



March 2026

# NEWSLETTER

Data Privacy & Cybersecurity Group

## CONTACT



Partner  
**Hwan Kyoung KO**  
T: +82.2.2191.3057  
E: [hwankyung.ko@leeko.com](mailto:hwankyung.ko@leeko.com)



Senior Advisor  
**Seok Young JANG**  
T: +82.2.772.4840  
E: [seokyoung.jang@leeko.com](mailto:seokyoung.jang@leeko.com)



Senior Advisor  
**Jeongsam KIM**  
T: +82.2.6386.7856  
E: [jeongsam.kim@leeko.com](mailto:jeongsam.kim@leeko.com)



Senior Advisor  
**Choonwhan BAE**  
T: +82.2.6386.0891  
E: [choonwhan.bae@leeko.com](mailto:choonwhan.bae@leeko.com)



Advisor  
**Jongseob PARK**  
T: +82.2.6386.6247  
E: [jongseob.park@leeko.com](mailto:jongseob.park@leeko.com)



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

## Amendments to the Network Act Passed by the National Assembly

### ••• Strengthening Information Security Governance and Incident Response Frameworks

Following the passage of amendments to the Personal Information Protection Act (PIPA) by the National Assembly on February 12, 2026, the National Assembly also approved amendments to the Act on Promotion of Information and Communications Network Utilization and Information Protection (Network Act) on March 12, 2026. In recent months, cybersecurity incidents — or suspected incidents — affecting major telecommunications carriers and financial institutions have underscored the need to strengthen information security management and incident response frameworks. Against this backdrop, multiple amendment bills were proposed, and a consolidated bill prepared by the National Assembly's Science, ICT, Broadcasting and Communications Committee has now been enacted.

The amendments focus on enhancing incident prevention and response mechanisms, strengthening corporate information security governance, and tightening regulation of illegal spam. Key measures—including the expansion of the Chief Information Security Officer's (CISO) role, mandatory establishment of information security committees, introduction of information security level assessments, enhanced certification standards for high-risk entities, and the implementation of incident response manuals and enforcement mechanisms—are expected to have a meaningful impact on corporate information security practices. The amended Network Act will generally take effect six months after promulgation, except for provisions relating to the information security level assessment system, which will take effect one year after promulgation.

This newsletter outlines the key amendments and their practical implications.

## 1. Key Amendments



Partner  
**Tae Joo KIM**  
T: +82.2.772.4976  
E: [taejoo.kim@leeko.com](mailto:taejoo.kim@leeko.com)



Partner  
**Minchae KANG**  
T: +82.2.772.4674  
E: [minchae.kang@leeko.com](mailto:minchae.kang@leeko.com)



Partner  
**Kyung Min SON**  
T: +82.2.772.4918  
E: [kyungmin.son@leeko.com](mailto:kyungmin.son@leeko.com)



Senior Foreign Attorney  
**Jaeyoung CHANG**  
T: +82.2.6386.6261  
E: [jaeyoung.chang@leeko.com](mailto:jaeyoung.chang@leeko.com)

### 1) Strengthening Information Security Governance

The amendments enhance corporate governance frameworks to promote more structured and effective information security management.

In particular, major information and communications service providers are now required to endeavor to secure personnel with relevant expertise and sufficient budget for information security (Article 45(5)).

In addition, service providers (other than small and medium-sized enterprises) must designate an executive officer as the CISO. The CISO's responsibilities have been expanded to include (i) oversight of personnel and budgeting for information security, and (ii) reporting on information security status and key matters to the board of directors (Article 45-3).

Further, certain service providers meeting prescribed thresholds must establish and operate an information security committee to deliberate on information security matters, with the CISO serving as chair (Article 45-4).

The Ministry of Science and ICT (**MSIT**) is also authorized to conduct annual information security level assessments for designated entities and to disclose the results or issue recommendations for improvement (Article 45-5).

### 2) Enhancements to the Information Security Management System (ISMS) Certification Regime

Building on the comprehensive reform plan announced on December 6, 2025 to enhance the effectiveness of ISMS and ISMS-P certifications, the amended Network Act further strengthens the ISMS certification framework.

Under the amendments, entities that process large volumes of data or whose services have significant societal impact may be subject to enhanced certification standards and procedures (Article 47-7(2)). In addition, ISMS certification may be revoked in cases of material violations of applicable information security laws (Article 47(10)(4)).

### 3) Strengthening Incident Response and Investigation Frameworks

The amendments refine reporting, notification, and analysis requirements to enable more prompt and systematic responses to cybersecurity incidents.

