PIPC Notification No. 2020-10 (2020.9.1.)
PIPC Notification No. 2021-1 (2021.1.21.)
PIPC Notification No. 2021-5 (2021.11.16.)

Supplementary rules for the interpretation and application of the Personal Information Protection Act related to the processing of personal data transferred to Korea

2020.1.21.

Personal Information Protection Commission

Contents

I Outline

Korea and the European Union (hereinafter referred to as the 'EU') have been engaged in adequacy discussions, as a result of which the European Commission determined that Korea is guaranteeing an adequate level of personal data protection according to Article 45 of GDPR.

In this context, the Personal Information Protection Commission adopted this Notification based on Article 5 (Obligations of State, etc). and Article 14 (International Cooperation)[1] of the Personal Information Protection Act to clarify the interpretation, application and enforcement of certain provisions of the Act, including in regard to the processing of personal data transferred to Korea based on the EU adequacy decision.

As this Notification has the status of an administrative rule that the competent administrative agency establishes and announces to clarify the standards for interpreting, applying and enforcing the 「Personal Information Protection Act」 in the legal system of Korea, it has legally binding force on the personal information controller in the sense that any violation of this Notification may be regarded as a violation of the relevant provisions of PIPA. In addition, if personal rights and interests are infringed due to a violation of this Notification, relevant individuals are entitled to obtain redress from the Personal Information Protection Commission or the court.

Accordingly, if the personal information controller, who processes the personal information transferred to Korea according to the EU adequacy decision, fails to take measures conforming to this Notification, it will be deemed "that there is substantial ground to deem that there has been an infringement with respect to personal information, and failure to take action is likely cause damage that is difficult to remedy", pursuant to Paragraphs 1 and 2 of Article 64 of the Act. In such cases, the Personal Information Protection Commission or related central administrative agencies may order the relevant personal information controller to take corrective measures, etc. according to the authority given by this provision, and, depending on specific violations of the law, corresponding punishment (penalties, administrative fines, etc.) may be imposed as well.

[1] Article 14 of the 「Personal Information Protection Act」 stipulates the Korean Government's authority to establish policies to improve the level of personal information protection in the international environment and prevent the infringement of the rights of data subjects due to the cross-border transfer of personal information.

II Definitions of terms

The definitions of the terms used in this provision are as follows:

(i). Act: Personal Information Protection Act (Act No. 16930, amended on February 4, 2020, and enforced on August 5, 2020)

(ii). Presidential Decree: Enforcement Decree of the Personal Information Protection Act (Presidential Decree No. 30509, 03. Mar, 2020., Amends Other Acts)

(iii). Data subject: an individual who is identifiable by the information processed hereby to become the subject of that information

(iv). Personal information controller: a public institution, legal person, organization, individual, etc. that processes personal information directly or indirectly to operate the personal information files for business purposes;

(v). EU: EU (As of the end of February 2020, 27 member countries[2], including Belgium, Germany, France, Italy, Luxemburg, the Netherlands, Denmark, Ireland, Greece, Portugal, Spain, Austria, Finland, Sweden, Cyprus, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia, Slovenia, Rumania, Bulgaria and Croatia) as well as countries associated to the EU through the EEA Agreement (Iceland, Liechtenstein, Norway).

(vi). GDPR: The EU's general personal information protection law, General Data Protection Regulation (Regulation EU 2016/679)

(vii). Adequacy decision: According to Paragraph 3 of Article 45 of GDPR, the European Commission decided that a third country, the territory of a third country, one or more areas or an international organization guarantees an adequate level of personal

[2] Until the end of the transition period, this also includes the United Kingdom, as provided by Articles 126, 127 and 132 of the Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community (2019/C 384 I/01).

information protection.

III Supplementary rules

1. Limitation to Out-of-Purpose Use and Provision of Personal Information (Articles 3, 15 and 18 of the Act)

<Personal Information Protection Act
(Act No. 16930, partially amended on February 4, 2020)>

Article 3 (Principles for Protecting Personal Information) (1) The personal information controller shall specify explicitly the purposes for which personal information is processed; and shall collect personal information lawfully and fairly to the minimum extent necessary for such purposes.

(2) The personal information controller shall process personal information in an appropriate manner necessary for the purposes for which the personal information is processed, and shall not use it beyond such purposes.

Article 15 (Collection and Use of Personal Information) (1) A personal information controller may collect personal information in any of the following circumstances, and use it with the scope of the purpose of collection:

1. Where consent is obtained from a data subject;
2. Where special provisions exist in laws or it is inevitable to observe legal obligations;
3. Where it is inevitable for a public institution's performance of its duties under its jurisdiction as prescribed by statutes, etc.;
4. Where it is inevitably necessary to execute and perform a contract with a data subject;
5. Where it is deemed manifestly necessary for the protection of life, bodily or property interests of the data subject or third party from imminent danger where the data subject or his or her legal representative is not in a position to express intention, or prior consent cannot be obtained owing to unknown addresses, etc.;
6. Where it is necessary to attain the justifiable interest of a personal information controller, which such interest is manifestly superior to the rights of the data subject. In such cases, processing shall be allowed only to the extent the processing is substantially related to the justifiable interest of the personal information controller and does not go beyond a reasonable scope.

