LIN LLC

Tech Legal Insights

A.P.T. – Personal Information Protection Team October 2026

The Evolving Legal Significance of Privacy Assessments and Certifications - Follow-Up Inspections of Privacy Policies and the Strengthening of ISMS-P Audits

This year's National Assembly audit of government agencies revealed that penalty surcharges imposed on companies responsible for personal data breaches from 2022 through the first half of this year totaled approximately KRW 700 billion. Moreover, under the amended Personal Information Protection Act (the "PIPA"), which took effect on September 11, penalty surcharges of up to 10% of total revenue may now be imposed for repeated or serious violations, significantly increasing the financial burden that a security incident places on a company. Notably, the recent policy direction of the Personal Information Protection Commission (the "PIPC") is shifting from holding companies accountable only for what follows an incident toward evaluating how thoroughly they had built and operated their data protection frameworks before an incident. Facts established before an incident occurs, such as holding a data protection certification or investing budget and personnel in data protection, serve as grounds for reducing a penalty surcharge. The recently announced follow-up inspections of privacy policies and the overhaul of the ISMS-P audit framework are a continuation of this trend.

Against this backdrop, and following our previous TLI, which examined the principal changes to the post-violation sanctions regime under the amended PIPA, this TLI examines the responses required of companies at the privacy policy assessment stage and the ISMS-P certification and post-certification audit stages, where a company's pre-incident level of data protection management is verified and documented.

Contact

Attorney **Taeeon Koo**
T. +82-2-3477-8695
E. tekoo@law-lin.com

Attorney **Seoyeon Ahn**
T. +82-2-3477-8695
E. syahn@law-lin.com

Attorney **Heeseung Cheon**
T. +82-2-3477-8695
E. hscheon@law-lin.com

1. Intensified Oversight After Assessment and Certification

The PIPC recently announced two measures together: the results of its follow-up inspections of businesses rated "insufficient" in the 2025 privacy policy assessment, along with the resulting recommendations for improvement issued to five businesses,1 and the pre-announcement, for public comment, of a proposed amendment to the Enforcement Decree of the Personal Information Protection Act (the "Enforcement Decree") to improve certification audits under the Personal Information & Information Security Management System ("ISMS-P").2

Although the two measures differ in their subjects and procedures, they share a common thread: the supervisory authority continues to examine how personal information controllers actually operate even after a one-time assessment or certification process has concluded. The privacy policy assessment and ISMS-P were originally designed as tools to encourage voluntary improvement by personal information controllers; now, coupled with follow-up inspections and recommendations for improvement, on-site audits, and revocation of certification, they function as part of the supervisory framework.

2. Privacy Policies: Follow-Up Inspections After Assessment

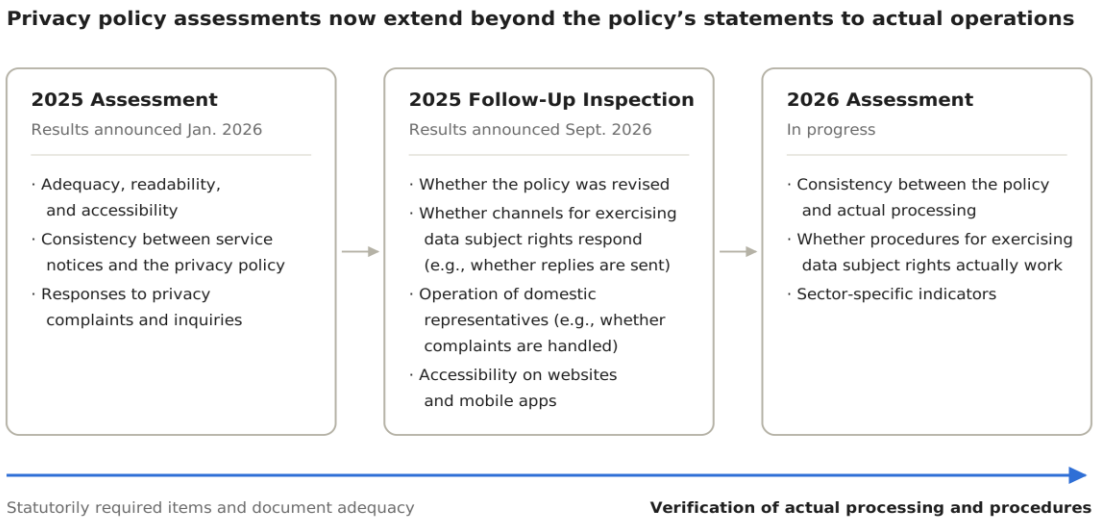
A. From Assessment to Follow-Up Inspections and Recommendations for Improvement

