data on tracing a location of information communications apparatus connecting to the information communications networks;

(g) The data on tracing a location of connectors capable of confirming the location of information communications apparatus to be used by the users of computer communications or the Internet for connecting with the information communications networks;

12. The term "electronic serial number" means an electronic unique identification number given to a mobile phone for which a contract for utilization has been concluded with a mobile communications business entity.

Article 3 (Protection of Secrets of Communications and Conversation)

(1) No person shall censor any mail, wiretap any telecommunications, provide communication confirmation data, or record or listen to any conversation between others that is not made public, except as provided for in this Act, the Criminal Procedure Act or the Military Court Act: Provided, That the following cases shall be governed by the relevant statutes: *<Amended by Act No. 6305, Dec. 29, 2000; Act No. 6546, Dec. 29, 2001; Act No. 7138, Jan. 29, 2004; Act No. 7428, Mar. 31, 2005; Act No. 8728, Dec. 21, 2007; Act No. 9819, Nov. 2, 2009>*

1. Handling of returned mail, etc.: Where parcel postal items (including any mail similar thereto) suspected of containing such contraband items as explosives are opened, where the mail cannot be delivered to the addressee or is returned to the sender because of the addressee's refusal to accept it, where the mail is opened in order to identify the address and name of the sender of the mail that the addressee refuses to receive because of missing address and name of the sender, or where any unreturnable mail containing valuables is handled, in accordance with Articles 28, 32, 35 and 36 of the Postal Service Act;

2. Inspection of import and export mail: Customs clearance of mail, other than personal correspondence under Articles 256 and 257 of the Customs Act;

3. Communications with persons under detention or in prison: Control of communications with the persons under detention or in prison under Article 91 of the Criminal Procedure Act; Article 131 of the Military Court Act; Articles 41, 43, and 44 of the Administration and Treatment of Correctional Institution Inmates Act; and Articles 42, 44, and 45 of the Act on the Execution of Criminal Penalties in the Armed Forces and the Treatment of the Military Inmates;

4. Communications with persons declared bankrupt: Where a trustee in bankruptcy receives communications addressed to a person declared bankrupt under Article 484 of the Debtor Rehabilitation and Bankruptcy Act;

5. Monitoring radio waves for the elimination of interference, etc.: Where radio waves are monitored in order to maintain order in radio waves by, for example, eliminating interference under Articles 49 through 51 of the Radio Waves Act.

(2) Any censorship of mail or any wiretapping of telecommunications (hereinafter referred to as "communication-restricting measures") shall be used as a supplementary means of facilitating a criminal investigation or ensuring national security, and efforts shall be made to minimize the violation of people's communication secrets. *<Newly Inserted by Act No. 6546, Dec. 29, 2001>*

(3) No person shall provide or be provided with an electronic serial number: Provided, That this shall not apply where an enterprise for manufacturing mobile phones or a mobile communications business entity provides or is provided with an electronic serial number for a performance of lawful business, such as the opening of a service for mobile phones and repairs. *<Newly Inserted by Act No. 7138, Jan. 29, 2004>*

Article 4 (Prohibition of Use of Contents of Mail Obtained through Illegal Inspection and Contents of Telecommunications Obtained through Illegal Wiretapping as Evidence)

Mail or its contents obtained through illegal inspection and the contents of communication acquired or recorded through illegal wiretapping in violation of Article 3 shall not be admitted as evidence in a trial or disciplinary procedure.

Article 5 (Requirements for Permission for Communication-Restricting Measures for Criminal Investigations)

(1) The communication-restricting measures shall be allowed only when there is a substantial reason to suspect that the following crimes are being planned or committed or have been committed, and it is impracticable to otherwise prevent a crime, arrest the criminal, or collect the evidence: *<Amended by Act No. 5454, Dec. 13, 1997; Act No. 6146, Jan. 12, 2000; Act No. 6546, Dec. 29, 2001; Act No. 8733, Dec. 21, 2007; Act No. 11731, Apr. 5, 2013; Act No. 12960, Jan. 6, 2015; Act No. 13717, Jan. 6, 2016; Act No. 13719, Jan. 6, 2016; Act No. 16849 Dec. 31, 2019>*

1. Part II of the Criminal Act - Chapter I Crime concerning Insurrection, crimes under Articles 92 through 101 from Chapter II Crimes concerning Foreign Aggression, crimes under Articles 107, 108, and 111 through 113 from Chapter IV Crimes concerning Diplomatic Relations, crimes under Articles

114 and 115 from Chapter V Crimes Harming Public Safety, Chapter VI Crimes concerning Explosives, crimes under Articles 127, and 129 through 133 from Chapter VII Crimes concerning Duties of Public Officials, Chapter IX Crimes of Escape and Sheltering Criminals, crimes under Articles 164 through 167, 172 through 173, 174, and 175 from Chapter XIII Crimes of Arson and Fire Caused by Negligence, Chapter XVII Crimes concerning Opium, Chapter XVIII Crimes concerning Currency, crimes under Articles 214 through 217, 223 (limited to attempted crimes under Articles 214 through 217), and 224 (limited to preparations or conspiracies under Articles 214 and 215) from Chapter XIX Crimes concerning Securities, Postage Stamps and Revenue Stamps, Chapter XXIV Crimes of Homicide, Chapter XXIX Crimes of False Arrest and Illegal Confinement, crimes under Articles 283 (1), 284, 285 (limited to habitual crimes under Articles 283 (1) and 284), and 286 *[limited to attempted crimes under Articles 283 (1), 284, and 285 (limited to habitual crimes under Articles 283 (1) and 284)] from Chapter XXX Crimes of Intimidation, Chapter XXXI Crimes of Abduction, Inducement and Human Trafficking, crimes under Articles 297 through 301-2, and 305 from Chapter XXXII Crimes concerning Rape and Sexual Harassment, crimes under Article 315 from Chapter XXXIV Crimes Against Credit, Business and Auction, crimes under Articles 324-2 through 324-4, and 324-5 (limited to attempted crimes under Articles 324-2 through 324-4) from Chapter XXXVII Crimes of Obstruction of Exercise of Rights, crimes under Articles 329 through 331, 332 (limited to habitual crimes under Articles 329 through 331), 333 through 341, and 342 [limited to attempted crimes under Articles 329 through 331, 332 (limited to habitual crimes under Articles 329 through 331), and 333 through 341] from Chapter XXXVIII Crimes of Larceny and Robbery, crimes under Articles 350, 350-2, 351 (limited to habitual crimes under Articles 350 and 350-2), and 352 (limited to attempted crimes under Articles 350 and 350-2) from Chapter XXXIX Crimes of Fraud and Intimidation, and crimes under Article 363 from Chapter XLI Crimes concerning Stolen Properties;*

2. Part II of the Military Criminal Act - Chapter I Crimes of Rebellion, Chapter II Crimes of Benefitting the Enemy, Chapter III Crimes of Abuse of Command, Chapter IV Crimes of Surrender and Escape of Commanders, Chapter V Crimes of Desertion of Defensive Post, crimes under Article 42 from Chapter VII Crimes of Neglecting Military Duty, Chapter VIII Crimes of Mutiny, Chapter IX Crimes of Violence, Intimidation, Inflicting Bodily Injury and Homicide, Chapter XI Crimes concerning Military Supplies, and crimes under Articles 78, 80, and, 81 from Chapter XII Crimes of Disobedience to Order;

3. Crimes under the National Security Act;

4. Crimes under the Military Secret Protection Act;

5. Crimes under the Protection of Military Bases and Installations Act;

6. Crimes under Articles 58 through 62 among those under the Narcotics Control Act;

7. Crimes under Articles 4 and 5 among those under the Punishment of Violences, etc. Act;

8. Crimes under Article 70 and subparagraphs 1 through 3 of Article 71 among those under the Act on the Safety Management of Guns, Swords, Explosives, Etc.;

9. Crimes under Articles 2 through 8, 11, and 12 among those under the Act on the Aggravated Punishment, etc. of Specific Crimes;

10. Crimes under Articles 3 through 9 among those under the Act on the Aggravated Punishment, etc. of Specific Economic Crimes;

11. Crimes committed in violation of statutes governing the aggravated punishment of crimes under subparagraphs 1 and 2;

12. Crimes under Articles 3 and 4 of the Act on Combating Bribery of Foreign Public Officials in International Business Transactions.