Article 18 (Limitation to Out-of-Purpose Use and Provision of Personal Information) (1) A personal information controller shall not use personal information beyond the scope

provided for in Articles 15 (1) and 39-3 (1) and (2), or provide it to any third party beyond the scope provided for in Article 17 (1) and (3).

(2) Notwithstanding paragraph (1), where any of the following subparagraphs applies, a personal information controller may use personal information or provide it to a third party for other purposes, unless doing so is likely to unfairly infringe on the interest of a data subject or third party: Provided, That information and communications service providers [as set forth in Article 2 (1) 3 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.; hereinafter the same shall apply] processing the personal information of users [as set forth in Article 2 (1) 4 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.; hereinafter the same shall apply] are only subject to subparagraphs 1 and 2, and subparagraphs 5 through 9 are applicable only to public institutions:

1. Where additional consent is obtained from the data subject;
2. Where special provisions in other laws so require;
3. Where it is deemed manifestly necessary for the protection of life, bodily or property interests of the data subject or third party from imminent danger where the data subject or his or her legal representative is not in a position to express intention, or prior consent cannot be obtained owing to unknown addresses;
4. Deleted;<by Act No. 16930, Feb. 4, 2020>
5. Where it is impossible to perform the duties under its jurisdiction as provided for in any Act, unless the personal information controller uses personal information for other purpose than the intended one, or provides it to a third party, and it is subject to the deliberation and resolution by the Commission;
6. Where it is necessary to provide personal information to a foreign government or international organization to perform a treaty or other international convention;
7. Where it is necessary for the investigation of a crime, indictment and prosecution;
8. Where it is necessary for a court to proceed with trial-related duties;
9. Where it is necessary for the enforcement of punishment, probation and custody.

omitted (3) ~ (4) (5) Where a personal information controller provides personal information to a third party for other purpose than the intended one in any case provided for in paragraph (2), the personal information controller shall request the recipient of the personal information to limit the purpose and method of use and other necessary matters,

or to prepare necessary safeguards to ensure the safety of the personal information. In such cases, the person in receipt of such request shall take necessary measures to ensure the safety of the personal information.

(i) Paragraphs 1 and 3 of Article 3 of the Act prescribe the principle that a personal information controller must collect only the minimum personal information necessary for performing the purpose of processing the personal information legally and lawfully, and should not use it for purposes other than the intended one.

(ii) According to this principle, Paragraph 1 of Article 15 of the Act prescribes that when a personal information controller collects personal information, personal information may be used within the purpose of collection, and Paragraph 1 of Article 18 prescribes that personal information should not be used beyond the purpose of collection or provided to a third party.

(iii) Also, even if personal information may be used for purposes other than the intended one or provided to a third party in the exceptional cases[3] described in the subparagraphs of Paragraph 2 of Article 18 of the Act, it must be requested that the purpose or method of use should be restricted so that personal information can be processed safely according to Paragraph 5, or measures necessary for ensuring the safety of personal information should be taken.

(iv). The above provisions shall be applied equally to the processing of all personal information received within the area of Korea's legal jurisdiction from a third country, regardless of the nationality of the data subject.

(v). For instance, if a personal information controller in the EU transfers personal information to a Korean personal information controller according to the adequacy decision of the European Commission, the EU personal information controller's purpose of transferring the personal information shall be regarded as the Korean personal information controller's purpose of collecting personal information, and in such cases, the Korean personal information controller may only use the personal information or provide it to a third party within the purpose of collection except for the exceptional cases described in the subparagraphs of Paragraph 2 of Article 18 of the Act.

[3] Information communication service providers are only subject to Article 18(2) subparagraphs 1 and 2. Subparagraphs 5 through 9 are applicable only to public institutions.

2. **Limitation to Onward transfer of Personal data (Articles 17(3) (4), Article 18 of the Act)**

<Personal Information Protection Act

(Act No. 16930, partially amended on February 4, 2020)>

Article 17 (Provision of Personal Information) (1) omit

(2) A personal information controller shall inform a data subject of the following matters when it obtains the consent under paragraph (1) 1. The same shall apply when any of the following is modified:

1. The recipient of personal information;
2. The purpose for which the recipient of personal information uses such information;
3. Particulars of personal information to be provided;
4. The period during which the recipient retains and uses personal information;
5. The fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent.

(3) A personal information controller shall inform a data subject of the matters provided for in paragraph (2), and obtain the consent from the data subject in order to provide personal information to a third party overseas; and shall not enter into a contract for the cross-border transfer of personal information in violation of this Act.

