PIPC Reveals its Key Priorities and Policy Agenda for 2025

In January 2025, the Personal Information Protection Commission ("Commission") unveiled six key policy initiatives under three major strategies: fostering AI and data-driven industry growth, enhancing global leadership in data privacy, and restructuring privacy protection for digital transformation.

1. Fostering the AI Industry and Building Underlying Trust

a. Revamp Privacy Legislation for the AI Era

The Commission plans to amend the Personal Information Protection Act ("PIPA") to permit the use of original data, particularly when research cannot be effectively conducted with pseudonymized data alone. The legal framework will also expand to support AI developers' collection and use of personal data, balancing business interests with the public interest.

To enhance regulatory flexibility, the Commission will utilize sandboxes and further promote the preliminary adequacy review system. It will also empower data subjects with the right to request the deletion of synthetic media and prohibit the unauthorized creation of synthetic data that infringes on another's rights, fostering trust in new technologies. Additionally, private sector compliance will be encouraged through the recognition of data impact assessments conducted within the AI sector.

b. Establish a Foundation for Sustainable Innovation

To keep pace with rapid technological advancements, the Commission will modernize regulatory frameworks to address the unique characteristics of visual and biometric data. Pseudonymized data usage will be promoted through "personal data innovation zones," streamlined procedures, and industry-specific expert committees. The pseudonymization support platform will also expand to process unstructured data critical for AI.

To strengthen data security and usability, the Commission will invest in privacy-enhancing technologies, develop standards for privacy vulnerability assessments in large language models, and advance de-identification and deepfake prevention technologies, while commercializing privacy technologies developed in 2024 to ensure their widespread adoption.

2. Enhancing Global Leadership in Data Privacy

a. Secure leadership in setting Global Privacy Norms

As global AI and privacy regulations evolve, the Commission aims to shape international standards, advocating for frameworks that reflect Asian perspectives alongside existing European and U.S.-led norms.

Efforts will also focus on securing cross-border data flows by advancing the equivalency recognition system, renewing adequacy decisions, and exploring similar agreements with the US, UK and Japan. In parallel, the Commission will enhance safe data transfer mechanisms by introducing stricter safeguards for international data sharing, including clearer criteria for suspending data transfers.

b. Advance the MyData Era

In March 2025, Korea's MyData initiative will expand into healthcare, telecommunications, and energy sectors, with plans for gradual expansion into education, employment, and leisure. To support seamless cross-sector data integration, the Commission will implement a fair cost-sharing framework for data transmission and promote interoperability through intermediary platforms.

To ensure a secure MyData ecosystem, the Commission will launch a "MyData Support Platform" to facilitate data portability rights, establish guidelines for data management institutions, and conduct rigorous compliance reviews. Additional safeguards against manipulative practices will be introduced, and user awareness will be strengthened through educational programs.

3. Restructuring the Privacy Protection Framework for Digital Transformation

a. Strengthen Privacy Enforcement and Investigative Capabilities

The Commission will intensify privacy enforcement in 2025 through targeted inspections, advanced investigative tools, and a rationalized penalty system. Focus areas include: (i) sectors closely tied to daily life (e.g, shared platforms and digital finance), (ii) emerging technologies (e.g., AI-integrated services) and (iii) the public sector.

To strengthen investigations, the Commission will establish a forensic lab for digital evidence analysis, implement an investigative management system, and expand its workforce with specialized investigators and a dedicated team for handling administrative appeals. Importantly, foreign businesses will face stricter compliance requirements, including mandatory documentation submissions, enhanced domestic representative obligations, and proportionate penalties for privacy violations.

b. Build a Robust Privacy Safety Net

The Commission will expand privacy-by-design certifications for IT devices, improve behavioral data management for personalized advertising, and evaluate privacy policies of major companies in AI, home IoT, edtech, broadcast, and telecommunications. It will also explore policies for post-mortem privacy and digital legacies.

In particular, the Commission will explore sector-specific measures to enhance data privacy, including: (i) mandatory disclosure of major data breaches, strengthened logging and security controls, and expanded compliance assessments for the public sector; and (ii) initiatives to improve the expertise of CCTV and control room operators, along with tailored data privacy training for private entities serving digitally vulnerable groups such as children, seniors, and small businesses.

Conclusion

The Commission's 2025 agenda reflect a comprehensive approach to data privacy, balancing innovation with regulatory oversight. Businesses should leverage regulatory frameworks, adapt to evolving privacy standards, and proactively address compliance risks to stay ahead in Korea's fast-evolving data privacy landscape.

By *Ho Sang Yoon (hsyoon@shinkim.com)*
Partner, ICT Group
and
Janelle J. Hyun (jhyun@shinkim.com)
Foreign Attorney, ICT Group

Shin & Kim LLC

** The opinions expressed in this article are the author's own and do not reflect the views of KOTRA.*