(2) The communication-restricting measures may be permitted when the target is any specific mail or telecommunications sent and received or transmitted and received by those falling under the conditions under paragraph (1) or any specific mail or telecommunications sent and received or transmitted and received by the applicable parties during a fixed period of time.

Article 6 (Procedures for Authorization for Communication-Restricting Measures for Criminal Investigations)

(1) Any prosecutor (including any military prosecutor; hereinafter the same shall apply) may ask a court (including a military court; hereinafter the same shall apply) to permit communication-restricting measures for each suspect or person under investigation when the requirements provided for in Article 5 (1) are met. *<Amended by Act No. 6546, Dec. 29, 2001; Act No. 13722, Jan. 6, 2016>*

(2) A judicial police officer (including a military judicial police officer; hereinafter the same shall apply) may apply to a prosecutor for authorization for communication-restricting measures for each suspect or person under investigation when the requirements under Article 5 (1) are met, and then the prosecutor may request the same from the court. *<Amended by Act No. 6546, Dec. 29, 2001>*

(3) The competent court in charge of the case involving the communication-restricting measures for which a request is filed under paragraphs (1) and (2) shall be the district court or its branch court (including any ordinary military court) having jurisdiction over the address and seats of both of communication parties or one of the communication parties subject to the communication-restricting measures, the place where any crime is committed or the address and seats of persons who are accomplices of such communication parties. *<Amended by Act No. 6546, Dec. 29, 2001>*

(4) The request for communication-restricting measures under paragraphs (1) and (2) shall be made in writing (hereinafter referred to as "written application"), indicating the details of the request such as kinds, objectives, targets, scope, effective period of communication-restricting measures, the place where such communication-restricting measures are executed, how such communication-restricting measures are executed and grounds for satisfying conditions for the permission for communication-restricting measures under Article 5 (1), together with the materials establishing a prima facie case of reasons for the application. In such cases, when an application is filed for permission for the communication-restricting measures against any suspect or any person under investigation for the same crime or any permission for such purpose is granted, the applicant shall specify the objective of and the grounds for filing an application again for the communication-restricting measures. *<Amended by Act No. 6546, Dec. 29, 2001>*

(5) The court shall, when it deems the application justified, grant permission for the communication-restricting measures to each suspect or person under investigation and then deliver a document attesting his or her granting such permission (hereinafter referred to as "written permission") to the applicant. *<Amended by Act No. 6546, Dec. 29, 2001>*

(6) The written permission referred to in paragraph (5) shall specify the kind, objective, target. scope, effective period, the place where the communication-restricting measures are executed and how the communication-restricting measures are executed. *<Amended by Act No. 6546, Dec. 29, 2001>*

(7) The effective period of communication-restricting measures shall not exceed two months and in the event that the objective of the communication restricting measures is attained during the period, such communication-restricting measures shall immediately be discontinued: Provided, That if the requirements for permission under Article 5 (1) are still valid, a request for extending the effective period of communication-restricting measures may be filed, together with materials establishing a prima facie case pursuant to paragraph (1) or (2), and such period shall not exceed two months. *<Amended by Act No. 6546, Dec. 29, 2001; Act No. 16849, Dec. 31, 2019>*

(8) Where a prosecutor or a judicial police officer requests for the extension of the effective period of communication-restricting measures pursuant to the proviso of paragraph (7), the extended period of the communication-restricting measures shall not exceed one year in total. Provided, That in the case of any of the following crimes, the extended period of the communication-restricting measures shall not exceed three years in total: *<Newly Interested by Act No. 16849, Dec. 31, 2019>*

1. Crimes under Chapter I Crimes concerning Insurrection, crimes under Articles 92 through 101 of Chapter II Crimes concerning Foreign Aggression, crimes under Articles 107, 108, 111 through 113 of Chapter IV Crimes concerning Foreign Relations, crimes under Articles 114 and 115 of Chapter V Crimes against Public Peace, and crimes under Chapter VI Crimes concerning Explosives under Part II of the Criminal Act;
2. Crimes under Chapter I Crimes of Insurrection, crimes under Chapter II Crimes of Benefitting the Enemy, crimes under Chapter XI Crimes relating to Military Supplies, and crimes under Articles 78, 80, and 81 of Chapter XII Crimes of Violation of Order under Part II of the Military Criminal Act;
3. Crimes set forth in the National Security Act;
4. Crimes set forth in the Military Secret Protection Act;
5. Crimes set forth in the Protection of Military Bases and Installations Act.

(9) Where the court considers that the request made pursuant to paragraphs (1) and (2) and the proviso of paragraph (7) is groundless, it shall dismiss such request and give notice thereof to the requester. *<Amended by Act No. 16849, Dec. 31, 2019>*

Article 7 (Communication-Restricting Measures for National Security)

(1) Only when the national security is expected to be put in grave danger or it is necessary for counterterrorism activities defined in subparagraph 6 of Article 2 of the Act on Counter-Terrorism for the

Protection of Citizens and Public Security, if the collection of intelligence is required to prevent such danger, the heads of the intelligence and investigative agencies prescribed by Presidential Decree (hereinafter referred to as "heads of intelligence and investigative agencies") may take communication-restricting measures as follows: *<Amended by Act No. 6546, Dec. 29, 2001; Act No. 14071, Mar. 3, 2016; Act No. 17090, Mar. 24, 2020>*

1. If either or both of the parties concerned with a communication are Korean nationals, permission therefor from a chief presiding judge of the high court shall be obtained: Provided, That the same shall not apply to the military telecommunications (limited to where the telecommunications are used to conduct operations) provided for in Article 2 of the Military Telecommunications Act;
2. Written approval shall be obtained from the President with respect to communications of countries hostile to the Republic of Korea, foreign agencies or groups and foreign nationals suspected of engaging in antinational activities, or members of groups within the Korean Peninsula effectively beyond the sovereignty of the Republic of Korea and their umbrella groups based in foreign countries, and in the event of the proviso of paragraph (1) 1.

