December 23, 2025

KEY CONTENTS OF THE「PROPOSED REVISION TO THE GUIDELINES FOR PROCESSING PSEUDONYMIZED INFORMATION」

I. BACKGROUND OF THE DISCLOSURE OF THE「PROPOSED REVISION TO THE GUIDELINES FOR PROCESSING PSEUDONYMIZED INFORMATION」

Although the system for processing pseudonymized information was introduced to strike a balance between personal information protection and data utilization, it has consistently been pointed out that the provision and utilization of pseudonymized information have not been fully utilized in practice. This is largely due to cumbersome pseudonymization and review procedures, the burden of preparing extensive documentation, and rigid, conservative processing practices. Furthermore, while demand for the use of the pseudonymized information system in the AI research and development sector has recently surged, issues have been raised regarding significant practical confusion and constraints caused by the gap between the characteristics of AI technology (such as its general-purpose nature, continuous learning, and processing of large-scale unstructured data) and the current pseudonymized information processing framework.

Accordingly, in order to alleviate the practical burden on stakeholders while maintaining a substantial level of personal information protection, the Personal Information Protection Commission (PIPC) disclosed the「Proposed Revision to the Guidelines for Processing Pseudonymized Information」(the "Proposed Revision") as part of the "Pseudonymized Information System Operation and Innovation Plan" announced jointly with relevant ministries on September 24, 2025. Opinions from stakeholders will be collected until December 26, 2025. Below, we examine the core contents and implications of the Proposed Revision.

II. KEY CONTENTS

The Proposed Revision includes provisions relating to: (i) the consolidation and simplification of documents related to pseudonymization; (ii) the establishment of standardized risk judgment criteria; (iii) the differentiation of pseudonymization procedures and documentation based on risk; and (iv) the improvement of operational guidelines to better align with the technical characteristics of AI.

1. Consolidation and Simplification of Pseudonymization-Related Documents

1) Abolition of document forms that are unnecessary to prepare separately or that can be replaced (from 24 types to 10 types)

(1) Retained: Application for Use/Provision of Pseudonymized Information; Result Report on Additional Inspection of Unstructured Data; Commitment to Implementation of Safety Measures.

(2) Integrated: Pseudonymized Information Utilization Plan; Risk Review Report; Pseudonymization Plan; Pseudonymization Result Report; Adequacy Review Result Report; Adequacy Evaluation Member Pledge; Management Ledger for Pseudonymized (Additional) Information.

(3) Abolished: Internal Management Plan*; Data Provision Agreement.

* If an Internal Management Plan has already been established pursuant to Article 29 of the Personal Information Protection Act, the same plan may be used by adding only matters related to pseudonymized information, without the need to separately prepare a new plan dedicated solely to pseudonymized information.

2) Integrated management of overlapping items between documents and simplification of content

Risk levels are classified as Low, Medium, or High, and the scope of required documentation is applied in a differentiated and phased manner. Where the pseudonymization risk is assessed as low, documentation requirements may be reduced to the minimum necessary.

3) Clarification of the drafting entity (Provider, User, Reviewer) for each document

To prevent confusion regarding responsibility for preparing documents, the drafting entities have been clarified as follows:

(1) Provider: Risk Review Report; Pseudonymization Plan (prepared in consultation with the User); Pseudonymization Result Report; Result Report on Additional Inspection of Unstructured Data; Management Ledger for Pseudonymized (Additional) Information (items related to provision).

(2) User: Application for Use/Provision of Pseudonymized Information; Pseudonymized Information Utilization Plan; Commitment to Implementation of Safety Measures (prepared at the Provider's request); Management Ledger for Pseudonymized (Additional) Information (items related to utilization and destruction).

(3) Reviewer: Adequacy Review Result Report; Adequacy Evaluation Member Pledge.

2. Establishment of Standardized Risk Judgment Criteria

By structuring the assessment process into "Basic Risk Judgment" (Step 1) and "Final Risk Adjustment" (Step 2), the Proposed Revision establishes clearer and more standardized risk judgment criteria. This is intended to enhance consistency and objectivity while providing rational standards tailored to actual risk levels.

1) Basic Risk Judgment: Risk is assessed based on the utilization entity (internal use or third-party provision) and the processing environment (whether it is controllable by the providing institution).

(1) Low Risk: Direct utilization by the same personal information controller.

(2) Medium Risk: Third-party provision where processing occurs in an environment controllable by the providing institution.

