March 2026

NEWSLETTER

Data Privacy & Cybersecurity Group

CONTACT

Partner
Hwan Kyoung KO
T: +82.2.2191.3057
E: hwankyoung.ko@leeko.com

Partner
Sunghee CHAE
T: +82.2.6386.6622
E: sunghee.chae@leeko.com

Partner
Tae Joo KIM
T: +82.2.772.4976
E: taejoo.kim@leeko.com

Partner
Minchae KANG
T: +82.2.772.4674
E: minchae.kang@leeko.com

Partner
Kyung Min SON
T: +82.2.772.4918
E: kyungmin.son@leeko.com

Partner
Il Shin LEE
T: +82.2.772.5982
E: ilshin.lee@leeko.com

PIPA Amendment Passes National Assembly Plenary Session

- Punitive administrative penalties of up to 10% of revenue for repeated or serious personal information infringements
- Strengthening of the role and authority of the CPO and the responsibilities of the representative and the board

The amendment to the Personal Information Protection Act (the **Amended PIPA**) was passed at the plenary session of the National Assembly on February 12, 2026.

Following a recent series of large-scale data breach incidents (i.e., incidents involving the loss, theft, or unauthorized disclosure of personal information) involving major telecommunications companies, financial institutions, and platform operators, public demand has grown for stronger preventive measures and enhanced corporate accountability.

While this amendment is widely known for introducing administrative penalties of up to 10% of revenue for violations of the PIPA, including data breaches, its significance extends further in that it calls for substantial changes to corporate data protection governance frameworks and security incident response systems.

In this newsletter, we review the specific details of the Amended PIPA and highlight its key implications.

1. Key Amendments

A. Increased cap on administrative penalties for repeated or serious personal information infringements and specification of data protection investments as grounds for mitigation

Senior Foreign Attorney
Jaeyoung CHANG
T: +82.2.6386.6261
E: jaeyoung.chang@leeko.com

Administrative penalties may now be imposed at up to 10% of a data handler(a concept analogous to a data controller under the GDPR)'s total revenue (excluding any amounts unrelated to the violation at issue)—or up to KRW 5 billion if there is no revenue or if calculating revenue is difficult, as prescribed by the Enforcement Decree (a proposed amendment to which is expected to be publicly notified)—in the following circumstances (Article 64-2(2)):

(i) if a violation constituting grounds for an administrative penalty is committed within three (3) years from the date of receiving a previous administrative penalty, with intent or gross negligence;

(ii) if a violation constituting grounds for an administrative penalty is committed with intent or gross negligence, and the number of affected data subjects is 10 million or more; or

(iii) where a data breach occurs as a result of failure to comply with a corrective order.

Conversely, the Amended PIPA requires the reduction of administrative penalties if grounds prescribed by the Enforcement Decree are met, such as the investment in and operation of data protection budgets, personnel, facilities, and equipment (excluding cases where the violation was committed with intent or gross negligence) (Article 64-2(6)).

B. Expansion of the concept of data breach and obligations related to data breach notification

The scope of "data breach" under the PIPA has been expanded beyond the current statutory categories of "loss, theft, or unauthorized disclosure" of personal information to additionally include "forgery, alteration, or damage" (Articles 23(2) and 34(1)).

The PIPA requires that certain information be notified to the affected data subjects in the event of a data breach. Under the Amended PIPA, the scope of required notification items has been expanded to include the following (Article 34(1)(6)):

(i) information regarding the data subject's legal rights and methods of exercising such rights, including claims for compensatory and statutory damages arising from the data breach or similar incident and dispute resolution procedures; and

(ii) other matters prescribed by the Enforcement Decree.

In addition, even prior to confirmation of a data breach, where a data handler becomes aware of the possibility of a data breach as prescribed by the Enforcement Decree—taking into account the type of personal information involved, the impact on data subjects, and the level of risk—the data handler is now required to notify, without delay, all potentially affected data subjects of such possibility, including information necessary to minimize potential damages and other matters to be prescribed by the Enforcement Decree (Article 34(2)).

C. Mandatory ISMS-P certification for data handlers above a certain scale

The PIPA provides that the Personal Information Protection Committee may certify the level of personal data protection of a data handler. Data handlers may apply for such certification—i.e., Personal Information & Information Security Management System (**ISMS-P**) certification—and, under the current PIPA, obtaining ISMS-P certification is voluntary. Under the Amended PIPA, however, data handlers that meet certain criteria prescribed by the Enforcement Decree—based on factors such as annual revenue and the scale of personal information processed—will be required to obtain ISMS-P certification (Article 32-2(1), proviso).

