Yulchon Legal Update

February 2026

Legislative and Regulatory Trends in Data Protection and Cybersecurity

1. Introduction

Recent large-scale data breaches across major sectors - including telecommunications, retail and finance sectors have sparked significant public concern. Consequently, the National Assembly and government agencies are advancing legislative amendments and stricter regulations to bolster the prevention of—and response to—cybersecurity threats targeting critical networks and personal data.

In this Legal Update, we examine the legislative bills under deliberation in the National Assembly and highlight the government's latest policy directions.

2. Key Contents of the Proposed Amendments

Cybersecurity incidents relating to information and communications networks are governed by the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (the "**Network Act**"), which falls under the jurisdiction of the Ministry of Science and ICT (the "**MSIT**"). Meanwhile, personal data breaches are governed by the Personal Information Protection Act (the "**PIPA**"), which is overseen by the Personal Information Protection Commission (the "**PIPC**"). Although the Network Act and the PIPA are separate legal regimes with different scopes and competent authorities, in practice, hacking incidents often involve the leakage of personal data, and therefore regulatory issues under both statutes commonly arise simultaneously.

The key provisions of the proposed amendments to the Network Act and the PIPA currently under deliberation by the National Assembly are as follows. Once the bills listed below are passed by the National Assembly plenary session, they will be transferred to the government and promulgated, and will

Related Areas

Data & Technology

Privacy & Cybersecurity

IP & Technology

Contact

Sun Hee KIM
+82-2-528-5838
kimsh@yulchon.com

Na Ray KIM
+82-2-528-5734
nrkim@yulchon.com

Sang Ho BAE
+82-2-528-6110
shbae@yulchon.com

Syng Hyok CHOI
+82-2-528-6156
synghyokchoi@yulchon.com

Hye Jin YUN
+82-2-528-6167
hjyun@yulchon.com

take effect six months after the date of promulgation. However, the provisions concerning information security level assessments will take effect one year after promulgation, and the mandatory implementation of ISMS-P will take effect from July 1, 2027.

The proposed amendments primarily address (1) the improvement of data protection and security governance and the strengthening of information management systems, and (2) raising the effectiveness of incident response, related investigations and sanctions in the event of security incidents.

The Network Act applies to information and communications service providers ("**ISPs**"), which means businesses that provide information or mediate provision of information through telecommunications network. This is a broad term that encompasses all types of online and mobile services (e.g. e-commerce, social media, fintech, mobile banking). In this Legal Update, we refer to them as ISPs or companies.

Category	Network Act Amendment	PIPA Amendment
Governance improvements and strengthening of information management systems	• Chief Information Security Officer's ("**CISO**") duties will include: (i) management of personnel and budgeting necessary for information security; and (ii) reporting the information security status to the board of directors. • ISPs above certain thresholds will be required to establish an information security committee. • Businesses above certain thresholds will be subject to annual information security level assessments. • ISMS certification standards and procedures will be strengthened, taking into account the scale of data processing and social impact.	• The CEO will be the person holding the ultimate responsibility for the processing and protection of personal data. Duties of the Chief Privacy Officer ("**CPO**") will include: (i) securing and managing the personnel and budget necessary for personal data protection, and (ii) reporting on the status of personal data protection to the CEO and the board of directors. • Data controllers exceeding certain thresholds will be obliged to (i) get approval from the board of directors regarding the appointment and dismissal of the CPO and to (ii) report to the PIPC regarding the designation of the CPO. • Data controllers that meet certain thresholds will be obligated to obtain ISMS-P certification.

Category	Network Act Amendment	PIPA Amendment
Incident response, investigations and sanctions	• ISPs should notify users within 24 hours from becoming aware of the occurrence of a cybersecurity incident. • Where the Cybersecurity Incident Investigation and Review Committee under the MSIT determines that an investigation into whether a cybersecurity incident has occurred is necessary, the MSIT may investigate the occurrence and cause of the cybersecurity incident and order the company to take necessary measures. • Charge for compelling performance may be imposed for failure to comply with corrective orders, refusal or false submission of materials, or obstruction of investigations (up to 0.03% of average daily sales per day). • Administrative surcharges of up to 3% of annual revenue may be imposed where cybersecurity incidents caused by intent or gross negligence recur within five years. • ISPs should establish cybersecurity incident management and response manuals.	• The scope of "data breach" that require notifying data subjects and reporting to the PIPC will be expanded to include falsification/ alteration and damage, in addition to the data loss, theft, and leakage (collectively, "data breach, etc."). • Where a data breach, etc. (to be specified by Presidential Decree) poses a significant impact and level of risk to data subjects, the data controller must notify all affected data subjects without delay upon becoming aware of the possibility that such a data breach, etc. may have occurred. • Data breach notice to the data subjects should include information regarding data subjects' legal rights and the methods for exercising such rights. • Enhanced administrative surcharge (up to 10% of total revenue) may be imposed where: (i) a person who has been subject to an administrative surcharge due to intent or gross negligence repeats the same type of violation within three years; (ii) a violation subject to an administrative surcharge is committed with intent or gross negligence and affects 10 million or more data subjects; or

Category	Network Act Amendment	PIPA Amendment
Incident response, investigations and sanctions		(iii) personal data breach, etc. occurred as a result of failure to comply with a corrective order issued by the PIPC. Meanwhile, administrative surcharge may be reduced on grounds of large investments in data protection in terms of budgets, personnel, facilities, and equipment (to be specified by Presidential Decree).