The privacy policy assessment has been conducted annually since 2024 under Article 30-2 of the PIPA. The PIPC Notification on privacy policy assessments provides that, where an assessment finds that improvement is needed, the PIPC may take measures such as issuing a recommendation for improvement under Article 61(2) of the PIPA and publishing the results under Article 66. The recent announcement is an instance in which such follow-up measures were actually carried out. The PIPC notified the businesses rated insufficient of their results and, for those that applied, sent assessment committee members on site to advise on how to make improvements. It then re-inspected whether the privacy policies had been revised, how the channels for data subjects to exercise their rights were operated, how domestic representatives were operated, and how accessible the privacy policies were on websites and mobile apps, in order to verify whether the improvements had been implemented.

13F, 14F, 316 Tower, 10 Seochojungang-ro 24-gil, Seocho-gu, Seoul, Korea | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com | © 2017 LIN. All Rights Reserved.

B. Expanding the Scope of Assessment: From Document Review to Inspection of Actual Operations

Under Article 30-2 of the PIPA, the privacy policy assessment evaluates whether a privacy policy properly sets out the statutorily required items (adequacy), is written in a manner that is easy to understand (readability), and is disclosed in a manner that allows data subjects to access it easily (accessibility). Recent assessments have broadened the scope of review by further examining whether the statements in a privacy policy are consistent with the company's actual processing of personal information and whether the procedures it describes, such as those for exercising data subject rights, are operating effectively. In particular, the recommendations for improvement issued following the latest follow-up inspections were directed not at the wording of privacy policies, but at the systems for operating channels through which data subjects exercise their rights and at the management and supervision of domestic representatives.



C. Legal Implications of Recommendations for Improvement

A recommendation for improvement is not, in itself, a sanction. However, many of the matters identified in the follow-up inspections bear directly on legal obligations. For example, a breach of the obligation to manage and supervise a domestic representative (Article 31-2(3) of the PIPA) may result in an administrative fine of up to KRW 20 million, and unjustly restricting or refusing a data subject's request for access (Article 35(3) of the PIPA) may result in an administrative fine of KRW 9 million for a first violation and KRW 30 million for a third or subsequent violation (Appended Table 2 of the Enforcement Decree).

13F, 14F, 316 Tower, 10 Seochojungang-ro 24-gil, Seocho-gu, Seoul, Korea | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com | © 2017 LIN. All Rights Reserved.

Accordingly, where the facts that gave rise to a recommendation constitute a breach of a legal obligation, they may, independently of the recommendation, become grounds for an administrative fine or a corrective order.

In addition, the Enforcement Decree designates the establishment, amendment, and implementation of the privacy policy as a duty of the chief privacy officer (the "CPO") (Article 32(5)(1) of the Enforcement Decree). Responses to privacy policy assessments and follow-up inspections should therefore be treated not as a mere matter of document management, but as a matter of data protection governance for which the CPO bears responsibility.

3. ISMS-P: Continuous Verification After Certification

A. Statutory Grounds for Revocation of Certification and the State of Enforcement

Article 32-2 of the PIPA already provides mechanisms for oversight after certification. The PIPC must conduct post-certification management at least once a year to maintain the effectiveness of certification (paragraph (4)), and may revoke a certification where (i) the certification was obtained by false or other fraudulent means, (ii) the certified entity refused or obstructed post-certification management, (iii) the entity no longer meets the certification standards, or (iv) the entity violated laws relating to personal information protection and the violation is serious (paragraph (3); revocation is mandatory in case (i)). Yet according to data disclosed during this year's National Assembly audit, although 115 security incidents occurred at ISMS-P-certified companies from 2021 through the first half of 2026, not a single certification was revoked. This led to questions about the effectiveness of the certification scheme, and the proposed amendment to the Enforcement Decree may likewise be understood as intended to look beyond whether certification has been obtained and to strengthen ongoing verification of whether certified entities continue to meet the certification standards.