(4) A personal information controller may provide personal information without the consent of a data subject within the scope reasonably related to the purposes for which the personal information was initially collected, in accordance with the matters prescribed by Presidential Decree taking into consideration whether disadvantages are caused to the data subject, whether necessary measures to secure safety, such as encryption, have been taken, etc.

※ Please see pages 3, 4 and 5 for Article 18

< Enforcement Decree of the Personal Information Protection Act

([Enforcement Date 05. Feb, 2021.] [Presidential Decree No. 30892, 04.Aug, 2020., Amends Other Acts])>

Article 14-2 (Standards on Additional Use/Provision of Personal Information, etc.)

(1) If a personal information controller uses or provides personal information (hereinafter referred to as "additional use or provision of personal information") without the consent of the data subject in accordance with Article 15 (3) of the Act or

Article 17 (4) of the Act, the personal information controller shall consider the following matters:

1. Whether it is reasonably related to the original purpose for which the personal information was collected;

2. Whether additional use or provision of personal information is foreseeable in light of the circumstances under which the personal information was collected and processing practices;

3. Whether additional use or provision of personal information does not unfairly infringe on the interests of the data subject; and

4. Whether the measures required to ensure security such as pseudonymization or encryption have been taken.

(2) The personal information controller shall disclose in advance the criteria for assessing the matters referred to in the subparagraphs of paragraph (1) in the Privacy Policy under Article 30 (1) of the Act, and the privacy officer under Article 31 (1) of the Act shall check whether the personal information controller is using or providing additional personal information in accordance with the relevant standards.

(i). If the personal information controller provides personal information to a third party overseas, he/she must inform data subjects in advance of all the matters described in Article 17(2) of the Act and obtain their consent, except for cases falling under (1) or (2). No contract should be entered concerning cross-border provision of personal data in violation of this Act.

(1) If personal information is provided within the scope reasonably related to the initial purpose of collection according to Paragraph 4 of Article 17 of the Act. However, the cases to which this provision can be applied are limited to cases where the standards for additional use and provision of personal information, prescribed in Article 14-2 of the Enforcement Decree, are met. In addition, the personal information controller must consider whether the provision of personal information may cause disadvantages to data subjects, and whether he/she has taken necessary measures for securing safety, such as encryption.

(2) If personal information can be provided to a third party in exceptional cases mentioned in Paragraph 2 of Article 18 of the Act (see pages 3~5). However even in such cases, if the provision of such personal information is likely to unfairly infringe the interests of the data subject or a third party, personal information cannot be provided to a third party. Moreover, the provider of personal information must request the recipient of personal information to limit the purpose or method of using the personal information or take measures necessary for ensuring the safety thereof so that the personal information can be processed safely.

(ii) If personal information is provided to a third party overseas, it may not receive the level of protection guaranteed by the Personal Information Protection Act of Korea due to differences in personal information protection systems of different countries. Accordingly, such cases will be deemed as ‘cases where disadvantages may be caused to the data subject’ mentioned in Paragraph 4 of Article 17 of the Act or ‘cases where the interest of a data subject or third party is infringed unfairly’ mentioned in Paragraph 2 of Article 18 of the Act and Article 14-2 of the Enforcement Decree of the same Act. In such cases, the personal information controller and third party must explicitly ensure a level of protection equivalent to the Act, including the guarantee of the data subject’s exercise of his/her rights in legally binding documents such as contracts, even after personal information is transferred overseas.

3. Notification for the data where personal data have not been obtained from the data subject (Article 20 of the Act)

<Personal Information Protection Act

(Act No. 16930, partially amended on February 4, 2020)>

Article 20 (Notification on Sources, etc. of Personal Information Collected from Third Parties) (1) When a personal information controller processes personal information collected from third parties, the personal information controller shall immediately notify the data subject of the following matters at the request of such data subject:

1. The source of collected personal information;

2. The purpose of processing personal information;

3. The fact that the data subject is entitled to demand suspension of processing of personal information, as prescribed in Article 37.

(2) Notwithstanding paragraph (1), when a personal information controller satisfying the criteria prescribed by Presidential Decree taking into account the types and amount of processed personal information, number of employees, amount of sales, etc., collects personal information from third parties and processes the same pursuant to Article 17 (1) 1, the personal information controller shall notify the data subject of the matters referred to in paragraph (1): Provided, That this shall not apply where the information collected by the personal information controller does not contain any personal information, such as contact information, through which notification can be given to the data subject.

(3) Necessary matters in relation to the time, method, and procedure of giving notification to the data subject pursuant to the main sentence of paragraph (2), shall be prescribed by Presidential Decree.

(4) Paragraph (1) and the main clause of paragraph (2) shall not apply to any of the following circumstances: Provided, That this shall be the case only where it is manifestly superior to the rights of data subjects under this Act:

1. Where personal information, which is subject to a notification request, is included in the personal information files referred to in any of the subparagraphs of Article 32 (2);

2. Where such notification is likely to cause harm to the life or body of any other person, or unfairly damages the property and other interests of any other person.