(2) The effective period of communication-restricting measures under paragraph (1) shall not exceed four months, and in the event that the objective of such communication-restricting measures is attained, the communication-restricting measures shall be immediately discontinued; but if the requirements prescribed in paragraph (1) continue to be in existence, the effective period of the communication-restricting measures may be extended up to four months with permission therefor from a chief presiding judge of the high court or approval therefor from the President after filing an application for such permission or approval, accompanied by the material establishing a prima facie case: Provided, That the communication-restricting measures provided for in the proviso of paragraph (1) 1 may be extended without approval therefor from the President until military operations are completed in the event that the nation is in time of war or incident, or at war with an enemy in the national emergency corresponding thereto. *<Amended by Act No. 6546, Dec. 29, 2001; Act No. 17090, Mar. 24, 2020>*

(3) Article 6 (2), (4) through (6), and (9) shall apply mutatis mutandis to the permission under paragraph 1 (1). In such cases, "judicial police officer (including military police officer; hereinafter the same shall apply)" shall be deemed “heads of intelligence and investigative agencies”; "court", " chief presiding judge of the high court"; "Article 5 (1)", "main sentence of Article 7 (1) 1"; and "communication-restricting measures for each suspect or person under investigation" in Article 6 (2) and (5), "communication-restricting measures", respectively. *<Amended by Act No. 16849, Dec. 31, 2019; Act No. 17090, Mar. 24, 2020>*

(4) Necessary matters such as procedures for a presidential approval referred to in paragraph (1) 2 shall be determined by Presidential Decree.

Article 8 (Emergency Communication-Restricting Measures)

(1) Where an act of conspiracy exists that threatens the national security, the planning or execution of any serious crime or any organized crime, or any similar is imminent that may directly cause death or serious injury, and an emergency exists that makes it impracticable to follow procedures under Article 6 or 7 (1) and (3), any prosecutor, any judicial police officer or any of the heads of intelligence and investigative agencies may take the communication-restricting measures without permission therefor from the court against any person who meets the requirements provided for in Article 5 (1) or 7 (1) 1.

(2) Any prosecutor, any judicial police officer or any of the heads of intelligence and investigative agencies shall, immediately after commencing the execution of the communication-restricting measures under paragraph (1) (hereinafter referred to as "emergency communication-restricting measures"), file an application for permission therefor with the court in accordance with Articles 6 and 7 (3); and immediately discontinue the emergency communication-restricting measures if he or she fails to obtain the permission from the court within 36 hours from the time when he or she takes the emergency communication-restricting measures.

(3) If any judicial police officer takes the emergency communication-restricting measures, he or she shall be placed under command of any prosecutor in advance: Provided, That if such emergency communication-restricting measures need to be taken urgently, making it impracticable for such judicial police officer to be placed under command of such prosecutor, approval therefor shall be obtained from such prosecutor immediately after commencing the execution of such emergency communication-restricting measures.

(4) Any prosecutor, any judicial police officer or any of the heads of intelligence and investigative agencies shall, if he or she intends to take the emergency communication-restricting measures, take such measures according to the emergency censorship statement or the emergency wiretapping statement (hereinafter referred to as "emergency wiretapping statement, etc.") and keep the records of emergency communication-restricting measures at the institution to which he or she belongs.

(5) Where the execution of communication-restricting measures is completed in a short time, making it unnecessary to obtain permission therefor from the court, the head of the competent District Prosecutor's Office (the head of the competent High Prosecutor's Office, where any of the heads of intelligence and investigative agencies takes the emergency communication-restricting measures against any person who meets the requirements under Article 7 (1) 1 in accordance with paragraph (1)) shall serve a notice of emergency communication-restricting measures, prepared by any prosecutor, any judicial police officer or any of the heads of intelligence and investigative agencies who takes the relevant communication-restricting measures, to the head of corresponding court: Provided, That where any military prosecutor or any military judicial official takes the emergency communication-restricting measures against any person who meets the requirements under Article 5 (1), a senior prosecutor of the competent Prosecutor's Office shall serve a notice of emergency communication-restricting measures to the military judge corresponding to him or her of the ordinary military tribunal. *<Amended by Act No. 13722, Jan. 6, 2016>*

(6) The notice referred to in paragraph (5) shall contain the objective, target, scope, period, the place of execution, the methods and the grounds for not filing a request for permission for the emergency communication-restricting measures, etc.

(7) The court or the military judge of the ordinary military tribunal shall, upon receipt of notice of the emergency communication-restricting measures notice served under paragraph (5), keep the records of emergency communication-restricting measures.

(8) Where an act of conspiracy exists that threatens the national security, the planning or execution of any serious crime, any organized crime, or any similar is imminent that may directly cause death or serious injury; it is short on time to obtain approval from the President for taking the emergency communication-restricting measures against any person who falls under Article 7 (1) 2; or it is judged that the national security may be put at risk unless the emergency communication-restricting measures are taken, the head of any intelligence and investigative agency may take the emergency communication-restricting measures after obtaining approval therefor from the Minister (including the Director General of the National Intelligence Agency) to whom he or she belongs.

(9) Where the emergency communication-restricting measures are taken in accordance with paragraph (8), approval therefor shall be obtained without delay from the President in accordance with Article 7; and if the head of any intelligence and investigative agency fails to obtain approval from the President within 36 hours from the time that an application therefor is filed, such emergency communication-restricting measures shall be immediately discontinued.

Article 9 (Execution of Communication-Restricting Measures)

(1) Communication-restricting measures under Articles 6 through 8 shall be executed by any prosecutor, any judicial police officer or the head of any intelligence and investigative agency who has made such request or application. In such cases, the execution may be commissioned to postal service organizations or other institutions concerned (hereinafter referred to as "communications institutions, etc.") or cooperation therewith may be sought from communications institutions, etc. *<Amended by Act No. 6546, Dec. 29, 2001>*

(2) Any person who intends to commission the execution of communication-restricting measures or ask for cooperation therewith, shall furnish any of the communications institutions, etc. with a written permission for the communication-restricting measures (referring to a written approval granted by the President in the case of Article 7 (1) 2; hereafter the same shall apply in this Article and Articles 16 (2) 1 and 17 (1) 1 and 3) or a copy of the cover of an emergency wiretapping statement, etc. and any person who is commissioned or asked for cooperation shall keep such written permission for the communication-restricting measures or such copy of the cover of an emergency wiretapping statement for a period fixed by Presidential Decree. *<Amended by Act No. 6546, Dec. 29, 2001>*

(3) Any person who executes the communication-restricting measures, is commissioned to execute such measures or asked for cooperation therewith, shall keep records in which the objectives of the relevant

communication-restricting measures, the execution of such measures, the date on which cooperation is provided, and the targets of such cooperation are entered for a period fixed by Presidential Decree. *<Newly Inserted by Act No. 6546, Dec. 29, 2001>*

(4) In the event that the telephone number or any similar of a person subject to the communication-restricting measures which is entered in the written permission for communication-restricting measures or the emergency wiretapping statement or any similar, is inconsistent with the fact, any of the communications institutions, etc. may refuse to execute the relevant communication-restricting measures and shall be prohibited from divulging secret numbers used for telecommunications in any case. *<Newly Inserted by Act No. 6546, Dec. 29, 2001>*

Article 9-2 (Notice of Execution of Communication-Restricting Measures)

(1) Any prosecutor shall, when he or she institutes a prosecution or takes a disposition not to institute any prosecution or indict in connection with a case involving the execution of the communication-restricting measures in accordance with Articles 6 (1) and 8 (1) (excluding any decision made to suspend any indictment), notify in writing a person subject to the mail censorship in cases of mail censorship and a subscriber to telecommunications who is subject to wiretapping in cases of wiretapping of the fact that the communication-restricting measures are executed, the institution that executes such measures and the period thereof, etc. within 30 days therefrom.