B. Significance of the Proposed Amendment to the Enforcement Decree

The proposed amendment to the Enforcement Decree, pre-announced for public comment on September 16, implements the "Plan to Strengthen the Effectiveness of the ISMS and ISMS-P Certification Schemes" announced by the government in April 2026,[3] and its principal provisions are as follows.

13F, 14F, 316 Tower, 10 Seochojungang-ro 24-gil, Seocho-gu, Seoul, Korea | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com | © 2017 LIN. All Rights Reserved.

Item	Proposed Amendment
Combined document and on-site audits	Clarifies that document reviews and on-site audits may be conducted together in certification audits and in the annual post-certification audits (Articles 34-2(4) and 34-5 of the proposed amendment)
Technical inspection upon an incident	Where a security incident or data breach occurs during the certification validity period, technical personnel meeting specified qualifications4 conduct vulnerability assessments and penetration testing on site using inspection tools (proviso to Article 34-2(4) of the proposed amendment)
Differentiated certification standards	Establishes a legal basis for applying differentiated certification standards that take into account factors such as the scale of personal information processing and potential societal impact (Article 34-2 of the proposed amendment)
Deferral of administrative fines upon revocation	Where an entity subject to mandatory certification has its certification revoked, the administrative fine for breach of the certification obligation is deferred for one year (except where the revocation results from the use of false or fraudulent means)

In particular, the fine-deferral provision is a mechanism designed to ensure that revocation of the certification of an entity subject to mandatory certification does not immediately result in an administrative fine for breach of the certification obligation. It affords such an entity a one-year period in which to establish measures to prevent recurrence and to obtain a new certification, while excluding cases in which the certification was obtained by false or fraudulent means and revoked on that basis. With mandatory ISMS-P certification set to take effect in July 2027, the provision is significant in that it anticipates the legal consequences that revocation would carry for entities subject to the mandate and addresses them in advance.

C. Timeline for Mandatory Certification

Mandatory ISMS-P certification under the proviso to Article 32-2(1) of the PIPA will take effect on July 1, 2027, a date set in consideration of the time companies and institutions need to secure the necessary budget. The entities subject to the mandate are to be prescribed by Presidential Decree, taking into account factors such as revenue and the scale of personal information processing. The proposed amendment to the Enforcement Decree pre-announced in June 2026 would have required, among others, mobile network

13F, 14F, 316 Tower, 10 Seochojungang-ro 24-gil, Seocho-gu, Seoul, Korea | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com | © 2017 LIN. All Rights Reserved.

operators, identity verification agencies, and businesses with prior-year revenue of KRW 1 trillion or more, revenue of KRW 10 billion or more from information and communications services, and a daily average of 30 million or more domestic data subjects whose personal information was stored and managed during the three months preceding the end of the prior year, to obtain certification by December 31, 2028.5 However, the amended Enforcement Decree promulgated on September 10 contains no such provision.

Thus, while the effective date of mandatory certification has been fixed, the covered entities and the deadline for obtaining certification have yet to be determined. Companies that may be affected should therefore continue to monitor further amendments to the Enforcement Decree. Moreover, because preparing for certification takes considerable time, it would be prudent to review the scope of certification and the response framework in advance, even before the criteria are finalized.

4. How Pre-Incident Management History Affects Sanctions

Follow-up inspections of privacy policies and ISMS-P post-certification audits carry practical significance for companies because the amended PIPA requires pre-incident management history to be reflected at each stage of determining whether to impose a penalty surcharge and of calculating its amount. Based on the amended PIPA, which took effect on September 11, and Appended Table 1-5 of the Enforcement Decree, the relevant framework may be summarized as follows.

A. Determining Whether to Impose a Penalty Surcharge and the Calculation Stages

First, a penalty surcharge for a data breach is not imposed where the personal information controller has taken all measures necessary to ensure security under Article 29 of the PIPA (proviso to Article 64-2(1)(9) of the PIPA). Whether security measures were implemented in the ordinary course thus determines whether a penalty surcharge is imposed at all. Even where a penalty surcharge is imposed, the protective measures and management systems that a company put in place before the incident are reflected at each calculation stage as follows.

13F, 14F, 316 Tower, 10 Seochojungang-ro 24-gil, Seocho-gu, Seoul, Korea | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com | © 2017 LIN. All Rights Reserved.

