

# NEWSLETTER

May 2024

Data Privacy & Cybersecurity Group

## CONTACT



Partner  
Kwang Bae PARK

T: +82.2.772.4343  
E: [kwangbae.park@leeko.com](mailto:kwangbae.park@leeko.com)



Partner  
Hwan Kyoung KO

T: +82.2.2191.3057  
E: [hwankyung.ko@leeko.com](mailto:hwankyung.ko@leeko.com)



Partner  
Sunghee CHAE

T: +82.2.6386.6622  
E: [sunghee.chae@leeko.com](mailto:sunghee.chae@leeko.com)



Partner  
Kyung Min SON

T: +82.2.772.4918  
E: [kyungmin.son@leeko.com](mailto:kyungmin.son@leeko.com)

## Concretizing Rights of Data Subjects in the AI Era

### ••• Implementation of the Second Amendment to the Enforcement Decree of PIPA

Following the amendment of the Personal Information Protection Act (promulgated on March 14, 2023, the **Amended PIPA**), the second amendment to its Enforcement Decree (the **Second Amended Enforcement Decree**) went into effect on March 15, 2024. This decree delineates the provisions of the Amended PIPA that take effect one (1) year after its promulgation. For information on the first amendment to the Enforcement Decree, which came into effect on September 15, 2023, please refer to the [link here](#).

The Second Amended Enforcement Decree specifies the rights of data subjects concerning automated decision-making, a response to the rising use of artificial intelligence (AI). It further details the criteria for appointing privacy officers, including their qualifications and independence, specifies additional elements to be included in privacy policies, relaxed standards for obtaining insurance or joining mutual aid societies to secure liability for damages, and an adjustment to the cycle of regular inspections on the management of unique identifiable information (for the Personal Information Protection Commission (PIPC)'s press release dated March 6, 2024, available only in Korean, please refer to the [link here](#).) However, the provision for data portability (Article 35-2 of the Amended PIPA) is not yet in effect and thus is not included in the Second Amended Enforcement Decree.

This newsletter aims to introduce the key contents of the Second Amended Enforcement Decree.

#### 1. Rights of Data Subjects Regarding Automated Decision-making Including AI

According to the newly established rights of data subjects regarding automated decision-making under the Amended PIPA (Article 37-2 of the Amended PIPA; for more details, please refer to the [link here](#)), **when a decision is made through a “fully automated process” without any human intervention, such as by using AI, the data subject may request an explanation or review of the decision. If the decision significantly affects the data subject’s rights or obligations, the data subject may also refuse the decision.** The Second Amended Enforcement Decree concretizes these matters, with the details as follows:

## Definition of the “automated decision-making”

An “automated decision-making” refers to a case where two key elements are present: (i) a data controller making **a final decision** that affects the rights or obligations of the data subject after (ii) processing personal information using a **fully automated system** without human intervention.

## Methods and Procedures for Data Subject’s Request

**Data controllers are required to establish methods and procedures for data subjects to exercise their rights regarding automated decision-making.** These methods and procedures and methods should be comparable to those used for requests to access data, and should not be more difficult than the methods and procedures used to collect personal information.

## Obligation to Disclose Criteria for Automated Decision-making

Data controllers are required to disclose the following through an internet homepage or similar means:

- i. the fact that automated decision-making is taking place, its purpose, the scope of affected data subjects;
- ii. the types of personal information used and their relationship with automated decision-making;
- iii. considerations in the automated decision-making process and the procedures involving the processing of key personal information;
- iv. in cases where sensitive information or personal information of children under the age of 14 is used in the automated decision-making process, the purpose and the specific items of personal information being processed; and
- v. the fact that data subjects can request refusal, explanation, etc. regarding the automated decision-making, and the methods and procedures for doing so.

## Data Controllers’ Obligation Regarding Data Subjects’ Exercise of Rights

- (Refusal of Automated Decision-making) **If a data subject refuses automated decision-making on the grounds that it significantly affects their rights or obligations**, such as regarding life, body, or property, the **data controller must**, unless there are legitimate grounds, either **(i) take measures not to apply the decision or (ii) if the data subject requests a re-processing involving human intervention, take measures accordingly and notify the data subject of the result.** “Legitimate grounds” here refer to cases where there is a risk of unduly infringing on the life, body, property, or other interests of others.
- (Request for Explanation) **Upon a data subject’s request for an explanation, the data controller must provide a concise and meaningful explanation** that is easy to understand, including the outcome of the decision, the types of personal information used, and their impact. However, if the decision does not significantly affect the data subject’s rights or obligations, it may suffice only to disclose the criteria for the automated decision-making.
- (Objection) **If a data controller refuses a data subject’s request for refusal or explanation as described above, they must establish and provide necessary procedures for the data subject to object** (Article 38(5) of the Amended PIPA).

