SHIN&KIM
법무법인(유) 세종

PIPC Announces “Transition Plan toward a Prevention-Focused Personal Information Management System”

2026.05.15

On May 12, 2026, the Personal Information Protection Commission (the “PIPC”) reported the “Transition Plan toward a Prevention-Focused Personal Information Management System” (the “Transition Plan”) at a Cabinet meeting presided over by the President. The following sections outline the key provisions and implications of the Transition Plan.

1. Background

As the scale and scope of personal information usage expand rapidly across all sectors—driven by AI, digital transformation, and the growth of the platform economy—data breaches are becoming increasingly massive. Furthermore, it is becoming clear that post-incident penalties alone are not adequate for effective damage recovery. Accordingly, through the Transition Plan, the PIPC aims to move beyond the existing “post-incident, penalty-centric” framework toward a proactive “pre-incident prevention and management” system that incentivizes substantive risk management and investment in prevention.

2. Key Provisions

The PIPC proposed the following specific tasks in accordance with the three strategic directions of the Transition Plan.

(1) Increasing sanctions for serious and repeated violations

(Introduction of Punitive Penalty Surcharge) In cases of intentional or gross negligence for repeated violations within three years, or serious incidents affecting 10 million or more people, a penalty surcharge of up to 10% of annual revenue will be imposed. This represents a substantial increase from the existing 3% cap, following the amended Personal

Information Protection Act (the “PIPA”) which is set to take effect on September 11, 2026. Furthermore, an amendment to the Enforcement Decree has strengthened the basis for calculating the penalty surcharge. Effective May 19, 2026, the amount will be determined by the higher of the preceding year's revenue or the 3-year average, replacing the current three-year average standard.

Category	Current	Amended	Effective Date
Punitive penalty surcharge	3% of revenue	10% of revenue in cases of serious incidents or repeated violations	September 11, 2026
Basis for calculating revenue	3-year average	The preceding year’s revenue or the 3-year average (whichever is greater)	May 19, 2026
Compulsory investigative authority	Administrative fine of up to 30 million KRW for non-cooperation	Implementation of non-compliance fines and orders for the preservation of evidence	Bill proposed (Feb. 2026)

(Enhancing compulsory investigative authority and introducing whistleblower rewards) To ensure prompt investigations and enforcement, non-compliance fines for non-cooperation will be introduced, as well as increased sanctions for the concealment or destruction of evidence. Furthermore, a whistleblower reward system will be implemented to encourage the reporting of violations. However, for small businesses, the opportunity for corrective action will be granted initially for minor violations, though a policy of strict enforcement will be maintained for repeated violations.

(2) Expanding voluntary investment in data protection and establishing a risk- based management system

(Incentivizing preventive security measures) To encourage proactive data protection, incentives such as reductions in penalty surcharge will be provided for voluntary preventive measures that exceed statutory requirements. These include preemptive safety measures, the operation of effective safety management systems, and investments in proactive cybersecurity. Key considerations are as follows.

Category	Examples of Key Considerations
Cybersecurity investment	Cybersecurity investment ratio exceeding industry average (e.g., 9.6% for finance and 6% for ICT)
Safety management system	Dedicated team/personnel, continuous risk management, and rapid recovery capabilities
Additional protection measures	Encryption, multi-factor authentication (MFA), and vulnerability disclosure/coordinated vulnerability disclosure (VDP/CVD) programs, etc.

(Establishing a risk-based management system) A differentiated, risk-based management framework will be implemented according to the severity of the risk. Inspections will be expanded across the entire supply

chain—including public institutions, corporations, cloud service providers, specialized outsourcers, and system suppliers—provided they process data for over 1 million individuals. Furthermore, starting in 2026, the scope of inspections will be extended to include funeral service providers, customer service centers, matchmaking agencies, and K-12 EdTech providers.

(Institutionalizing Privacy by Design) Given that it is difficult to detect or prevent breaches once a service has launched, the Privacy by Design (the "PbD") principle will be institutionalized. The PbD principles will be incorporated into the criteria for personal information impact assessments and ISMS-P certification. The ISMS-P certification system will be categorized into tiers (basic, standard, and enhanced), and the range of entities subject to such certification will also be expanded.

Category	Enhancements	Implementation Schedule
ISMS-P Certification	Strengthening certification standards (introducing basic, standard, and enhanced tiers), implementing continuous monitoring, and mandating compliance for key public and private data processors	Amendment to administrative notice (second half of 2026); Mandatory implementation (July 2027~)
Personal information impact assessment	Integrating PbD principles, improving assessment criteria and methodologies, expanding applicability to the private sector, and establishing impact assessment system for large-scale cross-border data transfers	Policy development (2026); Establishment of legal basis (2026~)

(Strengthening executive responsibility and fostering specialists) Effective September 11, 2026, the amended PIPA designates the CEO as the individual with ultimate responsibility for personal information protection. Companies meeting specific thresholds—processing data for over 1 million individuals with annual revenues exceeding 180 billion KRW—are now mandated to appoint a CPO possessing prescribed qualifications and experience (affecting approximately 700 companies). Furthermore, an early warning system for threats, based on collaboration between CPO councils, will become operational in 2026. Graduate programs for cultivating personal information protection specialists will be expanded across various regions. Additionally, newly designed, role-specific training programs will be implemented for policy officers, developers, and incident response teams.