(2) Any judicial police officer shall, when he or she is notified by any prosecutor that the latter institutes a prosecution or takes a disposition not to institute a prosecution or indict anyone in connection with a case involving the execution of the communication-restricting measures under Articles 6 (1) and 8 (1) (excluding any decision made to suspend any indictment) or he or she takes a disposition not to indict anyone in connection with a case of a person under investigation, notify in writing a person subject to the mail censorship in cases of mail censorship and a subscriber to telecommunications who is subject to wiretapping in cases of wiretapping, of the fact that the communication-restricting measures are executed, the institution that executes such measures, and the period thereof, etc. within 30 days therefrom.

(3) The head of any intelligence and investigative agency shall notify in writing a person subject to the mail censorship in cases of mail censorship and a subscriber to telecommunications who is subject to wiretapping in cases of wiretapping, of the fact that the communication-restricting measures are executed, the institution that executes such measures, and the period thereof, etc. within 30 days from the date the communication-restricting measures taken pursuant to the main sentence of Article 7 (1) 1 and Article 8 (1) are completed.

(4) Notwithstanding paragraphs (1) through (3), when any of the following grounds exists, the notice may be deferred until such ground ceases to exist:

1. When the notice of the communication-restricting measures is likely to seriously endanger national security and disrupt the public safety and order;

2. When the notice of the communication-restricting measures is likely to cause grave danger to lives and physical health of people.

(5) Any prosecutor or judicial police officer shall, when he or she intends to defer the notice in accordance with paragraph (4), obtain approval therefor from the head of the District Prosecutor's Office after filing an application therefor, accompanied by the material establishing a prima facie case, with the District Prosecutor's Office: Provided, where any military prosecutor or any military judicial police officer intends to defer the notice in accordance with paragraph (4), he or she shall obtain approval therefor from a senior prosecutor of the competent Prosecutor's Office after filing an application therefor, accompanied by the material establishing a prima facie case, with such Prosecutor's Office. *<Amended by Act No. 13722, Jan. 6, 2016>*

(6) Any prosecutor, judicial police officer or the head of any intelligence and investigative agency shall, when the grounds referred to in the subparagraphs of paragraph (4) cease to exist, serve the notice referred to in paragraphs (1) through (3), within 30 days from the date such grounds cease to exist.

Article 9-3 (Notice of Execution of Confiscation, Search, and Investigations)

(1) Where a prosecutor has executed confiscation, search or investigation into telecommunications the transmission and reception of which have been completed, when he or she has prosecuted such case or conducted disposition (excluding a decision of a stay of prosecution) not to prosecute a case or book a person involved in such case, he or she shall notify, in writing, a subscriber who has become the target of the investigation, of the fact that confiscation, search or investigation has been executed within 30 days from the date such disposition is made.

(2) Where a judicial police officer has executed confiscation, search or investigation into telecommunications the transmission and reception of which have been completed, when he or she receives a notice of disposition that a prosecutor has or has not prosecuted such case; or he or she conducts disposition not to book a person involved in the case on which he or she has conducted an internal investigation, he or she shall notify, in writing, a subscriber who has become the target of the investigation, of the fact that a confiscation, search or inspection has been executed within 30 days from the date such disposition is made.

Article 10 (Authorizing Agencies and Procedures for Wiretapping Equipment Authorization)

(1) Any person who intends to make, import, sell, distribute, possess, use or advertise any wiretapping equipment shall obtain authorization from the Minister of Science and ICT: Provided, That this shall not apply to government agencies. *<Amended by Act No. 5454, Dec. 13, 1997; Act No. 8867, Feb. 29, 2008; Act No. 11690, Mar. 23, 2013; Act No. 14839, Jul. 26, 2017>*

(2) Deleted. *<by Act No. 7138, Jan. 29, 2004>*

(3) Where the Minister of Science and ICT grants authorization under paragraph (1), he or she shall enter the name of the applicant for authorization, the date such authorization is granted, the types and quantities

of authorized wiretapping equipment and other necessary matters into a register and keep it ready. *<Amended by Act No. 5454, Dec. 13, 1997; Act No. 8867, Feb. 29, 2008; Act No. 11690, Mar. 23, 2013; Act No. 14839, Jul. 26, 2017>*

(4) Any person who makes, imports, sells, distributes, possesses, or uses any wiretapping equipment with the authorization under paragraph (1) shall enter the date such authorization is granted, the types and quantities of authorized wiretapping equipment, location where such equipment is installed and other necessary matters into a register and keep it ready: Provided, That the wiretapping equipment furnished to a local government for the performance of its duties, which is a fixture of the local government, shall be recorded in the register for fixtures of the relevant agency.

(5) Other matters necessary for the authorization under paragraph (1) shall be prescribed by Presidential Decree.

Article 10-2 (Report on Wiretapping Equipment Managed by State Organs)

(1) Any State organ (excluding intelligence and investigative agencies) shall, when introducing wiretapping equipment, report its dimensions and performances, including matters prescribed by Presidential Decree, every half year, to the Minister of Science and ICT. *<Amended by Act No. 8867, Feb. 29, 2008; Act No. 11690, Mar. 23, 2013; Act No. 14839, Jul. 26, 2017; Act No. 17347, Jun. 9, 2020>*

(2) Any intelligence and investigative agency shall, when introducing wiretapping equipment, report its dimensions and performances, including matters prescribed by Presidential Decree, every half year, to the Intelligence Committee of the National Assembly. *<Amended by Act No. 17347, Jun. 9, 2020>*

Article 10-3 (Registration of Illegal Wiretapping Equipment Detection Service)

(1) Any person who intends to engage in illegal wiretapping for the purpose of making profits, shall file for registration thereof with the Minister of Science and ICT, as prescribed by Presidential Decree. *<Amended by Act No. 8867, Feb. 29, 2008; Act No. 11690, Mar. 23, 2013; Act No. 14839, Jul. 26, 2017; Act No. 17347, Jun. 9, 2020>*

(2) Registration under paragraph (1) may be filed for only by a juristic person. *<Amended by Act No. 17347, Jun. 9, 2020>*

(3) Any person who intends to file for registration under paragraph (1), shall equip himself or herself with the plans for protecting users, business plans, technology, financial capability, detection equipment, and other necessary matters prescribed by Presidential Decree. *<Amended by Act No. 8867, Feb. 29, 2008; Act No. 17347, Jun. 9, 2020>*

(4) Necessary matters concerning requirements for alteration of registration under paragraph (1) and procedures therefor, the transfer, takeover, succession, suspension, or close-down of registered business and reports thereon, and the delegation, etc. of registered business shall be prescribed by Presidential Decree. *<Amended by Act No. 17347, Jun. 9, 2020>*

Article 10-4 (Grounds for Disqualifying Business Entities Responsible for Detecting Illegal Wiretapping Equipment)

Where the representative of a corporation falls under any of the following, no registration under Article 10-3 shall be filed for: *<Amended by Act No. 7428, Mar. 31, 2005; Act No. 12764, Oct. 15, 2014; Act No. 13591, Dec. 22, 2015; Act No. 17347, Jun. 9, 2020>*

1. A person under adult guardianship or under limited guardianship;
2. A person declared bankrupt and not yet reinstated;
3. A person for whom two years have not elapsed since his or her imprisonment without labor or greater punishment declared by a court was completely executed (including where it is deemed to have been completely executed) or exempted;
4. A person who is under suspension of the execution of his or her imprisonment without labor or greater punishment declared by a court;
5. A person whose qualification is forfeited or suspended by a judgment of a court or by other statutes;
6. A person who was the representative of a corporation as at the time the registration thereof was revoked under Article 10-5 (excluding where the registration was revoked on the ground that the representative fell under subparagraph 1 or 2 of Article 10-4) and for whom two years have not elapsed since the registration was revoked.