(i). If the personal information controller receives the personal information transferred from the EU based on its adequacy decision, he/she must notify the following information (1) through (5) to the data subject without undue delay, and in any event not later than one month from the transfer.

(1) The name and contact information of the persons who transfer and receive the personal information.

(2) The items or categories of the personal information transferred.

(3) The purpose of collecting and using the personal information (as set by data exporter pursuant to point 1 of this Notification).

(4) The personal information retention period.

(5) Information on the data subject's rights in regard to the processing of the personal information, the method and procedure of exercising the rights and any disadvantages if the exercise thereof causes disadvantages.

(ii) Also, if the personal information controller provides the personal information in (i) to a third party in the Republic of Korea or abroad, he/she must notify the information (1) through (5) to the data subject before the personal information is provided.

(1) The name and contact information of the persons who provide and receive the personal information.

(2) The items or categories of the personal information provided.

(3) The country to which the personal information shall be provided, the envisaged date and method of providing it (limited to cases where personal information shall be provided to a third party overseas).

(4) The personal information provider's purpose and legal basis of providing the personal information

(5) Information on the data subject's rights in regard to the processing of personal information, the method and procedure of exercising the rights, and any disadvantages if the exercise thereof causes disadvantages.

(iii) The personal information controller may not apply (i) or (ii) in any of the following cases (1) through (4).

(1) If the personal information that needs to be notified is included in any of the following personal information files mentioned in Paragraph 2 of Article 32 of the Act, to the extent that the interests protected by this provision are manifestly superior to the rights of the data subject, and only as long as the notification would threaten the pursuit of the interests at stake, for instance jeopardizing ongoing criminal investigations or threatening national security.

(2) If and for as long as the notification is likely to harm the life or body of another person, or unfairly infringe on the property interests of another person, where those rights or interests are manifestly superior to the rights of the data subject.

(3) If the data subject already possesses the information that the personal information

controller must notify according to (i) or (ii).

(4) If the personal information controller does not have any contact information of the data subject or it involves excessive efforts to contact the data subject, including in the context of processing under the conditions set out in Section 3 PIPA. In determining whether or not it is possible to contact the data subject, or whether this involves excessive efforts, the possibility to cooperate with the data exporter in the EU should be taken into account.

4. Scope of application of the special exemption to the processing of pseudonymised information (Articles 28-2, 28-3, 28-4, 28-5, 28-6 and 28-7, Article 3 and Article 58-2 of the Act)

<Personal Information Protection Act

(Act No. 16930, partially amended on February 4, 2020)>

Chapter III Processing of Personal Information

SECTION 3 Special Cases concerning Pseudonymous Data

Article 28-2 (Processing of Pseudonymous Data) (1) A personal information controller may process pseudonymized information without the consent of data subjects for statistical purposes, scientific research purposes, and archiving purposes in the public interest, etc.

(2) A personal information controller shall not include information that may be used to identify a certain individual when providing pseudonymized information to a third party according to paragraph (1).

Article 28-3 (Restriction on Combination of Pseudonymous Data) (1) Notwithstanding Article 28-2, the combination of pseudonymized information processed by different personal information controllers for statistical purposes, scientific research and preservation of records for public interest, etc. shall be conducted by a specialized institution designated by the Protection Commission or the head of the related central administrative agency.

(2) A personal information controller who intends to release the combined information outside the organization that combined the information shall obtain approval from the head of the specialized institution after processing the information into pseudonymized information or the form referred to in Article 58-2.

(3) Necessary matters including the procedures and methods of combination pursuant to paragraph (1), standards and procedures to designate, or cancel the designation of, a specialized institution management and supervision, and standards and procedures of exporting and approval pursuant to paragraph (2) shall be prescribed by Presidential Decree.

Article 28-4 (Obligation to Take Safety Measures for Pseudonymous Data) (1) When processing the pseudonymized information, a personal information controller shall take such technical, organizational and physical measures as separately storing and managing additional information needed for restoration to the original state, as may be necessary to ensure safety as prescribed by Presidential Decree so that the personal information may not be lost, stolen, divulged, forged, altered, or damaged.

(2) A personal information controller who intends to process the pseudonymized

information shall prepare and keep records relating to matters prescribed by the Presidential Decree including the purpose of processing the pseudonymized information, and a third party recipient when pseudonymized information is provided, to manage the processing of pseudonymized information.

Article 28-5 (Prohibited Acts for the Processing of the Pseudonymized Information) (1) No one shall process the pseudonymized information for the purpose of identifying a certain individual.

(2) When information identifying a certain individual is generated while the pseudonymized information is processed, the personal information controller shall cease the processing of the information, and retrieve and destroy the information immediately.