Calculation Stage	Pre-Incident Facts Considered	Range of Adjustment
Determination of the base amount	Efforts to implement security measures, such as encryption	Imposition rate of 0.03%–2.7%, depending on the seriousness of the violation (Appended Table 1-5 of the Enforcement Decree)
Investment-based reduction	Scale, ratio, continuity, and growth of investment in personal information protection; the degree to which the business owner or representative has fulfilled its responsibilities (Article 30-3 of the PIPA); the level at which the protection framework is operated, including the CPO's role, organization, and staffing; and the level of, or efforts toward, security measures beyond statutory obligations, such as the application of enhanced protection technologies	Up to 40% of the base amount; reduction is mandatory if the requirements are met (except for violations committed intentionally or through gross negligence)
Second-stage adjustment	Data protection certification; voluntary data protection activities	Increase or reduction of up to 50%
Limits on reductions	If the violation constitutes a "very serious violation," reductions under the first- and second-stage adjustments may be disallowed in whole or in part	—
Punitive penalty surcharge	Repetition of a violation under the same subparagraph within three years from the date of a penalty surcharge disposition (intentional or grossly negligent); an intentional or grossly negligent violation causing harm to 10 million or more data subjects; a data breach resulting from failure to comply with a corrective order	Up to 10% of total revenue

Among the calculation factors above, with respect to the investment-based reduction, the PIPC published the Guide to the Investment-Based Reduction of Penalty Surcharges to coincide with the entry into force of the amended PIPA, setting out detailed criteria for each requirement and the supporting documentation required. According to the Guide, eligibility for the investment-based reduction is assessed on the basis of measures taken within the three fiscal years immediately preceding the fiscal year in which the violation occurred, and the scale of investment is verified through audit reports, fixed-asset registers, expense ledgers, personnel-cost records, among other documents. Furthermore, additional efforts relating to security measures are considered

13F, 14F, 316 Tower, 10 Seochojungang-ro 24-gil, Seocho-gu, Seoul, Korea | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com | © 2017 LIN. All Rights Reserved.

primarily with reference to the measures that were applied and in operation at the time the data breach occurred, and such measures must be set out in the internal management plan and substantiated by supporting evidence.

5. Implications

The measures discussed above demonstrate that privacy assessments and certifications cannot be treated as a domain separate from penalty surcharge sanctions. Facts identified in the course of an assessment or certification are not confined to that process; they may later serve as a basis for determining the level of sanctions when a security incident occurs.

At the same time, the standards by which a personal information controller's level of management is examined are also changing. Privacy policy assessments, ISMS-P audits, and the investment-based reduction of penalty surcharges are all moving beyond confirming whether a management framework is in place toward asking whether it is actually working. In light of this trend, responding to individual assessments or audits on a case-by-case basis is not sufficient for data protection compliance. It is important to operate day-to-day management activities systematically so that they can serve as a consistent evidentiary basis at any later stage.

That said, the criteria for entities subject to mandatory ISMS-P certification and the final terms of the proposed amendment to the Enforcement Decree to improve certification audits have yet to be finalized, and cases applying the investment-based reduction have yet to accumulate. Companies concerned should continue to monitor how the specific operation of these regimes takes shape.

***

LIN's Personal Information Protection Team under the APT (AI, Platform, Technology) Group provides companies with strategic, one-stop total legal solutions for regulatory issues.

If you have any questions regarding the above, please feel free to contact LIN's Personal Information Protection Team (Tel. +82 - 2-3477-8695), Team Leader Taeeon Koo (tekoo@law-lin.com), Attorney Seoyeon Ahn (syahn@law-lin.com), or Attorney Heeseung Cheon (hscheon@law-lin.com).

1. PIPC Press Release
2. PIPC Press Release
3. https://pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=11976
4. Intermediate grade or higher under the qualification standards for technical personnel set forth in Appended Table 1 of the Enforcement Rule of the Act on the Promotion of Information Security Industry
5. https://pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=12137

13F, 14F, 316 Tower, 10 Seochojungang-ro 24-gil, Seocho-gu, Seoul, Korea | Tel: 02-3477-8695 | Fax: 02-3477-8694
E-mail: lin@law-lin.com | © 2017 LIN. All Rights Reserved.