Article 10-5 (Revocation of Registration)

Where a person who has filed for registration of illegal wiretapping equipment detection service falls under any of the following cases, the Minister of Science and ICT may either revoke his or her registration or order him or her to suspend the said business for a specified period up to six months: Provided, That in cases falling under subparagraph 1 or 2, the registration shall be revoked: *<Amended by Act No. 8867, Feb. 29, 2008; Act No. 11690, Mar. 23, 2013; Act No. 14839, Jul. 26, 2017; Act No. 17347, Jun. 9, 2020>*

1. Where registration or modified registration has been filed for by fraud or other improper means;
2. Where he or she falls under any of the grounds for disqualification under Article 10-4;
3. Where the secrets known to him or her in connection with business activities are divulged to other persons;
4. Where the certificate of registration of illegal wiretapping equipment detection service has been leased to other persons;
5. Where serious damage has been done to other persons by intention or gross negligence in connection with business activities;
6. The revocation of registration has been requested by the State or local governments under the provisions of other statutes.

Article 11 (Confidentiality Obligation)

(1) Any public official or former public official who has been engaged in the permission, execution, notice, and preparation of various documents, etc. in connection with the communication-restricting measures shall be prohibited from disclosing or divulging matters concerning the communication-restricting measures he or she has learned while performing his or her duties.

(2) The current or former employee of any communications institution shall be prohibited from disclosing or divulging matters concerning the communication-restricting measures.

(3) Any person other than those under paragraphs (1) and (2) shall be prohibited from disclosing or divulging what he or she has learned in connection with the communication-restricting measures except where he or she uses said knowledge according to this Act. *<Amended by Act No. 15493, Mar. 20, 2018>*

(4) Matters necessary to keep secret procedures for granting permission, whether to grant permission, the contents of permission, etc. for the communication-restricting measures by the court shall be prescribed by the Supreme Court Regulations.

Article 12 (Restriction on Using Materials Acquired through Communication-Restricting Measures)

Mail or its contents and contents of any telecommunications acquired through execution of the communication-restricting measures under Article 9 shall not be used except in the following cases:

1. Where they are used to investigate or prosecute the crimes under Article 5 (1) that have become the objective of the communication-restricting measures or the crimes related hereto, or prevent such crimes;
2. Where they are used in disciplinary proceedings for crimes under subparagraph 1;
3. Where a party concerned with communication uses them in a claim for damages;
4. Where they are used under the provisions of other statutes.

Article 12-2 (Management of Materials Acquired through Communication-Restricting Measures on Internet Connections for Criminal Investigation)

(1) Where a prosecutor executes communication-restricting measures under Articles 6 or 8 (limited to emergency communication-restricting measures on persons falling under the requirements under Article 5 (1)) regarding contents of telecommunications transmitted and received through internet connections and intends to use or store for the purpose of using (hereafter in this Article referred to as “storage, etc.”) such contents in accordance with subparagraph 1 of Article 12, he or she shall select the contents of telecommunications requiring storage, etc., and request the approval of the court that had permitted the communication-restricting measure for the storage, etc. within 14 days from the last day of execution.

(2) Where a judicial police officer executes communication-restricting measures under Article 6 or 8 (limited to emergency communication-restricting measures on persons who meet the requirements under Article 5 (1)) and intends to undertake the storage, etc., of the contents of telecommunications, he or she shall select the contents of telecommunications requiring storage, etc., and apply for the approval for the

storage, etc. within 14 days from the last day of execution, and the prosecutor shall request the approval therefor from the court that had permitted the communication-restricting measure within seven days from the application date.

(3) The request for approval under paragraphs (1) and (2) shall be made in writing, stating all the facts and circumstances leading to execution, summary of the materials acquired, and the reasons why storage, etc., are required, together with the following documents:

1. Materials establishing a prima facie case of reasons for the request;
2. A list of contents of telecommunications requiring storage, etc.;
3. Contents of telecommunications requiring storage, etc.: Provided, That the contents of telecommunications shall be submitted by storing such contents in a data storage medium and placing a seal thereon through appropriate means, such as dividing the contents into files of a specific size, etc.

(4) Where the court considers that there are grounds for such request, it shall approve the storage, etc., and issue a document evidencing such approval (hereafter in this Article referred to as “approval document”), and where the court considers that the request is groundless, it shall dismiss such request and give notice thereof to the requestor.

(5) Where any prosecutor or judicial police officer fails to make a request under paragraph (1) or an application under paragraph (2), he or she shall discard the contents of telecommunications acquired through the communication-restricting measures within 14 days (where a judicial police officer’s application is dismissed by a prosecutor, within seven days from such date) from the last day of execution, and where a request for approval is made to the court (including where a request is made only for a part of the contents of telecommunications acquired), any content of telecommunication, for which an approval document is not issued by the court in accordance with paragraph 4, or for which such request is dismissed by the court, shall be discarded within seven days from receipt of notification of dismissal of the request, shall be discarded.

(6) When discarding the contents of telecommunications acquired through the communication-restricting measures in accordance with paragraph (5), a prosecutor or judicial police officer shall prepare a report on the results of discarding, stating, among others, the reasons for, the scope, date and time of discarding, together with the record of investigating a suspect or a person under investigation, and deliver such report to the court that had permitted the communication-restricting measure within seven days from the date of discarding.

Article 13 (Procedures for Provision of Communication Confirmation Data for Criminal Investigations)

(1) Any prosecutor or judicial police officer may, when he or she deems it necessary to conduct any investigation or to execute any punishment, ask any telecommunications business entity under the Telecommunications Business Act (hereinafter referred to as "telecommunications business entity") for perusing or providing the communication confirmation data (hereinafter referred to as "provision of the

communication confirmation data").

(2) Notwithstanding paragraph (1), where any prosecutor or judicial police officer deems that any of the following communication confirmation data is necessary for his or her investigation, he or she may ask any telecommunications business entity for the perusal or the provision of the relevant materials only if it is impracticable to prevent the execution of a crime by other means, to identify and secure a criminal, or to collect and preserve the evidence: Provided, That where the communication confirmation data is required for any crime falling under any of the subparagraphs of Article 5 (1) or any crime committed through means of telecommunications, the request for perusal or provision under paragraph (1) may be made: *<Newly Inserted by Act No. 16849, Dec. 31, 2019>*

1. Data under items (f) and (g) of subparagraph 11 of Article 2 that is realtime tracking data;
2. Communication confirmation data concerning a specific base station.

