

NEWSLETTER

August 2020

Data Privacy and Cybersecurity Group

CONTACT



Kwang Bae PARK

T: +82.2.772.4343
E: kwangbae.park@leeko.com



Hwan Kyoung KO

T: +82.2.2191.3057
E: hwankyung.ko@leeko.com



Sung Hee CHAE

T: +82.2.6386.6622
E: sunghee.chae@leeko.com



Kyung Min SON

T: +82.2.772.4918
E: kyungmin.son@leeko.com

Amendments to the Personal Information Protection Act and Credit Information Use and Protection Act Go into Effect

Amendments to the Personal Information Protection Act ('PIPA') and Credit Information Use and Protection Act ('Credit Information Act') that were promulgated on February 4, 2020 took effect on August 5, 2020, along with their respective implementing regulations that were also amended to reflect the changes in the two laws. By balancing the need for the protection of personal information against the need for its wider use, the amended laws aim to pave the way for a data-driven economy. In practice, the sweeping nature of the amendments are expected to bring about significant changes in the way personal information is processed in Korea.

For more details on the amended PIPA and amended Credit Information Act, please see our previous newsletters ([newsletter 1](#)/[newsletter 2](#)). In this newsletter, we review some of the key provisions of the amended PIPA and amended Credit Information Act and take a look at some of the corresponding changes to their Enforcement Decrees.

I. Amendments to the PIPA and the Enforcement Decree of the PIPA

The amendments to the PIPA include, among others:

- (i) the introduction of pseudonymized information and the legal basis for using pseudonymized information for research and statistical purposes without the data subject's consent;
- (ii) the introduction of the compatibility concept;
- (iii) the transfer of the Act on the Promotion of Information and Communications Network Utilization and Information Protection's ('Network Act's') personal information-related provisions to the PIPA; and

- (iv) the elevation of the Personal Information Protection Commission's ('PIPC's') status to the sole supervisory authority responsible for the enforcement of the PIPA (accordingly, personal information protection matters that are currently handled by multiple agencies (i.e., the Ministry of the Interior and Safety and the Korea Communications Commission) will all be handled by the PIPC instead).

Meanwhile, the amendments to the Enforcement Decree of the PIPA that have been adopted include, among others:

- (i) the specification of rules regarding the use and management of pseudonymized information such as the security measures which must be implemented and the specification of the procedures for combining pseudonymized information among different entities;
- (ii) the specification of the standards used to determine compatibility;
- (iii) the transfer of the personal information-related provisions in the Enforcement Decree of the Network Act to the Enforcement Decree of the PIPA; and
- (iv) the addition of certain types of information to the scope of 'sensitive information.'

Further details on the above changes are provided below.

■ (1) Use of Pseudonymized Information

■ (A) Security Measures for Pseudonymized Information

Under the amended PIPA, the stringent consent-oriented regulations on processing have been relaxed, allowing data handlers to process pseudonymized information without the consent of the data subject for purposes including statistical compiling, scientific research, and record preservation for the public interest. However, in order to minimize the risk of re-identification and any other harm that may be caused to data subjects in relation to the processing of pseudonymized information, the PIPA requires that anyone who processes pseudonymized information must implement certain statutorily-prescribed security measures. The amended Enforcement Decree of the PIPA specifies these security measures as follows:

- (i) The same security measures that are required with respect to general personal information must be implemented for pseudonymized information as well. In other words, the security measures stipulated under the 'Standards of Personal Information Security Measures' must be taken. (The 'Standards of Personal Information Security Measures,' which is an implementing regulation of the PIPA, sets forth the detailed security measures that must be applied to general personal information under the PIPA.)
- (ii) Pseudonymized information and additional information (i.e., information which can be used to identify a specific individual by restoring the pseudonymized information to its original state)

must be stored separately, and access rights to each of these two types of information must also be segregated in order to prevent the re-identification of the pseudonymized information through the use of the additional information.

■ **(B) Restriction on Combining Pseudonymized Information**

Although the amended PIPA promotes the use of pseudonymized information, combining pseudonymized information between different entities is restricted in that the process may be conducted only by professional institutions designated by the PIPC (**'Specialized Agencies'**) or by the head of a pertinent central administrative agency, which currently is a requirement unique to Korea. Also, the combined information may only be transferred out of the Specialized Agency after obtaining the approval of the head of the said institution. The detailed process and method of combining pseudonymized information is stipulated in the amended Enforcement Decree of the PIPA.