Article 28-6 (Imposition of Administrative Surcharges for the Processing of the Pseudonymized Information) (1) The Commission may impose a fine equivalent to less than three-hundredths of total sales on data controller who has processed data for the purpose of identifying a specific individual in violation of Article 28-5 (1): Provided, That in case where there is no sales or difficulty in calculating the sales revenues, the data controller may be subject to a fine of not more than 400 million won or three-hundredths of the capital amount, whichever is greater.

(2) Article 34-2 (3) through (5) shall apply mutatis mutandis to matters necessary to impose and collect administrative surcharges.

Article 28-7 (Scope of Application) @Articles 20, 21, 27, 34 (1), 35 through 37, 39-3, 39-4, 39-6 through 39-8 shall not apply to the pseudonymized information.

Chapter Ⅰ General Provisions

Article 3 (Principles for Protecting Personal Information) (1) The personal information controller shall specify explicitly the purposes for which personal information is processed; and shall collect personal information lawfully and fairly to the minimum extent necessary for such purposes.

(2) The personal information controller shall process personal information in an appropriate manner necessary for the purposes for which the personal information is processed, and shall not use it beyond such purposes.

(3) The personal information controller shall ensure personal information is accurate, complete, and up to date to the extent necessary in relation to the purposes for which the personal information is processed.

(4) The personal information controller shall manage personal information safely according to the processing methods, types, etc. of personal information, taking into

account the possibility of infringement on the data subject's rights and the severity of the relevant risks.

(5) The personal information controller shall make public its privacy policy and other matters related to personal information processing; and shall guarantee the data subject's rights, such as the right to access their personal information.

(6) The personal information controller shall process personal information in a manner to minimize the possibility of infringing the privacy of a data subject.

(7) If it is still possible to fulfil the purposes of collecting personal information by processing anonymized or pseudonymised personal information, the personal information controller shall endeavor to process personal information through anonymization, where anonymization is possible, or through pseudonymisation, if it is impossible to fulfil the purposes of collecting personal information through anonymization

(8) The personal information controller shall endeavor to obtain trust of data subjects by observing and performing such duties and responsibilities as provided for in this Act and other related statutes.

Chapter Ⅸ Supplementary Provisions

Article 58-2 (Exemption from Application) This Act shall not apply to information that no longer identifies a certain individual when combined with other information, reasonably considering time, cost, technology, etc. <This Article Newly Inserted by Act No. 16930, Feb. 4, 2020>

(i) Chapter Ⅲ, Section 3 Special Cases concerning Pseudonymous Data (Art. 28-2 to Art.28-7) allows the processing of pseudonymised information without the consent of the data subject for the purpose of compiling statistics, scientific research, preservation of public records, etc. (Article 28-2), but in such cases, appropriate safeguards and prohibitions necessary for protecting the rights of data subjects are mandatory (Articles 28-4 and 28-5), penalty surcharges may be imposed on violators (Article 28-6) and certain safeguards otherwise available under PIPA do not apply (Article 28-7).

(ii) These provisions shall not apply to cases where pseudonymised information is processed for purposes other than compiling statistics, scientific research, preservation of public records, etc. For instance, if the personal information of an EU individual, which was transferred to Korea according to the adequacy decision of the European Commission, is pseudonymised for purposes other than compiling statistics, scientific research, preservation of public records, etc., the special provisions in Chapter III, Section 3 shall not apply.

(iii) Where a personal information controller processes pseudonymised information for the

purpose of compiling statistics, scientific research, preservation of public records, etc. and if the pseudonymised information has not be destroyed once the specific purpose of processing has been fulfilled in line with Article 37 of the Constitution and Article 3 (Principles for Protecting Personal Information) of the Act, it shall anonymise the information with a view to ensure that it no longer identifies a specific individual, alone or when combined with other information, reasonably considering time, cost, technology, etc., in accordance with Article 58-2 PIPA.

5. Corrective measures, etc. (Paragraphs 1, 2 and 4 of Article 64 of the Act)

<Personal Information Protection Act

(Act No. 16930, partially amended on February 4, 2020)>

Article 64 (Corrective Measures) (1) Where the Protection Commission deems that there is substantial ground to deem that there has been infringement with respect to personal information, and failure to take action is likely to cause damage that is difficult to remedy, it may order the violator of this Act (excluding central administrative agencies, local governments, the National Assembly, the Court, the Constitutional Court, and the National Election Commission) to take any of the following measures:

1. To suspend infringement with respect to personal information;

2. To temporarily suspend personal information processing;

3. Other measures necessary to protect personal information and to prevent personal information infringement.

(2) Where the head of a related central administrative agency deems that there is substantial ground to deem that there has been an infringement of personal information, and failure to take action is likely to cause damage that is difficult to remedy, he or she may order a personal information controller to take any of the measures provided for in paragraph (1) pursuant to the statutes under such related central administrative agency's jurisdiction.