(3) Any prosecutor or judicial police officer shall, when he or she asks for provision of the communication confirmation data pursuant to paragraphs (1) and (2), obtain permission therefor from the competent district court (including any ordinary military court; hereinafter the same shall apply) or branch court in writing stating the reason for such request, the relation with the relevant subscriber, and the scope of necessary data: Provided, That if the urgent grounds exist that make it impossible to obtain permission from the competent district court or branch court, he or she shall obtain permission without delay after asking for provision of the communication confirmation data and then send it to a telecommunications business entity. *<Amended by Act No. 7503, May 26, 2005; Act No. 16849, Dec. 31, 2019>*

(4) Any prosecutor or any judicial police officer shall, when he or she is provided with communication confirmation data due to the urgent grounds under the proviso of paragraph (3) but fails to obtain permission therefor from the district court or branch court, discard the communication confirmation data provided to him or her without delay. *<Amended by Act No. 7503, May 26, 2005; Act No. 16849, Dec. 31, 2019>*

(5) Any prosecutor or judicial police officer shall, when he or she is supplied with the communication confirmation data under paragraph (3), keep records in which necessary matters, including the fact that the request for provision of the relevant communication confirmation data is made, are entered and other relevant materials, including the written request for provision of the communication conformation data, at the institution to which he or she belongs. *<Amended by Act No. 7503, May 26, 2005; Act No. 16849, Dec. 31, 2019>*

(6) The district court or branch court shall preserve records with respect to the status of receiving requests for permission to provide the communication confirmation data, the status of granting such permission, and other materials related thereto under paragraph (3). *<Amended by Act No. 7503, May 26, 2005; Act No. 16849, Dec. 31, 2019>*

(7) When a telecommunications business entity provides any prosecutor, any judicial police officer, or the head of any intelligence and investigative agency with the communication confirmation data, he or she shall make a report on the status of providing the communication confirmation data twice a year to the Minister of Science and ICT; and shall keep records in which necessary matters, including the provision of

the corresponding communication confirmation data, are entered and other materials related to requests for provision of the communication confirmation data, etc. for seven years from the date each of such communication confirmation data is provided. *<Amended by Act No. 8867, Feb. 29, 2008; Act No. 11690, Mar. 23, 2013; Act No. 14839, Jul. 26, 2017; Act No. 16849, Dec. 31, 2019>*

(8) The Minister of Science and ICT may check the authenticity of reports filed by telecommunications business entities pursuant to paragraph (7) and the status of management of related materials, including records which need to be kept by them. *<Amended by Act No. 8867, Feb. 29, 2008; Act No. 11690, Mar. 23, 2013; Act No. 14839, Jul. 26, 2017; Act No. 16849, Dec. 31, 2019>*

(9) Except as provided in this Act, Article 6 (excluding paragraphs (7) and (8)) shall apply mutatis mutandis to the matters related to providing the communication confirmation data for the criminal investigations. *<Newly Inserted by Act No. 7503, May 26, 2005; Act No. 16849, Dec. 31, 2019>*

Article 13-2 (Provision of Communication Confirmation Data to Court)

When it is deemed necessary for trial, any court may ask any telecommunications business entity to provide the communication confirmation data under Article 294 of the Civil Procedure Act or Article 272 of the Criminal Procedure Act. *<Amended by Act No. 6626, Jan. 26, 2002>*

Article 13-3 (Notification of Provision of Communication Confirmation Data for Criminal Investigations)

(1) With respect to any case in which communication confirmation data is received pursuant to Article 13, a prosecutor or judicial police officer shall send a written notice of the fact that communication confirmation data is provided, the agency requesting the provision, and the relevant period, etc., within the following time periods to the person, who is the subject of such communication confirmation data: *<Amended by Act No. 16849, Dec. 31, 2019>*

1. Where any public prosecution is instituted or a disposition of not instituting a public prosecution or booking (excluding a decision of the suspension of prosecution, or decision of the suspension of reference witness) is taken: Within 30 days from the date said disposition is taken;
2. Where a disposition to suspend prosecution or reference witness is taken: Within 30 days from the date one year (in the case of crimes falling under any of the subparagraphs of Article 6 (8), three years) after said disposition is taken;
3. Where the investigation is still ongoing: Within 30 days from the date one year (in the case of crimes falling under any of the subparagraphs of Article 6 (8), three years) after the communication confirmation data is received.

(2) Notwithstanding subparagraphs 2 and 3 of paragraph (1), in any case falling under any of the following subparagraphs, the notice under the same paragraph may be deferred until such cause is resolved: *<Newly inserted by Act No. 16849, Dec. 31, 2019>*

1. Where national security, and public safety and order are likely to be endangered;

2. Where the lives or physical safety of the victims or other related parties in the case are likely to be jeopardized;

3. Where the implementation of a fair judicial process is likely to be hindered by the destruction of evidence, escape, threatening of witnesses, etc.;

4. Where the name or privacy of the suspect, victim or other related parties in the case are likely to be infringed upon.

(3) Any prosecutor or judicial police officer who intends to defer notice pursuant to paragraph (2) shall attach the materials establishing a prima facie case, and obtain the approval of the head of the competent District Prosecutor's Office in advance. *<Newly Inserted by Act No. 16849, Dec. 31, 2019>*

(4) Where any cause under the subparagraphs of paragraph (2) is resolved, the prosecutor or judicial police officer shall send the notice under paragraph (1) within 30 days from the date such cause is resolved. *<Newly Inserted by Act No. 16849, Dec. 31, 2019>*

(5) Any person receiving a notice of the fact, among others, of provision of communication confirmation data from a prosecutor or judicial police officer pursuant to paragraph (1) or (4) may file a written application seeking reasons for requesting the relevant communication confirmation data. *<Newly Inserted by Act No. 16849, Dec. 31, 2019>*

(6) Any prosecutor or judicial police officer who has received an application under paragraph (5) shall notify in writing the reasons for requesting provision of communication confirmation data within 30 days from the date of receipt of application, unless there are causes falling under any of the subparagraphs of paragraph (2). *<Newly Inserted by Act No. 16849, Dec. 31, 2019>*

(7) Except as provided in paragraphs (1) through (5), Article 9-2 (excluding paragraph (3) of said Article) shall apply mutatis mutandis to the facts, etc. of provision of communication confirmation data.

Article 13-4 (Procedures for Providing Communication Confirmation Data for National Security)

(1) Where the collection of information is necessary for preventing threats to national security, the head of any intelligence and investigative agency may request any telecommunications business entity to provide the communication confirmation data.

(2) Articles 7 through 9 and 9-2 (3), (4), and (6) shall apply mutatis mutandis to the procedures, etc. for providing communication confirmation data under paragraph (1). In such cases, the "communication restriction measures" shall be deemed the "request for providing communication confirmation data".

(3) Article 13 (4) and (5) shall apply mutatis mutandis to discarding communication confirmation data and keeping related data. *<Amended by Act No. 16849, Dec. 31, 2019>*

Article 13-5 (Confidentiality and Restrictions on Using Data)

@Articles 11 and 12 shall apply mutatis mutandis to providing communication confirmation data under Article 13, and obligations of confidentiality and the restrictions on using data following providing

communication confirmation data under Article 13-4, respectively.

Article 14 (Prohibition of Infringement of Others' Conversation Secrets)

(1) No person shall record a conversation between others that is not open to the public or listen to it through the employment of electronic or mechanical devices.