(3) Swift relief and recovery support

(Facilitating statutory damages) Under the amended PIPA, effective September 11, 2026, the burden of proof regarding intent or negligence in data breaches will shift to corporations/organizations, and a statutory damages system (capped at 3 million KRW) will be implemented.

(Strengthening citizens' rights) There will be thorough inspections for deceptive practices, such as dark patterns, that mislead users or make it difficult to edit personal information, withdraw consent, or close accounts. The role of the Personal Information Infringement Reporting Center will be gradually strengthened to provide a comprehensive support

system, including professional legal counseling and victim recovery assistance.

(Severe punishment for illegal distribution) In cases of sensitive data leaks, social media and the dark web will be monitored to detect and to remove any illegally distributed information. Furthermore, in coordination with law enforcement agencies, illicit distributors and users will be tracked down and prosecuted to the fullest extent of the law as part of a rigorous response strategy.

3. Implications

- **(Thorough preparation for punitive penalty surcharge is essential)** Punitive penalty surcharges of up to 10% of revenue for serious or repeated violations represent a critical financial risk that could threaten corporate existence. As the criteria for calculating these penalty surcharges have become more stringent, it is essential to closely examine current personal information security systems and establish an internal monitoring framework to prevent major incidents or recurring breaches. To this end, it is necessary to strengthen the CPO's authority and overhaul internal policies to ensure mandatory cooperation among departments
- **(Explore ways to leverage incentives for preventive security measures)** Given that the PIPC plans to actively recognize investments in proactive security measures that exceed statutory standards as grounds for reducing penalty surcharges, a strategic review of plans for increasing security budgets, personnel, and systems is necessary. Considering that proactive investment is not merely an expense but a means to mitigate potential financial risks, it is advisable to take timely actions, such as investing in such security measures in accordance with the incentive requirements as soon as they are finalized.
- **(Need to refine framework for executive accountability)** As the CEO's responsibility for personal information protection is now explicitly codified, it is imperative to redefine the personal information governance framework at the executive level. Furthermore, careful attention must be paid to newly imposed procedural requirements, such as appointment of CPO with specific qualifications and experience, as well as the mandate for board approval and notification to the PIPC regarding the appointment, change, or removal of the CPO.
- **(Need to prepare for ISMS-P certification and PbD implementation)** As the scope of companies required to obtain ISMS-P certification expands and the principles of PbD are set to be incorporated into the criteria for personal information impact assessments, it is essential to proceed with preparations without delay. In particular, the introduction of impact assessment system for large-scale cross-border data transfers may impose an additional compliance burden on companies with global operations, warranting close attention.
- **(Need to continuously monitor trends in relevant legislative amendments)** Among the tasks outlined in the Transition Plan, initiatives such as the introduction of non-compliance fines, the whistleblower reward system, and increased punishment for illegal distributors are currently in the legislative proposal stage or pending amendments to enforcement decrees or administrative notices. As such, it is necessary to build the corporate response framework in phases while continuously monitoring for subsequent legislative developments regarding these initiatives.

About Shin & Kim's ICT Group (Data Privacy Team)

Shin & Kim possesses distinctive expertise and an extensive professional network in the field of personal information protection (including former PIPC Chairman Jong-In Yoon, former Vice Minister of the Interior and Safety Young-Ho Kim, and former Vice Minister of Science and ICT Jae-You Choi). We provide specialized advisory services on personal information protection to corporations, covering domestic and international regulations such as the PIPA and the GDPR, responses to data breaches, and the establishment of personal information protection compliance frameworks. In particular, we possess expertise in establishing internal data governance structures, as evidenced by our participation in drafting and reviewing the recently published CPO Handbook by the PIPC/KCPO. Furthermore, we have played a leading role in the private sector regarding the second amendment to the PIPA, the enactment of subordinate statutes, and related institutional improvements. We provide legal advice on pseudonymized information, data utilization, regulatory trends in the ICT industry, government relations, legislative consulting, regulatory impact analysis, and corporate strategy development. Please contact us any time if you have any questions or require more specialized information.

[Korean version] 개인정보보호위원회, 「예방 중심 개인정보 관리체계 전환 계획」 발표

Key Contacts

Jong-In Yoon
Senior Advisor

+82-2-316-4209
jiyoon@shinkim.com

Sinook Kang
Senior Partner

+82-2-316-4059
sokang@shinkim.com

Jeong Ho Ahn
Partner

+82-2-316-2891
jhahn@shinkim.com

Jin Hong Noh
Partner

+82-2-316-1639
jhnoh@shinkim.com

Ho Sang Yoon
Partner

+82-2-316-2584
hsyoon@shinkim.com

Hunyoung Choi
Associate

+82-2-316-7247
hyochoi@shinkim.com

Hyeonjeong Yoo
Associate

+82-2-316-1865

hjyoo@shinkim.com