SHIN&KIM
법무법인(유) 세종

PIPC Announces "Transition Plan toward a Prevention-Focused Personal Information Management System" – Risk-Based Inspections to Begin in June

2026.06.01

On May 22, 2026, the Personal Information Protection Commission (the "PIPC") announced the "Transition Plan toward a Prevention-Focused Personal Information Management Framework" (the "Transition Plan") at the Economic Ministers' Meeting. It further elaborates on the initial transition plan that was reported to the Cabinet on May 12, 2026, which was previously discussed in our newsletter (link). The Transition Plan is intended to accelerate the shift toward a prevention-focused personal information protection framework that preemptively identifies and manages risks of personal information breaches and leaks.

With the rapid proliferation of AI, platform, and cloud-based services, both the scale and methods of personal information processing are evolving quickly, leading to increased risks of personal information breaches, including hacking incidents, across industries. In response, the PIPC plans to strengthen risk-proportionate inspections and management to encourage companies to proactively implement necessary safeguards, while reinforcing the overall personal information protection framework by expanding investment in data protection, fostering a robust personal information protection ecosystem, and cultivating a culture of trust.

The following sets out an overview of the key aspects of the Transition Plan and its implications.

1. Establishing and Operating a Risk-Based Preventive Management Framework

(Risk-Based Inspections) The PIPC plans to classify personal information processing sectors into high, medium, and low-risk categories, taking into account the scale, sensitivity, and industry-specific characteristics of personal information processing, and to conduct differentiated inspections and management measures accordingly.

For high-risk sectors, the PIPC plans to focus on and conduct in-depth oversight of internal control operations by performing inspections after publicly disclosing the inspection areas in advance, issue corrective recommendations for any deficiencies identified, and continuously track and monitor the implementation of such measures over a certain period. These inspections targeting high-risk sectors are expected to be primarily led by the Preliminary Inspection Division, newly established at the end of last year, and can be seen as aligned with the various preliminary inspections that have been underway since the beginning of this year.

Additionally, for sectors that do not fall within the high-risk category, the PIPC will promote the conduct of privacy impact assessments and the application of the Privacy by Design ("PbD") principles. It will also provide self-inspection tools and consulting support to help personal information controllers independently establish a baseline level of protection.

The classification criteria for each risk category and the corresponding preventive management measures are as follows.

[Proposed Risk-Based Preventive Management Framework]

Category	Classification Criteria	Preventive Management Measures
High-Risk	Sectors such as telecommunications, finance and health and welfare that process personally identifiable information and sensitive information, on a large scale (1 million data subjects or more)	Regular and ad hoc inspections; mandatory ISMS-P certification and privacy impact assessments; disclosure of protection-related activities, etc.
Medium-Risk	Sectors that do not fall within high or low-risk categories but require systematic inspections and management	Ad hoc and joint inspections; self-conducted impact assessments; compliance with PbD principles, etc.
Low-Risk	Cases where data subjects are difficult to identify or the impact is low (small-scale processing involving less than 10,000 data subjects)	Self-inspections; support for security measures; subscription-based consulting support, etc.

Furthermore, potential personal information breaches in emerging technology sectors, including IoT devices and agent-based AI, are expected to be preemptively included within the scope of these inspections.

(Enhancement of Preventive Protection Framework) Recognizing that the current standards for security measures have been applied uniformly regardless of the scale of personal information processing or the level of risk involved, the PIPC intends to develop a mid to long-term plan to revise the standards that would allow for tiered application and varying levels of security measures, taking into account the results of risk analysis as well as the flow and types of personal information processing. In addition, the ISMS-P certification and privacy impact assessment frameworks will be enhanced to go beyond formalistic compliance checks and evolve into continuous management and risk assessment-based frameworks that incorporate emerging technology risks and Privacy by Design (PbD) principles.

2. Facilitating the Early Expansion of Voluntary Investment in Personal Information Protection and Security

(Integration of PbD Principles) The PIPC plans to institutionalize the PbD principle, ensuring that personal information protection is embedded by default from the planning, design, and development stages of services. While the PbD certification scheme has so far been applied only to certain product categories—such as IP cameras and robot vacuum cleaners—its scope will be expanded through amendments to the PIPA. In addition, guidelines and best practices that can be referenced at the planning and design stages will be developed and disseminated. Furthermore, PbD principles will be incorporated into existing evaluation and certification frameworks, including ISMS-P, so that personal information protection becomes not merely an ex post compliance check, but a core design principle applied throughout the entire service lifecycle.

(Incentive Restructuring and Reinforcement of Accountability) The PIPC plans to revise relevant frameworks, such as incentive structures, to encourage companies to move beyond mere compliance with minimum legal requirements and expand substantive investments in personal information protection. Specifically, it is expected to encourage the inclusion of details of additional protection measures and the internal control processes of Chief Privacy Officers (CPOs) within the 'Information Security Disclosure' and to consider granting incentives such as reduction in penalty surcharges where such additional protection measures are confirmed to have been effectively implemented. Moreover, for minor violations by SMEs and micro businesses, a more lenient approach will be pursued, whereby sanctions may be mitigated on the condition that corrective actions are undertaken with technical support.

