SHIN&KIM
법무법인(유) 세종

Korea's PIPC Releases Comprehensive Guidelines on Processing Pseudonymized Data

On August 5, 2020, the amendments to the "T**hree Major Data Privacy Laws**" became effective – the Personal Information Protection Act (the "**PIPA**"), the Act on the Promotion of the Use of the Information Network and Information Protection (the "**Network Act**"), and the Credit Information Use and Protection Act (the "**Credit Information Act**").

Among the key changes under the amended PIPA include the introduction of the concept of "pseudonymized data," and through pseudonymization, allowing the use and transfer of data (previously not allowed without the data subject's consent). As such, there is now an increased potential for greater use of personally identifiable information ("**PII**" or "**personal data**" or "**personal information**"). Consequently, it is expected that businesses can create added value by combining pseudonymized data from various industries, including IT, financial, and medical sectors.

Another noteworthy change under the amended PIPA is the transformation of the Personal Information Protection Commission (the "**PIPC**") into South Korea's central data privacy regulatory authority under the Prime Minister's Office. In such a capacity, the PIPC published its "Comprehensive Guidelines on Processing

Pseudonymized Data" (the "**Guidelines**") on September 24, 2020. In the Guidelines, the PIPC clarifies, among others: (i) how personal data may be anonymized or pseudonymized; (ii) how to combine pseudonymized data from different personal information procesors and issues arising from combining pseudonymized data; and (iii) security measures for the safe use of pseudonymised data. Also, theoretical and technical examples are used to clarify how the Guidelines should be followed by data controllers[1] and processors (or "outsourcee")[2] when handling pseudonymized and anonymized data.

Summary of Key Aspects

We focus our discussion on the chapter on pseudonymization, and the chapter on combination and transfer of pseudonymized data.

1. Pseudonymization

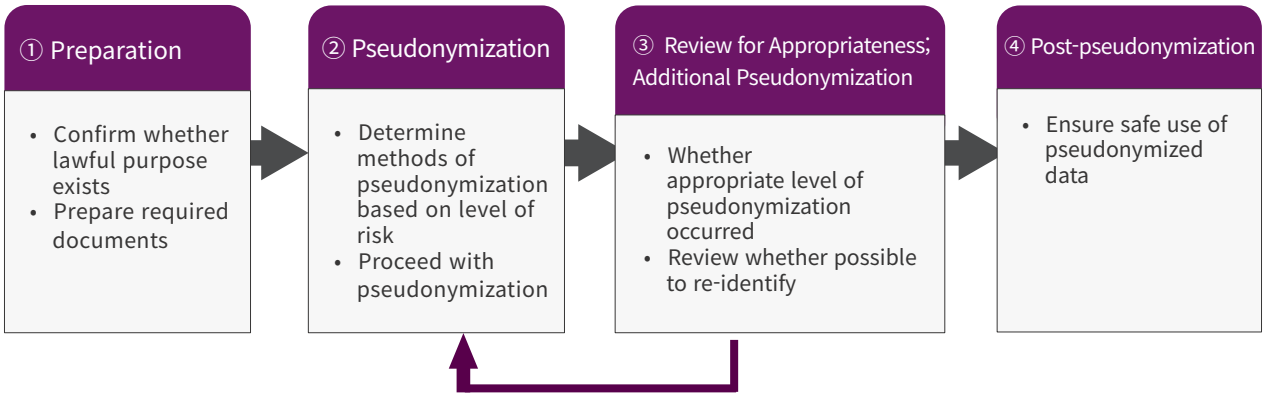
Pseudonymization means the processing of personal information by deleting part of, or replacing all or part of, personal information so that the personal information can no longer be attributed to a specific person without the use of additional information. Accordingly, in pseudonymizing personal information, the data processor should consider:

(a) Whether a specific person can be identified by the pseudonymized data only; and
(b) The possibility that additional information[3] or other information may be combined with the pseudonymized data.

---

1. Data or "personal information controller" under the PIPA refers to a public institution, legal entity, organization, or an individual, among others, that processes personal information directly or indirectly.
2. Data processor is not used under the Korean PIPA; rather, the term "outsourcee" is used instead to refer to an entity that processes personal information of data subjects under an outsourcing contract.
3. Additional information refers to the means or methods (e.g., algorithms) used to replace all or part of the personal information, and the information that may be used to recover the deleted or replaced personal information through comparison with pseudonymized data or other processing (e.g., mapping table information, personal information used in pseudonymization)

The **process of pseudonymization** consists of the following four stages:



1) <u>Preparation stage:</u>

(a) Clarify/specify the purpose of use for the pseudonymized data to define the items subject to pseudonymization (from the personal information files) and to determine the level of processing; and

(b) Prepare required documents (including any necessary agreements if the pseudonymized data is to be provided to a third party).

2) <u>When determining the method of pseudonymization, a comprehensive review should include:</u>

(a) Purpose of the pseudonymization; the environment in which the personal data is processed (i.e., internally processed or provided a third party for processing); type of the processing (i.e., internal use, provision to a third party, etc.); and the nature of the information processed (i.e., comprehensively consider the characteristics of the information).

(b) More specifically, pseudonymization stage consists of: (1) selection of personal information to be processed (pseudonymized); (2) risk measurement (for reidentification); (3) determination of the level of pseudonymization; and (4) pseudonymization.