Under the amended Enforcement Decree of the PIPA, an entity that wishes to combine pseudonymized information (**'Applying Entity'**) must first submit its request/application to the Specialized Agency. After the Specialized Agency combines pseudonymized information in a way that makes the specific data subject unidentifiable, the Applying Entity must pseudonymize or anonymize such combined information in a space where technical, organizational and physical measures necessary for the secure processing of personal information have been implemented, installed at the Specialized Agency. The Applying Entity must obtain the approval of the Specialized Agency in order to be able to export the combined information, in which case the Specialized Agency applies the following criteria in determining whether to grant the request:

- (i) the purpose for which the pseudonymized information has been combined is related to the information to be exported;
- (ii) there is no likelihood that an individual might be identified due to such export of information; and
- (iii) measures are taken to ensure the security of the information to be exported.

Once the Specialized Agency approves the export request, they may bill the Applying Entity for the costs associated with the combination and export of the pseudonymized information. More details on the combining and removal of pseudonymized information will be provided in the 'Public Notice on the Combination and Removal of Pseudonymized Information' to be issued by the PIPC.

■ **(2) Compatibility Provision - Standards for the Further Use and Provision of Personal Information within the Scope Reasonably Related to the Original Purpose of Collection**

The amended PIPA allows data handlers to use or provide personal information to a third party without the consent of the data subject if

the scope of such further use or provision is within the scope reasonably related to the original purpose of the collection. As such, the amended Enforcement Decree of the PIPA provides detailed standards on what qualifies as ‘reasonably related to’ (i.e., compatible with) the original purpose of collection. In making this determination, the following factors are to be considered:

- (i) the processing is related to the original purpose for which the personal information was collected;
- (ii) the processing was foreseeable in light of the circumstances surrounding the collection of such personal information or the customary practice of processing such personal information;
- (iii) the processing does not unfairly infringe the rights and interests of the data subject; and
- (iv) whether pseudonymization, encryption, or other necessary safeguards to ensure the security of the personal information have been implemented.

The amended Enforcement Decree of the PIPA also requires that (i) the data handler disclose the standards which form the basis on which the above factors are assessed in its privacy policy and (ii) the Chief Privacy Officer check whether the further use and provision of personal information occurs in accordance with these standards.

■ (3) Others

■ (A) Transfer of Network Act’s Personal Information-related Provisions to the PIPA

Prior to the PIPA’s amendment, regulations on the processing of personal information by information and communications service providers and recipients of personal information provided by such information and communications service providers were set forth in the Network Act.

However, in line with the transfer of such provisions to the PIPA, the personal information-related provisions under the Enforcement Decree of the Network Act have also been transferred to the Enforcement Decree of the PIPA. Examples of such provisions include those on the implementation of security measures, method for confirming the legal guardian’s consent, method of notification and report of personal information leakages, destruction of personal information of inactive users (i.e., users who have not shown any account activity for at least 1 year), notification of personal information usage details/records, and criteria for calculating penalty surcharges.

■ (B) Expanded Scope of Sensitive Information

Under the amended Enforcement Decree of the PIPA, (i) biometric data such as fingerprint, iris, and face and (ii) race and ethnicity data are newly added to the scope of sensitive information, which was previously defined to just include information on an individual’s

ideology, creed, membership of a labor union or political party, political view, health, sexual preferences, genetic information, and criminal records.

■ (C) Additional Developments

Following the enforcement of the amended PIPA and its Enforcement Decree, the PIPC is expected to issue more practical guidance on the standards for pseudonymization and combining pseudonymized information through the ‘Pseudonymization Guidelines’ and ‘Guidelines on the Combination and Export of Pseudonymized Information,’ respectively. The current ‘Manual on Personal Information Protection Laws, Guidelines, and Public Notices’ will also be updated to reflect the recent amendments to the PIPA and its Enforcement Decree.

II. Amendments to the Credit Information Act and the Enforcement Decree of the Credit Information Act

The amendments to the Credit Information Act are broader and more diverse than the amendments to the PIPA as they include provisions on data protection as well as the regulatory system for the use and management of credit information (please see our [previous newsletter](#) for more information).