Meanwhile, the MSIT has included "response to hacking incidents in the private sector" as a key issue in its Work Plan for 2026. In addition, the PIPC has disclosed its investigation policy directions, including areas to be prioritized for investigation in 2026 and improvements to investigation systems and procedures. The main points announced by the two authorities are summarized below.

MSIT	PIPC
• Rapid investigation of cybersecurity incidents and transparent disclosure of results • Strict enforcement against legal violations • Ex officio investigations where hacking indications are detected • Strengthened sanctions (e.g., introduction of administrative surcharge for repeat offenders, enforcement fines for failure to implement recurrence-prevention measures)	• Areas to be prioritized for investigation - Data controllers that handle a large volume of personal data will be prioritized, taking into account the frequency of incidents, the nature of the services provided, and the sensitivity of the processed data - Inspections of the processing of high-risk personal information, such as biometric and video data - Monitoring of major web and app services to identify dark patterns, including practices that distort or manipulate users' choices - Inspections on the personal data processing practices in the entertainment industry (e.g., excessive collection of children's and adolescents' personal data at concert venues)

MSIT	PIPC
	- Inspections on AI recruitment solutions and their business users to assess whether the transparency requirement is fulfilled, including whether the AI recruitment solutions constitute automated decision-making, whether explanation obligations are fulfilled, and whether key evaluation criteria are disclosed - Strengthened obligations of major public systems to conduct vulnerability assessments and to establish remedial measures - Inspections on the legality and security of the transfer and destruction of users' personal data in connection with corporate M&As and insolvency (bankruptcy or rehabilitation) proceedings • Improvements to investigation systems and processes - Strengthened functions of the data breach report center - Introduction of (1) a charge for compelling performance for failure to submit materials and (2) evidence preservation orders - Regularized inspections of large-scale data controllers - Strengthened standards for imposing an administrative surcharge - Establishment of standards for proactive large-scale preventive investments - Expansion of corrective orders to include preventive measures - Introduction of enforcement fines for failure to comply with corrective orders

3. Key Takeaways for Businesses

As discussed above, the National Assembly and the government are encouraging companies to take proactive measures to prevent information security incidents while also calling for **stronger data protection and information security governance**. In light of these regulatory developments, companies should focus their responses on the following areas:

- **Assess your current information security status**. The proposed amendments contemplate differentiated regulatory obligations based on factors such as a company's revenue size, the nature of its services, the types and volume of personal data processed, and its potential social impact. Therefore, the first step would be to identify the level of regulation applicable to your business and assess your current information security status based on the updated requirements.

- **Improve your information security and data protection governance framework**. The proposed amendments expand the scope of duties and authority of the CISO and CPO and expressly specify the responsibilities of the company's representative, thereby strengthening governance requirements. Accordingly, companies should review whether their current information security and data protection governance framework satisfies the enhanced statutory standards and whether the responsibilities and authorities of the CISO and CPO are clearly defined in accordance with the law.

- **Invest and strengthen your information security and data protection organization**. The proposed amendments strengthen ex ante regulatory oversight, such as regular information security level assessments, mandatory ISMS-P certification, and the obligation to prepare cybersecurity incident management and response manuals. At the same time, they grant CISOs and CPOs the authority and responsibility to manage personnel and allocate budgets for the necessary information security. Companies should therefore establish a system for operating an information security organization of an appropriate size on an ongoing basis.

In addition to preventive measures, there is a growing need to establish frameworks that enable prompt and effective **response to cybersecurity and personal data breach incidents**.

- **Review your incident response policies and align them with statutory requirements**. The proposed amendments impose an obligation to prepare cybersecurity incident management and response manuals and expand notification obligations to users and data subjects, thereby strengthening incident response regulations. Companies should proactively assess whether their existing incident response procedures, internal reporting systems, and notification processes satisfy the strengthened requirements and implement necessary improvements.

- **Establish a prompt and effective response system for regulatory authorities' requests for information, investigations and corrective orders**. The proposed amendments strengthen sanctions for failure to comply with corrective orders or refusal to submit materials, and regulatory authorities have indicated that they will strictly enforce sanction provisions to ensure the effectiveness of investigations. Accordingly, companies should refine internal decision-making procedures and response processes to enable prompt and appropriate responses to regulatory demands, and may consider establishing a dedicated organization or task force to handle regulatory matters where necessary.

- **Establish a post-incident management system to prevent the recurrence of incidents**. As the proposed amendments strengthen sanctions for repeated incidents, companies should identify root causes and improvement measures and reflect them in their information security management systems to ensure that the same type of incident does not recur.

Yulchon team, drawing on extensive experience in advising on governance improvements, ex ante regulatory compliance, ISMS-P certification, and responses to cybersecurity incidents and personal data breaches, will provide strategic support to help companies respond proactively in the evolving regulatory environment.