Upon an objection, the data controller must take necessary actions considering the content of the objection and inform the data subject of the result.

- (Timeline for Taking Measures) In principle, the above **measures must be taken within 30 days of receiving the data subject's request**, which may be extended by up to 60 days if there are legitimate grounds.

In addition to the above, further details, including the specific scope, content, and criteria for implementation, are expected to be specified in public notices issued under the authority delegated by the Enforcement Decree.

## 2. Designation of Privacy Officer

The **Amended PIPA newly introduced a provision to ensure the independence of privacy officers in performing their duties** (Article 31(6) of the Amended PIPA) and delegated the specification of the qualifications of the privacy officer to the Enforcement Decree (Article 31(9) of the Amended PIPA). The specifics of the qualifications under the Second Amended Enforcement Decree are as set forth below.

Firstly, the requirements for ensuring the independence of the privacy officers have been specified as follows:

- ensuring privacy officers' access to information related to personal information processing;
- establishing a regular reporting system for privacy officers to report to the representative or board of directors directly; and
- establishing an organizational structure and providing human and material resources for privacy officers to perform their duties.

Secondly, the specific qualifications for privacy officers have been strengthened. Previously, the requirements under the Enforcement Decree for appointing a privacy officer were limited to "the business owner, the representative, or an executive (or the head of a department in charge of personal information processing in the absence of an executive)." However, the **Second Amended Enforcement Decree now requires certain data controllers** (i.e., those with an annual sales or income of at least KRW 150 billion and process either (i) sensitive or unique identifier information of more than 50,000 data subjects, or (ii) personal information of more than 1 million data subjects) **to designate a person with at least four (4) years of combined experience** in personal information, information security, and information technology, including at least two (2) years specifically in personal information protection, and specifies the criteria for recognizing such experience (for more information, only available in Korean, please refer to the [link here](#)).

Accordingly, when appointing privacy officers going forward, it will be necessary to ensure that they meet these requirements. However, if a privacy officer who does not meet these requirements was appointed at the time the Second Amended Enforcement Decree came into effect, the Second Amended Enforcement Decree provides a two-year grace period so that they can meet the qualification requirements by March 14, 2026, enabling a gradual transition (Article 2 of the Addendum to the Second Amended Enforcement Decree).

### 3. Content of Privacy Policy and Disclosure Methods

The Second Amended Enforcement Decree has added the following items that must be included in privacy policies:

- if collecting and processing personal information of domestic data subjects from overseas, the names of the countries where the processing takes place; and
- the legal basis for transferring personal information overseas and the statutory notification requirements for such cross-border transfers.

### 4. Securing Liability for Damages

Under the Amended PIPA, **the obligation to secure liability for damages to data subjects**, using means such as insurance policies and reserve funds, **has been expanded** from information communications service providers (ICSPs, such as online business operators) **to include all data controllers**, now **covering both offline business operators and the public sector** (Article 39-7 of the Amended PIPA). Correspondingly, the Second Amended Enforcement Decree has rationally adjusted the criteria for obligated entities and established exemptions from these obligations. Previously, ICSPs were required to meet these obligations only if they had more than 1,000 users and revenues exceeding KRW 50 million. However, the Second Amended Enforcement Decree has heightened these thresholds for entities with over 10,000 data subjects and revenues exceeding KRW 1 billion. Moreover, public institutions, public interest corporations, non-profit private organizations, and small business owners who have outsourced their operations to professional contractors insured for liability are specifically identified as exempt from these obligations

Lee & Ko has a Data Privacy & Cybersecurity Group composed of the largest team of experts in the fields of personal information protection and information security in Korea. Our comprehensive legal services encompass consultations, legal investigation responses, and litigation representation concerning personal information matters. If you require advice or assistance concerning the Amended PIPA and Second Amended Enforcement Decree, please feel free to contact us at your convenience.

For key revisions to the Personal Information Protection Act and details on the first amendment to the Enforcement Decree, please refer to the newsletter below.

[Second Major Amendment to the Personal Information Protection Act Passed by National Assembly \(I\)](#)

[Second Major Amendment to the Personal Information Protection Act Passed by National Assembly \(II\)](#)

[Second Major Amendment to the Personal Information Protection Act Passed by National Assembly \(III\)](#)

[Amended Enforcement Decree of the Personal Information Protection Act of Korea](#)

The Lee & Ko newsletter is provided as a service and promotion for general information purposes. It does not contain legal advice. Although we try to provide quality information, we do not guarantee any results and Lee & Ko is not liable for any damages from the use of the information contained in the newsletter. We reserve all copyrights on text or images in the newsletter. The text or images in the newsletter may not be copied or distributed without the prior permission of Lee & Ko. If you no longer wish to receive our newsletter, please click [here](#) or reply to this email with UNSUBSCRIBE in the subject line.

[More L&K Newsletters](#)