This newsletter will discuss the provisions in the amended Credit Information Act and the amended Enforcement Decree of the Credit Information Act relating to data protection which may be enforced by the Financial Services Commission (‘FSC’)/Financial Supervisory Service (‘FSS’) (if provisions apply to financial companies) or the PIPC (if provisions apply to non-financial companies which process personal credit information). Thus, the Credit Information Act will apply ahead of the PIPA where an entity processes personal credit information regardless of whether such entity is in the financial sector or not.

As in the case of the amended PIPA, the amended Credit Information Act also provides legal grounds for the processing of pseudonymized information without consent and introduces the compatibility concept. However, the amended Acts may differ, in terms of the permitted scope of data processing without consent and other details in application, so companies are advised to review closely these differences when processing pseudonymized information. Also, unlike the amended PIPA, the amended Credit Information Act contains provisions (taking effect from February 4, 2021) which (i) grants data subjects the right to request financial companies and public institutions to transmit their personal credit information to other financial companies (i.e., the right to data portability) and (ii) streamlines (simplify and visualize) the consent process so that data subjects may provide their informed consent more easily.

Accordingly, the amended Enforcement Decree of the Credit Information Act contains detailed provisions related to the processing pseudonymized information, the right to data portability, and streamlining of the consent process. For this newsletter, we summarize in greater detail below the provisions related to the processing of pseudonymized information as follows:

■ (1) Security Measures for Pseudonymized Information

Similar to the amended PIPA, the amended Credit Information Act requires the implementation of certain security measures to ensure the safety of pseudonymized information. Accordingly, the amended Enforcement Decree of the Credit Information Act sets forth detailed standards of such security measures and measures necessary to prevent pseudonymized information from being combined with additional information. However, there are certain important differences between the measures required under the respective Acts. For example, with respect to the specific security measures which must be taken for pseudonymized information, if the Credit Information Act applies then security measures prescribed by the 'Regulations on the Supervision of Credit Information Businesses' (issued under the Credit Information Act) will need to be implemented as opposed to the security measures prescribed by the 'Standards of Personal Information Security Measures' (issued under the PIPA). As such, it would be advisable for companies to review closely these differences when processing pseudonymized information.

■ (2) Restriction on Combining Pseudonymized Information

Similar to the amended PIPA, the amended Credit Information Act provides that the combination of pseudonymized information managed by different data handlers may be performed only by a Specialized Agency. However, because the details on the combination process and the Specialized Agencies permitted to combine pseudonymized information are different under the amended PIPA and the amended Credit Information Act, it will be important to confirm which law applies to the situation at hand to ensure the request for the combination of pseudonymized information is made to the appropriate Specialized Agency.

■ (3) Retention Periods for Pseudonymized Information

The amended PIPA and the amended Enforcement Decree of the PIPA do not impose any particular restrictions on the retention of pseudonymized information. Thus, unlike in the case of ordinary personal information, there is no requirement to retain pseudonymized information only for the minimum duration necessary to achieve the purposes of processing. On the other hand, the amended Enforcement Decree of the Credit Information Act provides that pseudonymized information may be retained past the retention period of ordinary personal credit information only when retention is within a pre-determined retention period set after considering the following:

- (i) level of administrative, physical, and technical protection needed to protect the pseudonymized information and additional information;
- (ii) effect on the credit information subject in the event re-identification takes place through the pseudonymized information;
- (iii) possibility of re-identification from the pseudonymized information; and

- (iv) the purpose for the processing of the pseudonymized information and the minimum duration necessary to achieve such purpose.

The FSC published additional guidance on the safe processing of anonymized data and pseudonymized information through its ‘Guide to the Processing of Anonymized and Pseudonymized Information in the Financial Sector’ on August 6. Meanwhile, the ‘Regulations on the Supervision of Credit Information Businesses,’ which further specify certain matters prescribed by the amended Enforcement Decree of the Credit Information Act, are also expected to be soon published by the FSC.

For more information pertaining to this newsletter, please contact the attorneys identified on the left.

The Lee & Ko Legal Newsletter is provided for general information purposes only and should not be considered as the rendering of legal advice for any specific matter. If you no longer wish to receive our newsletter service, please click [here](#) or reply to this email stating UNSUBSCRIBE in the subject line. The contents and opinions expressed in the Lee & Ko Legal Newsletter are protected by law against any unauthorized use.



Hanjin Building 63 Namdaemun-ro, Jung-gu Seoul 04532, Korea | Tel: +82-2-772-4000 | Fax: +82-2-772-4001/2 | www.leeko.com

[More L&K Newsletters](#)

[COVID-19 Resource Center](#)