(2) Articles 4 through 8, the former part of Article 9 (1), and Articles 9 (3), 9-2, 11 (1), (3) and (4) and 12 shall apply to recording or listening as referred to in paragraph (1). *<Amended by Act No. 6546, Dec. 29, 2001>*

Article 15 (Control of the National Assembly)

(1) Any of the standing committees and any committee for inspection and investigation of state administration of the National Assembly may, when it is deemed necessary, ask the Minister of Court Administration or the heads of agencies or institutions that have filed requests or applications for the communication-restricting measures or have executed such communication-restricting measures to file a report on any specific communication-restricting measures, etc., and ask the Minister of Science and ICT to file a report detailing wiretapping equipment authorized and reports filed in connection with such wiretapping equipment, respectively. *<Amended by Act No. 8867, Feb. 29, 2008; Act No. 11690, Mar. 23, 2013; Act No. 14839, Jul. 26, 2017>*

(2) Any of the standing committees and any committee for inspection and investigation of state administration of the National Assembly may, by a resolution, conduct on-the-spot inspection or other inspection of wiretapping equipment currently possessed by investigative agencies, telephone switchboard rooms and other places of agencies that have executed the wiretapping or institutions that have cooperated in wiretapping. In such cases, any person participating in the on-the-spot inspection and other inspection shall be prohibited from divulging secrets he or she has learned therefrom without any good cause.

(3) The on-the-spot investigation or other investigations under paragraph (2) shall not be conducted for the purpose of violating any person's privacy or intervening in any pending trial or the prosecution of a case under investigation.

(4) The head of any central administrative agency that has executed the communication-restricting measures, has been commissioned to execute such communication-restricting measures or has cooperated in executing the communication-restricting measures shall, upon receipt of a request from any standing committee or any committee for inspection and investigation of state administration of the National Assembly, file a report on the communication-restricting measures related to Articles 5 through 10 to the National Assembly as prescribed by Presidential Decree: Provided, That the head of any intelligence and investigative agency shall file such report with the Intelligence Committee of the National Assembly.

Article 15-2 (Telecommunications Business Entities’ Obligation to Cooperate)

(1) Telecommunications business entities shall cooperate in the communication-restricting measures and the request for provision of communication confirmation data taken and made under this Act by any prosecutor, judicial police officer or the head of any intelligence and investigative agency.

(2) Matters necessary for the cooperation by telecommunication business entities for the execution of communication-restricting measures under paragraph (1), the period for keeping communication confirmation data and other matters for the cooperation of telecommunication business entities, shall be prescribed by Presidential Decree.

Article 16 (Penalty Provisions)

(1) Any of the following persons shall be punished by imprisonment with labor for not less than one year but not more than 10 years or by suspension of qualification for not more than five years: *<Amended by Act No. 12229, Jan, 14, 2014; Act No. 15493, Mar. 20, 2018>*

1. A person who has censored any mail, wiretapped any telecommunications or recorded or eavesdropped on any conversations between other individuals in violation of Article 3;
2. A person who has disclosed or divulged the contents of communications or conversations he or she has learned in a manner under subparagraph 1.

(2) Any of the following persons shall be punished by imprisonment with labor for not more than 10 years: *<Amended by Act No. 7503, May 26, 2005>*

1. A person who has commissioned the execution of communication-restricting measures or asked for cooperation in the execution of such communication-restricting measures without delivering a written permission for communication-restricting measures or a copy of the cover of an emergency wiretapping statement; or any other person who has executed the commissioned communication-restricting measures or cooperated in the execution of such communication-restricting measures without receiving a written permission for communication-restricting measures or a copy of the cover of an emergency wiretapping statement in violation of Article 9 (2);
2. A person who has violated Article 11 (1) (including a person to whom Article 14 (2) shall apply and to whom Article 13-5 shall apply mutatis mutandis).

(3) Any person who has violated Article 11 (2) (including a person to whom Article 13-5 shall apply mutatis mutandis) shall be punished by imprisonment with labor for not more than seven years. *<Amended by Act No. 7503, May 26, 2005>*

(4) Any person who has violated Article 11 (3) (including a person to whom Article 14 (2) shall apply and to whom Article 13-5 shall apply mutatis mutandis) shall be punished by imprisonment with labor for not more than five years. *<Amended by Act No. 7503, May 26, 2005>*

Article 17 (Penalty Provisions)

(1) Any of the following persons shall be punished by imprisonment with labor for not more than five years or by a fine not exceeding 30 million won: *<Amended by Act No. 7138, Jan. 29, 2004; Act No. 15493,*

Mar. 20, 2018>

1. A person who has failed to keep a cover copy of a written permission for communication-restricting measures or an emergency wiretapping statement, etc. in violation of Article 9 (2);

2. A person who has failed to keep records in violation of Article 9 (3) (including a person to whom Article 14 (2) shall apply);

3. A person who has failed to confirm a telephone number of any person subject to the communication-restricting measures which is entered in the written permission for communication-restricting measures or the emergency wiretapping statement, or divulged any password used for telecommunications in violation of Article 9 (4);

4. A person who has manufactured, imported, sold, distributed, possessed or used wiretapping equipment, and advertised them for the aforementioned purposes without obtaining authorization therefor in violation of Article 10 (1);

5. A person who has failed to make or keep authorization records of wiretapping equipment in violation of Article 10 (3) and (4);

5-2. A person who has engaged in detecting illegal wiretapping equipment either by failing to file for registration under Article 10-3 (1), or by filing for false registration;

6. Deleted. *<by Act No. 15493, Mar. 20, 2018>*

(2) Any of the following persons shall be punished by imprisonment with labor for not more than three years or by a fine not exceeding 10 million won: *<Amended by Act No. 7138, Jan. 29, 2004; Act No. 8867, Feb. 29, 2008; Act No. 11690, Mar. 23, 2013; Act No. 14839, Jul. 26, 2017; Act No. 16849, Dec. 31, 2019>*

1. A person who has given or received an electronic serial number in violation of Article 3 (3);

2. A person who has failed to discontinue immediately the emergency communication-restricting measures in violation of the latter part of Article 8 (2) or the latter part of Article 8 (9);

3. A person who has failed to give notice with respect to the execution of the communication-restricting measures in violation of Article 9-2 (including a person to whom Article 14 (2) shall apply);

4. A person who has failed to report the current status of the provision of communication confirmation data, etc. to the Minister of Science and ICT or to keep relevant materials in violation of Article 13 (7).

Article 18 (Attempted Crime)

A person who attempts to commit the crimes prescribed in Articles 16 and 17 shall be punished.

ADDENDA *<Act No. 4650, Dec. 27, 1993>*

(1) (Enforcement Date) This Act shall enter into force six months after the date of its promulgation.

(2) (Repealed Statute) The Temporary Post Control Act is hereby repealed.

(3) (Transitional Measures) A person carrying or using any wiretapping equipment who is subject to authorization as at the time this Act enters into force, shall, with the authorization referred to in Article 10, prepare and keep a register within three months after the date this Act enters into force; and a person who

violates it shall be governed by subparagraph 2 of Article 17.

ADDENDUM *<Act No. 5454, Dec. 13, 1997>*

This Act shall enter into force on January 1, 1998. (Proviso Omitted.)

ADDENDA *<Act No. 5681, Jan. 21, 1999>*

Article 1 (Enforcement Date)

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

Articles 2 through 4 Omitted.

ADDENDA *<Act No. 6146, Jan. 12, 2000>*

Article 1 (Enforcement Date)

This Act shall enter into force on July 1, 2000.

Articles 2 through 9 Omitted.