(3) High Risk: Third-party provision where processing occurs in an environment not controllable by the providing institution.

2) Final Risk Adjustment: Risk levels may be adjusted upward or downward by reflecting data characteristics (e.g., whether the data includes highly sensitive information) and the processing context (e.g., whether processing is conducted within a secure institution).

3. Differentiation of Pseudonymization Procedures and Documentation Based on Risk

To address inefficiencies caused by uniform and conservative adequacy reviews regardless of risk level, the Proposed Revision improves the efficiency of pseudonymized information utilization by applying differentiated procedures and documentation requirements according to risk.

1) Low Risk: (1) Review by the officer in charge and (2) Preparation of only the necessary minimum documents, such as the Pseudonymized Information Utilization Plan, Risk Review Report, and Management Ledger for Pseudonymized (Additional) Information.

2) Medium Risk: (1) Internal deliberation and (2) Omission of certain documents possible, such as the Adequacy Evaluation Member Pledge, Commitment to Implementation of Safety Measures, and (if unstructured data is not included) Result Report on Additional Inspection of Unstructured Data.

3) High Risk: (1) Review by a Data Deliberation Committee and (2) Preparation and retention of all documents.

4. Improvement of Operational Guidelines to Better Align with AI Technical Characteristics

1) Refinement of Criteria for Setting Pre-defined Purposes for Pseudonymized Information Processing

When setting the initial purpose for processing pseudonymized information, it is now permitted to pre-define a "scope of extendable purposes" that share similar characteristics. This is limited to: (i) additional analytical purposes directly related to the initial purpose; or (ii) applied research for similar purposes derived from the same research process. In all cases, the extended purpose must rely on the same dataset as the initial purpose.

2) Supplementation of Criteria for Setting Processing Periods for Pseudonymized Information

(1) Setting Processing Period

For the purpose of developing and upgrading AI models, the processing period for pseudonymized information may be broadly set until the "termination of AI service development and operation."

(2) Procedure for Extension of Processing Period

As extensions of processing periods generally fall within the Low Risk category, a simplified renewal procedure has been introduced. Even upon expiration of the initially set period, the officer in charge may extend the period by verifying the reason for extension and any changed elements, without preparing separate documentation.

3) Enhancement of the Ability to Utilize Outliers in AI Learning

The Proposed Revision clarifies that outliers—namely, values deviating from general data patterns or exceptional data such as rare disease names or traffic accident scenarios—do not necessarily need to be deleted if they are required for the processing purpose. Conditions for the safe use of such outliers are presented, including: (i) data-level safety measures, such as strengthening pseudonymization of other identifiable data elements; and (ii) environmental safety measures, such as use within a "Personal Information Innovation Zone."

4) Establishment of Sampling-Based Inspection Schemes for Unstructured Data

Recognizing that a full review of unstructured data is not required in all cases, the Proposed Revision introduces various inspection methods, including sampling-based inspections tailored to risk levels.

III. IMPLICATIONS

Recently, institutional improvements have been implemented in stages to ease operational rigidity in the pseudonymized information system and to address legal uncertainties identified in practice. In particular, beginning in November 2025, the PIPC has been piloting a "No-Action Letter" system, under which it reviews acts of pseudonymized information processing and notifies relevant parties that no administrative measures will be taken if the acts are deemed lawful. Based on the results of this pilot program, the PIPC plans to further refine the system and establish a formal legal basis in the future.

Furthermore, as procedures under the pseudonymization guidelines are simplified pursuant to the Proposed Revision, it is anticipated that excessive administrative burdens and concerns regarding liability—which have previously discouraged the use of pseudonymized information—will be significantly reduced. As a result, a more enabling environment is expected to emerge for the active utilization of pseudonymized information across research, development, and general data use, consistent with the original intent of the system.

* * *

For any inquiry or questions regarding the content of this newsletter, please contact us.

Related Professionals

Taeuk Kang
Partner
T 82.2.3404.0485
E taeuk.kang@bkl.co.kr

Junho Lee
Partner
T 82.2.3404.6965
E junho.lee@bkl.co.kr

Jiyoung Sohn
Senior Foreign Attorney (New York)
T 82.2.3404.0241
E jiyoung.sohn@bkl.co.kr

Min Kwon contributed to this update.

This publication is provided for general informational purposes only, and should not be construed as legal or professional advice on any particular matter, nor create an attorney-client relationship. Before you take any action that may have legal implications, please inquire with your contact at Bae, Kim & Lee LLC, or the authors of this publication.