Yulchon Legal Update

September 2026

TMT Regulatory Briefing: Amended Personal Information Protection Act Taking Effect on September 11

— Penalty Surcharge of Up to 10% of Revenue, Strengthened CEO and CPO Responsibilities, and More

The Personal Information Protection Commission (the "**PIPC**") promulgated the partial amendment to the *Personal Information Protection Act* (the "**Amended Act**") on March 10, 2026. The Amended Act and the amendment to the *Enforcement Decree of the Personal Information Protection Act* (the "**Enforcement Decree**"), which specifies the delegated matters under the Amended Act, came into force on September 11, 2026. The Amended Act raises the upper limit of administrative surcharges for repeated or serious personal information infringements up to 10% of total revenue under certain conditions, and strengthens the ultimate liability of the business owner or representative as well as the role of the Chief Privacy Officer ("**CPO**").

In addition, the Amended Act also expands the scope of "breach incidents," which encompasses not only the leakage of personal information but also its forgery, alteration, and damage, and establishes a new obligation to notify data subjects of the possibility of the data breach even before the data controllers are able to confirm the list of data subjects affected by the breach.

The Enforcement Decree specifies in detail: the specific scope of entities subject to board resolution and reporting to the PIPC upon the appointment or dismissal of a CPO; the criteria, timing, and methods for notifying data subjects of potential breach incidents; the standards for mitigating penalty surcharges based on investments in personal information protection; and the increased levels of administrative fines.

This Legal Update examines the Amended Act and the Enforcement Decree together and summarizes the practical matters that businesses should prioritize immediately following implementation.

1. Background and Regulatory Direction

As large-scale personal information breach incidents have recurred, the focus of regulation has shifted beyond merely imposing sanctions after an incident occurs, to also requiring management-level accountability, proactive preventive investment, and prompt notification at the earliest stage of an incident.

The Amended Act treats personal information protection not as the task of individual officers but as a matter of management governance involving the representative, board of directors, and CPO. It strengthens sanctions for serious and repeated violations while introducing a mitigation incentive structure for substantive personal information protection investment.

2. Key Provisions of the Amended Act and Enforcement Decree

Category	Amendment Details	Business Impact
CEO Responsibility	Clarified that the business owner or representative bears ultimate responsibility for personal information processing and protection	Requires management-level involvement and documented evidence of budget allocation, staffing, risk management, and remedial measures
CPO Role and Reporting	Strengthened CPO's role in personnel management, budget allocation, and reporting to the representative/board of directors. Businesses above a certain threshold must obtain board approval and file a report with the PIPC upon CPO appointment or dismissal	Businesses must assess applicability based on revenue and scale of data processing
Notification of Potential Breach	Even if the affected data subjects have not been confirmed, notification must be given within 72 hours if circumstances prescribed in the Enforcement Decree are met	Necessitates changes in the initial incident assessment criteria and closer coordination among legal, security, and communications teams
Strengthened/ Mitigated Administrative Surcharges	Up to 10% of total revenue for certain serious or repeated violations. Investment and operational efforts in personal information protection specified as separate mitigating factors	Requires managing prior enforcement history alongside evidence of investment and operational track record

Category	Amendment Details	Business Impact
Increased Administrative Fines	Raises find amounts for major violations, including violations of security safeguard obligations	Elevates the importance of ongoing inspection of technical and administrative safeguards
Personal Information Protection Certification	Mandatory certification for data controllers above a certain threshold (effective July 1, 2027)	Requires advance review to determine certification applicability and preparation timeline

(1) Criteria for Board Resolution and Reporting Obligations regarding CPO

The Enforcement Decree specifies the criteria under which a data controller must obtain board approval and file a report with the PIPC upon appointment or dismissal of the CPO. For private-sector data controllers, these obligations apply where annual revenue exceeds KRW 180 billion and the data controller either (a) processes sensitive information or unique identification information pertaining to 50,000 or more data subjects, or (b) processes personal information pertaining to 1,000,000 or more data subjects. The obligations also extend to universities with 20,000 or more enrolled students, advanced general hospitals, and public system operating institutions are also included.

Data controllers subject to this obligation must file a report with the PIPC within six months from the date on which the grounds for CPO designation, change, or removal arise. Where unavoidable circumstances make it difficult to comply in time, such as difficulty convening the board of directors, an extension of up to one year may be granted upon request. Businesses that have already designated a CPO prior to the effective date must file a report within six months from the effective date of September 11, 2026.

(2) Criteria for Notifying Potential Breaches and the 72-Hour Notification Requirement

The Enforcement Decree establishes two types of situations requiring proactive notification to data subjects of the possibility of the data breach.

- Where unauthorized access has occurred to a personal information processing system or an information device used by a personal information handler, and while there are circumstances suggesting a breach incident, it is difficult to identify which data subjects' personal information has been compromised; or

- Where personal information being processed by the data controller has been confirmed to have been unlawfully traded by a third party (i.e., a partial breach incident has been confirmed), and it is recognized that personal information of other data subjects may also have been compromised.