ADDENDA *<Act No. 6305, Dec. 29, 2000>*

Article 1 (Enforcement Date)

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

Articles 2 through 8 Omitted.

ADDENDA *<Act No. 6346, Jan. 8, 2001>*

(1) (Enforcement Date) This Act shall enter into force three months after the date of its promulgation. (Proviso Omitted.)

(2) Omitted.

ADDENDA *<Act No. 6546, Dec. 29, 2001>*

Article 1 (Enforcement Date)

This Act shall enter into force three months after the date of its promulgation.

Article 2 (Applicability)

(1) The amended provisions of Articles 5 (1), 6 (1) through (7), 7 (1) through (3), 8, 9, 9-2, and 14 (2) shall begin to apply from the first communication-restricting measures for which a request is filed for

permission or approval (including where a judicial police officer files such request) or whose execution commences after this Act enters into force.

(2) The amended provisions of Articles 13 and 13-2 shall begin to apply from the first communication confirmation data for which a request is filed for approval therefor or provision thereof after the date this Act enters into force.

Article 3 (Transitional Measures concerning Wiretapping Equipment of State Organs)

Any State organ that is in possession of wiretapping equipment as at the time this Act enters into force shall file a report thereon to the Minister of Information and Communication or notify the Intelligence Committee of the National Assembly in accordance with the amended provisions of Article 10-2 within three months after the date this Act enters into force.

Article 4 (Transitional Measures concerning Penalty Provisions)

The previous provisions shall apply to the imposition of penalty provisions for acts committed before this Act enters into force.

ADDENDA *<Act No. 6626, Jan. 26, 2002>*

Article 1 (Enforcement Date)

This Act shall enter into force on July 1, 2002.

Articles 2 through 7 Omitted.

ADDENDA *<Act No. 7138, Jan. 29, 2004>*

(1) (Enforcement Date) This Act shall enter into force on the date of its promulgation: Provided, That the amended provisions of Article 10-3 shall enter into force six months after the date of its promulgation.

(2) (Transitional Measures) A person who engages in the business of detecting illegal wiretapping equipment as at the time this Act enters into force shall file for registration under the amended provisions of Article 10-3 within six months from the date this Act enters into force.

ADDENDUM *<Act No. 7371, Jan. 27, 2005>*

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

ADDENDA *<Act No. 7428, Mar. 31, 2005>*

Article 1 (Enforcement Date)

This Act shall enter into force one year after the date of its promulgation.

Articles 2 through 6 Omitted.

ADDENDUM *<Act No. 7503, May 26, 2005>*

This Act shall enter into force three months after the date of its promulgation.

ADDENDA *<Act No. 8728, Dec. 21, 2007>*

Article 1 (Enforcement Date)

This Act shall enter into force one year after the date of its promulgation.

Articles 2 through 6 Omitted.

ADDENDA *<Act No. 8733, Dec. 21, 2007>*

Article 1 (Enforcement Date)

This Act shall enter into force nine months after the date of its promulgation. (Proviso Omitted.)

Articles 2 through 11 Omitted.

ADDENDA *<Act No. 8867, Feb. 29, 2008>*

Article 1 (Enforcement Date)

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

Articles 2 through 12 Omitted.

ADDENDA *<Act No. 9752, May 28, 2009>*

(1) (Enforcement Date) This Act shall enter into force on the date of its promulgation.

(2) (Applicability) The amended provisions of Article 9-3 shall begin to apply from the first confiscation, search or investigation executed after this Act enters into force.

ADDENDA *<Act No. 9819, Nov. 2, 2009>*

Article 1 (Enforcement Date)

This Act shall enter into force six months after the date of its promulgation.

Articles 2 through 6 Omitted.

ADDENDA <*Act No. 11690, Mar. 23, 2013*>

Article 1 (Enforcement Date)

(1) This Act shall enter into force on the date of its promulgation.

(2) Omitted.

Articles 2 through 7 Omitted.

ADDENDA <*Act No. 11731, Apr. 5, 2013*>

Article 1 (Enforcement Date)

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

Articles 2 and 3 Omitted.

ADDENDUM <*Act No. 12229, Jan. 14, 2014*>

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

ADDENDA <*Act No. 12764, Oct. 15, 2014*>

Article 1 (Enforcement Date)

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

Article 2 (Transitional Measures concerning Grounds for Disqualification of Incompetent Persons)

Notwithstanding the amended provision of subparagraph 1 of Article 10-4, the previous provisions shall apply to persons for whom the declaration of incompetency or quasi-incompetency pronounced as at the time the aforementioned amended provision enters into force, remains effective under Article 2 of the Addenda to the Civil Act (Act No. 10429).

ADDENDA <*Act No. 12960, Jan. 6, 2015*>

Article 1 (Enforcement Date)

This Act shall enter into force one year after the date of its promulgation.

Articles 2 through 6 Omitted.

ADDENDUM <*Act No. 13591, Dec. 22, 2015*>

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

ADDENDA <*Act No. 13717, Jan. 6, 2016*>

Article 1 (Enforcement Date)

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

Articles 2 and 3 Omitted.

ADDENDA <*Act No. 13719, Jan. 6, 2016*>

Article 1 (Enforcement Date)

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

Articles 2 and 3 Omitted.

ADDENDA <*Act No. 13722, Jan. 6, 2016*>

Article 1 (Enforcement Date)

This Act shall enter into force one year and six months after the date of its promulgation.

Articles 2 through 10 Omitted.

ADDENDA <*Act No. 14071, Mar. 3, 2016*>

Article 1 (Enforcement Date)

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

Article 2 Omitted.

ADDENDA <*Act No. 14839, Jul. 26, 2017*>

Article 1 (Enforcement Date)

(1) This Act shall enter into force on the date of its promulgation: Provided, That the amendments to the statutes to be amended pursuant to Article 5 of the Addenda, which were promulgated before this Act enters into force, but the dates on which they are to enter into force, have yet to arrive, shall enter into force on the enforcement date of the relevant statute.

Articles 2 through 6 Omitted.

ADDENDUM <*Act No. 15493, Mar. 20, 2018*>

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

ADDENDUM <*Act No. 16849, Dec. 31, 2019*>

Article 1 (Enforcement Date)

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

Article 2 (Applicability regarding Extension of Communication-Restricting Measures)

The amended provisions of the proviso of Article 6 (7) and Article 6 (8) shall begin to apply for extensions of communication-restricting measures for which a request is filed for permission after this Act enters into force.

Article 3 (Applicability regarding Provision of Communication Confirmation Data and Notice of the Fact of Provision)

The amended provisions of Articles 13 (2) and 13-3 (1) through (6) shall apply for the provision of communication confirmation data for which a request is filed after this Act enters into force.

ADDENDUM <*Act No. 17090, Mar. 24, 2020*>

Article 1 (Enforcement Date)

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

Article 2 (Applicability regarding Management of Materials Acquired through Communication-Restricting Measures on Internet Connections for Criminal Investigation)

The amended provisions of Article 12-2 shall begin to apply for communication-restricting measures on telecommunications transmitted and received through internet connections for which a request is filed after this Act enters into force.

ADDENDA <*Act No. 17125, Mar. 24, 2020*>

Article 1 (Enforcement Date)

This Act shall enter into force on February 9, 2021. (Proviso Omitted.)

Articles 2 through 4 Omitted.

ADDENDUM <*Act No. 17347, Jun. 9, 2020*>

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