(4) When a central administrative agency, a local government, the National Assembly, the Court, the Constitutional Court, or the National Election Commission violates this Act, the Protection Commission may recommend the head of the relevant agency to take any of the measures provided for in paragraph (1). In such cases, upon receiving the recommendation, the agency shall comply therewith unless there are extraordinary circumstances.

(i). First, court precedents[4] [5] interpret 'damage that is difficult to remedy' as a case that

[4] (Supreme Court Judgement 97Da10215,10222 dated January 26, 1999) If the criminal facts of the accused are disclosed through the media, it is likely to cause irreparable mental and physical damage to not only the victim, i.e. the plaintiff,

could cause damage to an individual's personal rights or privacy.

(ii). Accordingly, 'substantial ground to deem that there has been an infringement with respect to personal information, and failure to take action is likely to cause damage that is difficult to remedy' prescribed in Paragraphs 1 and 2 of Article 64, refer to cases where a violation of the law is deemed to be likely to infringe on the rights and freedom of individuals in regard to personal information. This will be applicable whenever any of the principles, rights and duties, included in the law to protect personal information, are violated.

(iii) According to Paragraph 4 of Article 64 of the Personal Information Protection Act is a measure in regard to 'a violation of this Act,' i.e. action against an infringement of PIPA.

A central administrative agency, etc., as a public authority bound to the rule of law, may not violate any law and is obligated to take a corrective measure, including to immediately stop the action, and compensate for damages in the exceptional case where an illegal act was nevertheless committed.

Accordingly, even without any intervention by the Protection Commission according to Paragraph 4 of Article 64 of PIPA, a central administrative agency etc. must take a corrective measure against violations if it becomes aware of any violation of the law.

In particular, where the Protection Commission has recommended a corrective measure, it will normally be objectively clear to the central administrative agency, etc. that it has violated the law. Thus, in order to justify why it considers that a recommendation by the Protection Commission should not be followed, a central administrative agency, etc. must present clear grounds that can prove that it did not violate the law. The recommendation must be followed unless the Protection Commission determines that this is indeed not the case.

In consideration of this, the 'extraordinary circumstances' in Paragraph 4 of Article 64 of the Personal Information Protection Act must be strictly limited to extraordinary circumstances in which there are clear grounds for central administrative agencies etc. to prove that 'this Act was in fact not violated,' such as 'cases where there are extraordinary (factual or legal) circumstances' that the Protection Commission did not know when making its recommendation initially and the Protection Commission determines that indeed no violation has occurred.

---

but also people around him/her, including families.

[5] (Seoul High Court Judgment 2006Na92006 dated January 16, 2008) If a defamatory article is published, it is likely to cause serious irreparable damage to the person involved.

6. Application of PIPA to the processing of personal data for national security purposes including investigation of infringements and enforcement in accordance PIPA(Article 7-8, Article 7-9, Article 58, Article 3, Article 4 and Article 62 of PIPA)

Article 7-8 (Work of the Protection Commission) (1) The Protection Commission shall perform the following work: […]

3. Matters concerning investigation into infringement upon the right of data subjects and the ensuing dispositions;
4. Handling of complaints or remedial procedures relating to personal information processing and mediation of disputes over personal information;

[…]

Article 7-9 (Matters Subject to Deliberation and Resolution by the Protection Commission) (1) The Protection Commission shall deliberate and resolve on the following matters: […]

5. Matters concerning the interpretation and operation of law related to the protection of personal information;

[…]

Article 58 (Partial Exclusion of Application) (1) Chapter III through VII shall not apply to any of the following personal information:
1. Personal information collected pursuant to the Statistics Act for processing by public institutions;
2. Personal information collected or requested to be provided for the analysis of information related to national security;
3. Personal information processed temporarily where it is urgently necessary for the public safety and security, public health, etc.;
4. Personal information collected or used for its own purposes of reporting by the press, missionary activities by religious organizations, and nomination of candidates by political parties, respectively.

[omitted (2) and (3)]

(4) In the case of processing personal information pursuant to paragraph (1), a personal information controller shall process the personal information to the minimum extent necessary to attain the intended purpose for the minimum period; and shall also make necessary arrangements, such as technical, managerial and physical safeguards, individual grievance handling and other necessary measures for the safe management and appropriate

processing of such personal information.

Article 3 (Principles for Protecting Personal Information) (1) The personal information controller shall specify explicitly the purposes for which personal information is processed; and shall collect personal information lawfully and fairly to the minimum extent necessary for such purposes.
(2) The personal information controller shall process personal information in an appropriate manner necessary for the purposes for which the personal information is processed, and shall not use it beyond such purposes.
(3) The personal information controller shall ensure personal information is accurate, complete, and up to date to the extent necessary in relation to the purposes for which the personal information is processed.
(4) The personal information controller shall manage personal information safely according to the processing methods, types, etc. of personal information, taking into account the possibility of infringement on the data subject's rights and the severity of the relevant risks.
(5) The personal information controller shall make public its privacy policy and other matters related to personal information processing; and shall guarantee the data subject's rights, such as the right to access their personal information.
(6) The personal information controller shall process personal information in a manner to minimize the possibility of infringing the privacy of a data subject.
(7) If it is still possible to fulfil the purposes of collecting personal information by processing anonymized or pseudonymised personal information, the personal information controller shall endeavor to process personal information through anonymization, where anonymization is possible, or through pseudonymisation, if it is impossible to fulfil the purposes of collecting personal information through anonymization.
(8) The personal information controller shall endeavor to obtain trust of data subjects by observing and performing such duties and responsibilities as provided for in this Act and other related statutes.