D. Clarification of the representative's responsibility and strengthening of the CPO's role

The Amended PIPA expressly provides that the representative (e.g., CEO) or business owner bears ultimate responsibility for the secure processing of personal information and the protection of data subjects' rights, and must effectively implement comprehensive management measures, including the allocation of qualified personnel and sufficient budgetary support (Article 30-3).

In addition, the statutory duties of the Chief Privacy Officer (**CPO**) have been expanded to include (Article 31(4)(2) and (3)):

(i) managing qualified personnel and securing the budget necessary for the protection of personal information; and

(ii) reporting to the representative and the board of directors on the status of personal information protection and other related matters of importance.

Furthermore, for data handlers meeting criteria prescribed by the Enforcement Decree—based on factors such as annual revenue and volume of personal information processed—are now subject to obligations to (Article 31(3)):

(i) obtain board approval when appointing, changing, or dismissing the CPO; and

(ii) report matters concerning the appointment, change, or dismissal of the CPO to the Personal Information Protection Commission in accordance with the Enforcement Decree.

E. Effective Date

The Amended PIPA will enter into force six (6) months after the date of its promulgation; provided, however, that the provisions mandating ISMS-P certification will take effect on July 1, 2027 (Addendum, Article 1).

2. Implications

A. Increased importance of establishing robust data protection governance and investment

The Amended PIPA introduces punitive administrative penalties, thereby significantly increasing the level of sanctions for data breaches and other infringements. At the same time, it strengthens not only the duties and role of the CPO but also the responsibilities of the representative and the board regarding data protection, while incentivizing corporate investment in data protection by providing additional grounds for mitigation of administrative penalties. Accordingly, before the Amended PIPA takes effect, businesses should establish or refine governance structures to ensure the effective implementation of data protection measures and proactively invest in adequate personnel, systems, and infrastructure. Regarding specific compliance measures, it will also be important to closely monitor how the provisions of the Amended PIPA are further specified through the forthcoming amendment to the Enforcement Decree.

In this context, the presence or absence of intent or gross negligence on the part of a data handler will serve as a key factor in determining the amount of an administrative penalty.

However, as the responsibilities of the representative and other directors with respect to data protection have now been expressly articulated—and as they are expected to participate in related decision-making—the propriety of the board's conduct, in addition to that of the CPO and personnel directly handling personal information, may also be considered in assessing intent or gross negligence. Therefore, guidance from legal experts may be necessary from the very beginning—such as when preparing guidelines for board reporting matters—to ensure compliance and mitigate potential liability risks.

In addition, with respect to ISMS-P certification, businesses should note that the certification review process is expected to become more rigorous, and that the Personal Information Protection Commission has indicated that it will actively revoke certifications in light of the seriousness of violations.

B. Need to strengthen monitoring systems and revise incident response processes

The scope of incidents subject to data breach notifications and the required notification items have been broadened, and notably, the notification obligation now extends to circumstances where only the possibility of a data breach or similar incident has been identified, even if no actual breach has been confirmed. Companies should therefore review and update their existing incident response processes. In particular, it has become increasingly important to enhance monitoring at pre-breach stages (e.g., upon detection of a security incident) and to establish corresponding response mechanisms at an earlier stage.

As these changes may necessitate amendments to internal regulations or policies, as well as adjustments to the roles of relevant departments, companies should begin preparations well in advance of the Amended PIPA's effective date.

Lee & Ko's Data Privacy & Cybersecurity (**DPC**) Practice Group comprises more than 50 professionals—including dedicated privacy attorneys, former regulatory officials, and information security and technology experts—and maintains close collaborative relationships with external IT and cybersecurity specialists. Through this integrated network, we provide fast and accurate one-stop advisory services across the full spectrum of data protection and information security

matters, including the establishment of information security governance frameworks, incident response relating to data breaches and similar leakage/infringement incidents, and assistance with ISMS and ISMS-P certification.

Should you require advice regarding the Amended PIPA or any other data protection or information security matters, please do not hesitate to contact Lee & Ko's DPC Practice Group.

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

Lee & Ko

Seoul, Korea | SeoCho, Korea | PanGyo, Korea | Beijing, China | Ho Chi Minh City, Vietnam | Hanoi, Vietnam

+82.2.772.4000 | mail@leeko.com | www.leeko.com