Service providers are now required to report incidents — including the timing and response status—within 24 hours of becoming aware of the incident (Article 48-3(1)).

Where certain incidents prescribed by Presidential Decree occur, service providers must promptly notify affected users (Article 48-3(4)).

The scope of incident analysis has been expanded from focusing solely on the “cause” to covering both the “occurrence and cause” of incidents (Article 48-4).

An Incident Investigation Review Committee will be established under the MSIT to deliberate on matters such as the need for investigation and the formation of joint public-private investigation teams (Article 48-2(7)).

In addition, designated entities operating information and communications networks must prepare and submit incident response manuals tailored to the scale and nature of their services, in accordance with standard guidelines issued by the Ministry. The Ministry is also authorized to review the implementation of such manuals (Article 48-9).

#### **4) Introduction of Sanctions and User Protection Measures**

To strengthen accountability, the amendments introduce new enforcement tools in relation to cybersecurity incidents.

Penalty surcharges may be imposed for failure to comply with corrective orders, refusal to submit materials, or obstruction of investigations (Article 48-7).

Further, where incidents occur repeatedly (two or more times within five years) due to willful misconduct or gross negligence, administrative fines of up to 3% of relevant revenue may be imposed (Article 48-8), subject to certain exceptions under the PIPA.

The amendments also introduce user protection provisions requiring service providers to take necessary measures to prevent the spread of harm and to facilitate prompt remedies, and to report such measures to the Ministry (Article 48-10).

#### **5) Strengthening Regulation of Illegal Spam**

The amendments also tighten regulation of illegal spam, particularly in relation to bulk messaging services.

Where a party outsources the transmission of commercial advertising messages, such outsourcing must be made only to

entities certified under the Telecommunications Business Act (Article 50-3).

Where a service is used for unlawful transmission of advertising messages, the service provider must take prescribed measures, including (i) immediate suspension of such transmissions, (ii) denial of service or termination of contracts, (iii) inspection and remediation of security vulnerabilities, (iv) improvement of terms of service, and (v) implementation of recurrence prevention measures (Article 50-4(4)).

In addition, violations of advertising message transmission regulations may result in administrative fines of up to 6% of related revenue, significantly strengthening enforcement.

## **2. Key Implications**

### **1) Need to Strengthen Information Security Governance**

As with the recent amendments to the PIPA, the amended Network Act places significant emphasis on strengthening corporate information security governance. Companies should therefore review and enhance their internal governance structures, including the expanded role of the CISO, the requirement to establish information security committees, and the introduction of information security level assessments.

In addition, as enhanced ISMS certification standards may apply to high-risk entities, such companies should proactively upgrade their security management systems. Given that certification may be revoked in cases of material legal violations, ongoing compliance and post-certification management will also become increasingly important.

### **2) Need to Review Incident Response Processes and Internal Policies**

The amendments introduce significant changes to incident response and investigation frameworks, including new user notification obligations and the establishment of the Incident Investigation Review Committee. Companies should comprehensively review their existing incident response processes in light of the expanded scope of investigation and analysis and the introduction of mandatory incident response manuals.

In particular, incident response manuals, reporting timelines, and notification procedures will play a critical role in practice. Companies are therefore advised to update relevant internal policies and systems in advance of the amendments taking effect.

Moreover, given that repeated incidents caused by willful misconduct or gross negligence may result in administrative fines of up to 3% of revenue, post-incident remediation measures, security investments, and internal controls are likely to be key factors in determining enforcement outcomes.

### 3) Need to Strengthen Spam Compliance

With the introduction of administrative fines of up to 6% of relevant revenue for violations relating to advertising messages, the importance of internal controls and compliance frameworks in this area will increase significantly.

In addition, as outsourcing of advertising message transmission is restricted to certified entities, companies utilizing messaging services should review their vendor selection processes and contractual arrangements accordingly.

Lee & Ko's Data Privacy & Cybersecurity Practice Group comprises more than 50 professionals, including specialized privacy lawyers, former regulators, and security technology experts, and maintains close collaboration with external IT and security specialists. The group provides comprehensive, one-stop advisory services across all areas of data protection and information security, including governance design, incident response, and ISMS/ISMS-P certification support.

If you require advice in relation to the amended Network Act or other data protection and cybersecurity matters, please feel free to contact Lee & Ko's Data Privacy & Cybersecurity 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](#)



Seoul, Korea | SeoCho, Korea | PanGyo, Korea | Beijing, China | Ho Chi Minh City, Vietnam | Hanoi, Vietnam  
+82.2.772.4000 | [mail@leeko.com](mailto:mail@leeko.com) | [www.leeko.com](http://www.leeko.com)