Article 4 (Rights of Data Subjects) A data subject has the following rights in relation to the processing of his or her own personal information:
1. The right to be informed of the processing of such personal information;
2. The right to determine whether or not to consent and the scope of consent regarding the processing of such personal information;
3. The right to confirm whether or not personal information is being processed and to request access (including the provision of copies; hereinafter the same applies) to such personal information;
4. The right to suspend the processing of, and to request correction, deletion, and destruction of such personal information;
5. The right to appropriate redress for any damage arising out of the processing of such personal information through a prompt and fair procedure.

Article 62 (Reporting on Infringements) (1) Anyone who suffers infringement of rights or interests relating to his or her personal information in the course of personal information processing by a personal information controller may report such infringement to the Protection Commission.
(2) The Protection Commission may designate a specialized institution in order to efficiently receive and handle the claim reports pursuant to paragraph (1), as prescribed by Presidential Decree. In such cases, such specialized institution shall establish and operate a personal information infringement call centre (hereinafter referred to as the "Privacy Call Centre").
(3) The Privacy Call Center shall perform the following duties:
1. To receive claim reports and provide consultation in relation to personal information processing;
2. To investigate and confirm incidents and hear opinions of related parties;
3. Duties incidental to subparagraphs 1 and 2.
(4) The Protection Commission may, if necessary, dispatch its public official to the specialized institution designated under paragraph (2) pursuant to Article 32-4 of the State Public Officials Act in order to efficiently investigate and confirm the incidents pursuant to paragraph (3) 2

(ⅰ) The collection of personal information for national security purposes is regulated by specific laws that empower competent authorities (e.g. the National Intelligence Service) to intercept communications or request disclosure under certain conditions and safeguards (hereafter: "national security laws"). These national security laws include, for instance, the Communications Privacy Protection Act, the Act on Anti-Terrorism for the Protection of Citizens and Public Security or the Telecommunications Business Act. In addition, the collection and further processing of personal information has to comply with the requirements of PIPA. In this regard, Article 58(1) lit. 2 PIPA provides that Chapters III through VII shall not apply to personal information collected or requested to be provided for the analysis of information related to national security. This partial exception therefore applies to the processing of personal information for national security purposes.

At the same time, Chapter I (General provisions), Chapter II (Establishment of personal information protection policies, etc.), Chapter VIII (Class-action lawsuit over data infringement), Chapter IX (Supplementary provisions) and Chapter X (Penalty provisions) of PIPA apply to the processing of such personal information. This includes the general data protection principles set out in Article 3 (Principles of protecting personal information) and the individual rights guaranteed by Article 4 PIPA (Rights of data subjects).

In addition, Article 58(4) PIPA provides that such information must be processed to the minimum extent necessary to attain the intended purpose and for the minimum period; in

addition, it requires the personal information controller to put in place the necessary measures to ensure safe data management and appropriate processing, such as technical, managerial and physical safeguards, as well as measures for the appropriate handling of individual grievances.

Finally, the provisions governing the tasks and powers of the PIPC (including Article 60-65 PIPA on the handling of complaints and the adoption of recommendations and corrective measures) as well as the provisions on administrative and criminal penalties (Article 70 et seq. PIPA) apply. According to Article 7-8(3), (4) and Article 7-9(5) PIPA, these investigatory and corrective powers, including when exercised in the context of handling complaints, also cover possible infringements of the rules contained in specific laws setting out the limitations and safeguards with respect to the collection of personal information, such as the national security laws. Given the requirements in Article 3(1) PIPA for the lawful and fair collection of personal information, and such infringement constitutes a violation of "this Act" within the meaning of Articles 63 and 64, allowing the PIPC to carry out an investigation and to take corrective measures.[6] The exercise of these powers by the PIPC supplements, but does not replace, the powers of the National Human Rights Commission under the Human Rights Commission Act.

The application of the core principles, rights and obligations of PIPA to the processing of personal information for national security purposes reflects the guarantees enshrined in the Constitution for the protection of the individual's right to control his or her own personal information. As recognised by the Constitutional Court, this includes the right of an individual[7] "to personally decide when, to whom or by whom, and to what extent his or her information will be disclosed or used. It is a basic right[8], […], existing to protect the personal freedom of decision from the risk caused by the enlargement of state functions and info-communication technology". Any restriction to that right, for example when necessary for the protection of national security, requires a balancing of the rights and interests of the individual against the relevant public interest and may not affect the essence of the right (Article 37(2) of the Constitution).