3) **During the appropriate level review & additional pseudonymization stage, review:**

(a) Whether pseudonymized data will achieve the intended purpose;

(b) Whether the data was appropriately pseudonymized; and

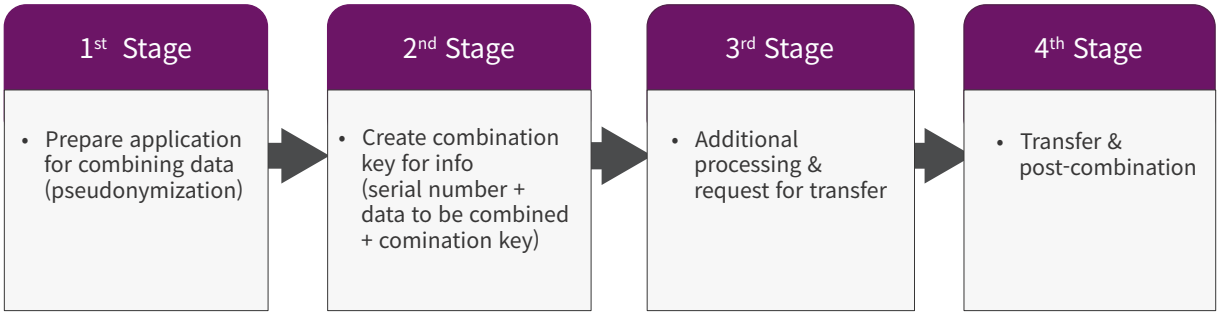
(c) Whether there is any potential risk of re-identifying the relevant living individual using the pseudonymized data.[4] If necessary, the 2nd stage may be repeated to ensure appropriate pseudonymization.

4) During the post-pseudonymization stage, if the pseudonymization is deemed appropriate based on the third stage review (as noted above), then the pseudonymized data may be processed for the original purpose; during the processing, any risk for re-identification of the data subjects should be monitored[5].

2. Combination and Transfer of Pseudonymized Data

Parties who intend to combine and use their pseudonymized data ("**Combination Applicants**") may discuss and agree on the provision of the Combination Applicants' pseudonymized data, and combine their data by following the procedures described below.

Combination and Transfer Application Procedures



4. Even if personal information is pseudonymized with the above risks in mind, if the relevant person is still identifiable using his or her unique identifier, then additional pseudonymization processing may be required.

5. If a specific living individual is re-identified, then the relevant measures should be taken to eliminate such a risk by immediately suspending the processing, withdrawing or destroying such data.

1) During the preparation and application for combination stage, the Combination Applicants prepare for the combination process through pseudonymization or by preparing the relevant applications, which must be submitted to the organization designated by the PIPC or the relevant government agency for combining pseudonymized data ("**Combination Processor**").

2) During the creation of the combination key and transfer of information stage, the Combination Applicants discuss and agree with the Combination Processor on the combination schedule, method of transfer, among others. In addition, the Combination Applicants create a combination key using the relevant information provided by the designated organization for managing the combination keys. [6]

3) During the additional processing and request for transfer stage, the Combination Applicants must conduct additional pseudonymization or anonymization on the combined pseudonymized data in a designated location on the Combination Processor's premises before transferring such data. In order to request for transfer of the combined pseudonymized data, the Combination Processor's Data Transfer Evaluation Committee must first assess the data.[7]

4) During the transfer and post-combination stage, the Combination Applicants may process the transferred data from the third stage for the original purpose of applying for the combination. In addition, the Combination Applicants must comply with the safe handling requirements applicable to the processing of pseudonymized data.

---

6. A Combination Applicant sends "the combination key and the relevant serial number" to the Combination Processor through the Pseudonymized Data Combination Support System, and transmits "information regarding the target data with which to be combined and the relevant serial number" to the Combination Processor by using the method of transfer provided by the Combination Processor.

7. If the intended purpose may be achieved with anonymized data, then the combined pseudonymized data must be anonymized before transmission.

About Shin & Kim

Shin & Kim's data protection and security experts provide comprehensive advice on personal information protection and data security based on our in-depth experience in the relevant areas, including data protection regulations of Korea and of other countries, such as Korea's *Personal Information Protection Act* ("PIPA") and the EU GDPR, responding to personal information leakage, establishing a personal information protection/data privacy compliance system, among others. In particular, our professionals have advised numerous public and the private sector clients, **performing leading roles in the amendments to Korea's "Three Major Data Privacy Laws" and its subordinate regulations. Our team of experts continue to advise numerous private sector clients, both domestic and foreign, in their efforts to improve their data protection and compliance systems.** Should you have any questions or comments on the contents of this newsletter, or if you wish to further discuss the Guidelines or the "Three Major Data Privacy Laws" in relation to your specific situation, please do not hesitate to contact us.

Contact us

Sinook Kang
Partner

T. +82-2-316-4059
E. sokang@shinkim.com

Juneyoung Jang
Partner

T. +82-2-316-4410
E. jyojang@shinkim.com

Junghyun Hwang
Associate

T. +82-2-316-1775
E. jhhwang@shinkim.com

Ho Sang Yoon
Associate

T. +82-2-316-2584
E. hsyoon@shinkim.com

Claudia Hong
Senior Foreign Attorney

T. +82-2-316-4487
E. cahong@shinkim.com

Jayden Lee
Foreign Attorney

T. +82-2-316-7281
E. jalee@shinkim.com

SHIN&KIM
법무법인(유) 세종