Notification must be provided in writing or by equivalent means within 72 hours of becoming aware of the unauthorized access (in the first case) or becoming aware of the fact that the personal information has been unlawfully traded (in the second case). The notification must include: the categories of personal information potentially affected; the suspected or recognized timing and circumstances; methods for minimizing harm; the rights of data subjects and how to exercise them; and a statement that additional notification will be provided once the breach status is confirmed. If it is subsequently confirmed that no actual breach incident occurred, that fact must also be promptly notified.

Where there are legitimate reasons such as inability to identify contact information, notification may be substituted by posting on the organization's website for at least 30 days.

(3) Mitigation Criteria for Administrative Surcharges Based on Investment

The Amended Act newly establishes investment and operational efforts for personal information protection as grounds for penalty surcharge mitigation, and the Enforcement Decree specifies the factors for assessing such mitigation. The relevant factors include: (a) the scale, proportion, and continuity of investment in budget, personnel, facilities, and equipment; (b) the degree to which the business owner or representative has fulfilled their responsibilities; (c) the operational maturity of the personal information protection framework, including the CPO's role and organizational structure; and (d) additional efforts toward security safeguards. A calculation procedure has been established so that investment-based mitigation may reduce the administrative surcharge by up to 40% of the base amount for calculating the administrative surcharge.

(4) Increased Administrative Fine Standards

The Enforcement Decree raises administrative fine amounts that had previously been set below the statutory ceiling. Most notably, for violations of the obligation to implement security safeguards, the fines have been increased from the previous amounts of KRW 6 million (1st offense), KRW 12 million (2nd offense), and KRW 24 million (3rd offense or more) to KRW 9 million, KRW 18 million, and KRW 30 million, respectively. As a result, the sanction risk has materially increased even for administrative and technical obligation violations that do not trigger administrative surcharges.

3. Immediate Action Items for Businesses

Checkpoint	Practical Review Items
CPO Applicability Assessment	Verify annual revenue, total number of data subjects whose personal information is processed, and the number of data subjects whose sensitive information or unique identification information is processed, per legal entity; confirm whether the KRW 180 billion + 50,000/1,000,000 data subject thresholds are met
Board Resolution and Reporting Procedures	Establish board resolution procedures for CPO appointment/dismissal, and set up a management framework for the responsible department, deadlines, and reporting forms. Businesses that have already designated a CPO must file reports by March 11, 2027
Incident Assessment Framework	Incorporate into the incident response manual: criteria for detecting suspected circumstances prior to "confirmed breach," the starting point for the 72-hour clock, the designated decision-maker, evidence preservation, and notification approval procedures
Investment Documentation	Systematically preserve board and management reports so that security/privacy budgets, dedicated personnel, facility/solution investments are documented, together with their continuity, the CEO involvement, and CPO's organizational and reporting structure
Enforcement History	Centrally manage recent penalty surcharges, corrective orders, and the status of recurrence prevention measures; assess exposure to the 10% penalty surcharge track for repeated or serious violations
Administrative Fine Controls	Reflect the increased administrative fine items—security safeguard measures, document submission/investigation cooperation, corrective order compliance, etc.—in the compliance checklist

4. Compliance Implications

This amendment is significant because it expands the regulatory assessment criteria for personal information protection well beyond the simple question of whether an incident has occurred. Regulators will now also examine: whether the representative and board of directors manage personal information

protection as a business risk, backed by adequate budget, personnel, and controls; whether a framework exists that allows the CPOs to fulfill their role independently; and whether prompt and reasonable assessment and notification (even at the suspicion stage) before a breach was confirmed.

In particular, as the Enforcement Decree has finalized the criteria for CPO reporting obligations and deadlines, the specific requirements and 72-hour deadline for notifying potential breaches, and the assessment factors for investment-based mitigation, businesses must go beyond merely formally amending their internal policies and incident response manuals. They need to ensure that the actual decision-making, reporting, budget execution, and incident assessments are documented as they happen – not reconstructed after the fact.

Because the investment in personal information protection and management-level involvement may now directly affect penalty surcharge calculations, the routine operation of governance frameworks and documentation of evidence are expected to become core elements of data protection compliance framework.

Related Areas

Integrated TMT Center	TMT	Data Privacy

Contact

Doil SON
+82-2-528-5836
dison@yulchon.com

Kum Ju SON
+82-2-528-5094
kjson@yulchon.com

Seung Hyuck HAN
+82-2-528-5633
shhan@yulchon.com

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

Dayeon AHN
+82-2-528-5254
dyahn@yulchon.com

Seung Jin HEO
+82-2-528-5567
sjheo@yulchon.com

So Jung KIM
+82-2-528-5057
sojungkim@yulchon.com

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

YULCHON 律村 Attorneys at Law YULCHON

Material included in our newsletter has been prepared for informational purposes only and is not offered as legal advice on any particular matter. Yulchon and contributing authors disclaim all liability for the newsletter's content and are not responsible for any third-party content which can be accessed through this newsletter.

Copyright 2026 Yulchon LLC. All rights reserved