---

[6] As regards corrective measures pursuant to Article 64, see also Section 5 above.

[7] Constitutional Court Judgment, 99HunMa513, 2004HunMa190, dated May 26, 2005

[8] Constitutional Court Judgment, 2003HunMa282, dated July 21, 2005

Therefore, when processing personal information for national security purposes, the controller (e.g. NIS) shall, inter alia:

(1) Specify explicitly the purposes for which personal information is processed and collect personal information lawfully and fairly to the minimum extent necessary for such purposes (Article 3(1) PIPA); specifically, it shall only collect and further process the personal information for the purpose of performing duties under the relevant statutes such as the National Intelligence Service Act;

(2) Process personal information to the minimum extent, and for the minimum period, necessary to attain the intended purpose (Article 58(4) PIPA); upon attainment of the purpose of processing, the controller shall irreversibly destroy the personal information, unless further retention is specifically mandated by statute, in which case the relevant personal information shall be stored and managed separately from other personal information, not be used for any purpose other than that specified in the statute and destroyed upon the end of the retention period;

(3) Process personal information in an appropriate manner necessary for the purposes for which the personal information is processed, and shall not use it beyond such purposes (Article 3(2) PIPA);

(4) Ensure that personal information is accurate, complete and up to date to the extent necessary in relation to the purposes for which the personal information is processed (Article 3(3) PIPA);

(5) Manage personal information safely according to the processing methods, types, etc. of personal information, taking into account the possibility of infringements of the data subject's rights and the severity of the relevant risks (Article 3(4) PIPA);

(6) Make public its privacy policy and other matters related to personal information processing (Article 3(5) PIPA);

(7) Process personal information in a manner such as to minimise the possibility of infringing the privacy of a data subject (Article 3(6) PIPA).

(ii) In accordance with Article 58(4) PIPA, the controller (e.g. authorities competent for national security such as the NIS) shall make the necessary arrangements, such as putting in place technical, managerial and physical safeguards, to ensure compliance with these principles and the appropriate processing of personal information. This may for instance include specific measures to ensure the safety of personal information, such as restrictions on access to personal information, access controls, logs, providing employees with dedicated training on the handling of personal information, etc.

In addition, in accordance with Articles 3(5) and 4 PIPA, data subjects shall, inter alia, have the following rights with respect to personal information processed for national security

purposes:

(1) The right to obtain confirmation as to whether or not his or her personal information is being processed as well as information about the processing, and to access that information, including the provision of copies (Article 4(1), (3) PIPA);

(2) The right to suspend processing, and to the correction, deletion and destruction, of personal information (Article 4(4) PIPA).

(iii) A data subject may file a request in the exercise of these rights directly with the controller or indirectly via the Protection Commission, and may authorise his or her representative to do so. Where the data subject files a request, the controller shall grant the right without delay; provided, however, that it may delay, limit or deny the right if specifically provided for or inevitable to comply with other statutes to the extent and for as long as necessary and proportionate to protect an important objective of public interest (for instance to the extent that and for as long as granting the right would jeopardise an ongoing investigation or threaten national security), or where granting the right may cause damage to the life or body of a third party, or unjustified infringement of property and other interests of a third party. Where the request is denied or restricted, it shall notify the data subject of the reasons without delay. The controller shall prepare the method and procedure to enable data subjects to file requests and publicly announce them so that data subjects may become aware of them.

Moreover, in accordance with Article 58(4) PIPA (requirement to ensure the appropriate handling of individual grievances) and Article 4(5) PIPA (the right to appropriate redress for any damage arising out of the processing of personal information, through a prompt and fair procedure), data subjects shall have the right to obtain redress. This includes the right to report an alleged violation to the Personal Information Infringement Report Center (in accordance with Article 62(3) PIPA), file a complaint with the PIPC pursuant to Article 62 PIPA about any violation with respect to rights or interests relating to an individual's personal information and to obtain judicial redress against decisions or inaction of the PIPC under the Administrative Litigation Act. In addition, data subjects may obtain judicial redress under the Administrative Litigation Act if there has been an infringement upon their rights or interests due to a disposition or omission by the controller (e.g. unlawful collection of personal data), or obtain compensation for damages in accordance with the State Compensation Act. These redress avenues are available both in case of possible infringements of the rules contained in specific laws setting out the limitations and safeguards with respect to the collection of personal information, such as the national security laws, and of PIPA.

An individual from EU may submit a complaint to the PIPC through his/her national data protection authority, and PIPC will notify the individual through the national data protection authority, after the investigation and corrective measure (if applicable) is concluded.

Addendum

This Notification shall take effect at the same point in time when the European Commission’s adequacy decision regarding Korea according to the GDPR becomes effective.