Examples of key considerations for additional protection measures are as follows:

[Examples: Additional Protection Measures Across the Entire Service Lifecycle]

Category	Examples of Key Considerations
Cybersecurity investment exceeding industry average	Proportion of investment in protection measures relative to overall IT spending (e.g., 9.6% for finance and 6% for ICT)
Establishment and operation of an effective personal information security management system	Dedicated team/personnel; continuous risk management (i.e. privacy impact assessments); and rapid recovery capabilities
Additional protection measures exceeding legal requirements	Encryption, multi-factor authentication (MFA), and vulnerability disclosure/coordinated vulnerability disclosure (VDP/CVD) programs, etc.

3. Fostering the Personal Information Protection Ecosystem and

Cultivating a Culture of Trust.

The PIPC plans to strengthen oversight across the personal information processing supply chain, including Software as a Service (SaaS), cloud services, and specialized personal information processors where large volumes of personal information are concentrated. Also, the PIPC will promote research and development of preventive Privacy Enhancing Technologies (PETs) to proactively prevent personal information breaches and misuse, as well as foster the development of specialized professionals in the field.

Furthermore, the PIPC will expand personal information protection education for children, adolescents, and other vulnerable groups, and review and improve practices—such as dark patterns—that may undermine data subjects' trust, thereby supporting the establishment of personal information protection as a culture of everyday practice.

4. Implications

- **(Need for Proactive Response to the Shift Toward a Risk-Based Inspection Framework)** This Transition Plan demonstrates that the supervisory approach of the PIPC is shifting from a sanctions-oriented, ex post model toward one centered on prevention and risk-based management. Accordingly, companies should go beyond merely verifying compliance with the minimum requirements under the PIPA and proactively assess the risks associated with its personal information processing. Such risk assessments should take into account factors including the volume and sensitivity of personal information, processing methods, and industry characteristics. Based on these risk assessments, companies are expected to establish internal monitoring and control systems commensurate with the level of risk identified.
- **(Need to Integrate Personal Information Protection Framework Across the Entire Service Lifecycle and Supply Chain)** This Transition Plan underscores that personal information protection must be consistently integrated across all stages of a service, including planning, design, development, and operation. Accordingly, companies should, from the initial planning stage, review the necessity of personal information collection, the appropriateness of processing purposes, and measures to protect data subjects' rights. They should also continuously assess emerging risk factors arising from expanded use of AI and data throughout development and operation. In addition, it is advisable to strengthen oversight and management of processors across the supply chain, along with incident response procedures. In addition, given the strengthening of personal information controllers' obligations to manage and supervise personal information processors, as well as the increasing number of enforcement actions against processors for legal violations, it is also necessary to enhance compliance frameworks related to the outsourcing of personal information processing activities.
- **(Refining CPO-Based Internal Controls and Documentation for Protection Measures)** Moving forward, the effective implementation of personal information protection activities is expected to become an increasingly important factor in audits, evaluations, and the determination of sanction levels. As the PIPC drives initiatives such as the reporting requirement for CPO designation, the disclosure of protection activities through the 'Information Security Disclosure' and the provision of incentives for additional protection measures, companies should clearly define and incorporate into their internal policies the authority and responsibilities of the CPO, personal information-related decision-making procedures, and internal control processes. Furthermore, to demonstrate that these protection measures are effectively implemented in practice, companies are advised to systematically

maintain relevant records, such as audit findings and logs of corrective actions.

- **(Continuous Monitoring of Developments)** The enforcement decree related to PIPA, as amended on May 19, 2026, is expected to be announced for public comment in the near future and the PIPC is also expected to continue providing additional details on the initial transition plan reported on May 12. Accordingly, it will be necessary to closely monitor forthcoming subordinate legislation and policy developments.

About Shin & Kim's ICT Group

Shin & Kim's ICT Group provides comprehensive, one-stop legal services by leveraging the firm's distinctive expertise and extensive professional network in the ICT sector, having consistently earned the highest client recognition in recent years. Drawing upon our deep-seated capabilities in broadcasting, telecommunications, personal information protection, and internet IT, we deliver the highest level of legal advisory services encompassing regulatory trend analysis in broadcasting, telecommunications, and ICT; government affairs, legislative improvement and legislative consulting; regulatory impact assessment; and corporate strategic planning. Furthermore, we possess extensive experience and exceptional expertise in personal information/AI compliance and risk management, providing holistic analysis and strategic responses to legal issues and regulatory risks associated with AI adoption and deployment across diverse industry sectors. Please feel free to contact us with any questions or if you require our assistance on any ICT-related legal matters.

[Korean version] 개인정보위, 「예방 중심 개인정보 관리체계 전환 계획」 발표 – 올해 6월부터 위험 기반 실태점검 본격 실시

Key Contacts

Jong-In Yoon
Senior Advisor

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

Kwang-Hee Choi
Senior Advisor

+82-2-316-4651
khchoi@shinkim.com

Sinook Kang
Senior Partner

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

Jeong Ho Ahn
Partner

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

Ho Sang Yoon
Partner

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

Sally Lim
Foreign Attorney

+82-2-316-7266
slim@shinkim.com

Dawon Lee
Associate

+82-2-316-7962
dwlee@shinkim.com