



PIPC Reveals its Key Priorities and Policy Agenda for 2025

2025.01.15

On January 13, 2025, Korea’s central privacy authority, the Personal Information Protection Commission (“**Commission**”), unveiled its key policy initiatives for 2025 (“**Plan**”). The Plan outlines six key initiatives that the Commission will be pursuing under three major strategies, as follows:

Major Strategies	Key Initiatives
Foster the growth of data-driven AI industry and build underlying trust	<ul style="list-style-type: none">- Innovate privacy regulations for the AI era- Establish a foundation for sustainable industry innovation guests
Enhance global leadership in data privacy	<ul style="list-style-type: none">- Secure leadership in setting global privacy norms- Advance the MyData era and deliver tangible results
Restructure the privacy protection framework to address accelerated digital transformation	<ul style="list-style-type: none">- Strengthen the role as a privacy protection control tower- Build a robust privacy safety net

For the specific agendas the Commission will be pursuing and implications for the industry, read on:

1. Innovate Privacy Regulations for the AI Era

(a) Overhaul and revamp privacy legislation for the AI age

The Commission plans to introduce special provisions under the PIPA to permit the use of original data in specific circumstances. Specifically, these provisions would provide a legal basis for the use of original data particularly when research purposes cannot be adequately achieved with pseudonymized data alone, subject to the Commission’s review and approval.

Additionally, the Commission aims to broaden the legal basis for AI developers to collect, use, and process personal data by considering the “legitimate interests” of businesses involved in AI development and the “public interest.”

(b) Address practical challenges within the current legal framework

To address the legal uncertainties that small and medium enterprises (SMEs) face when applying principles-based privacy regulations to emerging technologies and industries, the Commission will establish clearer standards for AI and data processing. Alongside legislative amendments, the Commission will promote regulatory flexibility through regulatory sandboxes and preliminary adequacy review system, among others.

(c) Build trust in new technologies

The Plan also includes empowering data subjects by granting them the right to request the deletion of synthetic media, such as deepfakes, and prohibiting and penalizing the act of synthesizing personal data that infringes on the right of publicity. Moreover, the Commission is considering expanding private sector participation by recognizing personal data impact assessments autonomously conducted in the AI sector and offering incentives to businesses for voluntary compliance.

► **Takeaways:** The Commission recognizes that the use of data (including personal data) is essential for emerging technologies and industries such as AI. The Plan shows that the Commission aims to overhaul relevant legislation so that it is more appropriate for the AI era and adopt more flexible interpretations of the law to address the challenges faced by business entities.

Therefore, AI developers and relevant stakeholders should (i) actively utilize the regulatory frameworks available, such as regulatory sandboxes and preliminary adequacy review system, (ii) continuously monitor the Commission’s policy directions, and (iii) take proactive measures to address issues arising from new AI technologies, such as deepfakes, to secure reliability in the technology and minimize regulatory risks.

2. Establish a Foundation for Sustainable Industry Innovation

(a) Adapt legal frameworks to rapid technological changes

The Commission aims to enact a new law to address the unique characteristics of visual data and improve the regulatory framework for biometric data, including facial images and fingerprints.

(b) Promote the use of pseudonymized data to drive the growth of emerging industries

To support industry growth, the Commission will establish “personal data innovation zones (tentative),” where data pseudonymization can be facilitated. The Commission will streamline pseudonymization procedures, set up regional

support centers, and form industry-specific expert committees. Additionally, the Commission plans to expand the pseudonymization support platform to cover the processing of unstructured data (such as video and image data), which are critical inputs for AI technologies.

(c) Build technical infrastructure for safe data utilization

The Commission will invest in privacy-enhancing technologies and develop standards for key areas. Specifically, the Commission will focus on conducting privacy vulnerability assessments for large language models, developing de-identification technologies for multimodal data, and preventing deepfakes. Commercialization of technologies developed in 2024 will also be prioritized.

► **Takeaways:** The Commission has unveiled plans to improve the institutional framework and provide technical support for various types of personal data, including visual data, biometric data, and pseudonymized data. These efforts will involve providing clearer regulatory guidance on the interpretation of relevant law and regulations and expanding the functions of the platforms, which are expected to broaden the scope of personal data usage in the field. Businesses should thus consider proactive utilization of these institutional changes.

3. Secure Leadership in Setting Global Privacy Norms

(a) Lead global discussions on AI and privacy regulations

Currently, Europe and the United States lead the global discussion on privacy norms. However, with the upcoming Global Privacy Assembly (GPA) in September 2025, the Commission aims to play a key role in shaping new privacy standards that incorporate the perspectives of the Asian countries and beyond.

(b) Build secure and free data transfer frameworks

Efforts will also be made to strengthen bilateral cooperation between the EU and Korea on data transfers, including advance the equivalency recognition system and renewing adequacy decisions. The Commission will explore similar agreements with the US, UK and Japan, and actively participate in the Global Cross Border Privacy Rules (CBPR) Forum to enhance certification requirements and improve interoperability with the Korean law.

(c) Improve overseas data transfer systems and investigation capabilities

The Commission plans to expand safe data transfer mechanisms, such as standard contractual clauses, and enhance protections for overseas data transfers. It will reinforce the security framework by establishing detailed criteria for suspending international data transfers and providing clearer guidance for foreign businesses, aimed at establishing a robust framework for international data sharing and enhancing foreign investigative capabilities.

► **Takeaways:** In line with the global trend, the Commission is also committed to leading normative discussions and establishing frameworks for more active cross-border data transfers. Specifically, the Commission is working to secure equivalency recognition with the EU and is also pursuing international cooperation with the United States.

4. Advance the MyData Era and Delivering Tangible Results

(a) Expand MyData services

Starting in March 2025, MyData services will launch in key sectors that have a significant impact on daily life, including healthcare, telecommunications, and energy. Pilot services offered by participating companies include: (i) personalized chronic disease management, (ii) integration of medical records for citizens residing overseas, (iii) medication management and prescription support, (iv) recommendations for optimal mobile carrier plans, and (v) travel expense planning proposals.

(b) Gradual expansion across all sectors

The Commission plans to expand the parties and types of data subject to the MyData initiative in the healthcare and telecommunications sectors and will discuss a phased expansion into new sectors, such as education, employment, and leisure. Additionally, the Commission will support data integration between sectors where MyData services have already launched (e.g., finance and public sectors) and will newly launch (e.g., healthcare and telecommunications), create a reasonable cost-sharing system for data transmission, and promote data linkage through the operation of intermediaries to support the spread of MyData services.

(c) Build a transparent and secure MyData ecosystem

The Commission's agenda also includes launching a "MyData Support Platform" to support data subjects' exercise of their right to data portability, publishing guidelines for personal data management institutions, and conducting rigorous reviews. The Commission also plans to foster a sound culture for MyData services by developing guidelines to prevent unfair inducements through dark patterns, for example, and offering educational programs for data subjects.

► **Takeaways:** MyData services, which has been implemented in the public and financial sectors, will soon be expanded to other sectors such as healthcare and telecommunications. Businesses in these sectors must thoroughly review the MyData scheme, ensuring they meet the necessary requirements and set in place the required systems. Other sectors should also prepare for the potential expansion of the initiative in the future.

5. Strengthen the Role of the Privacy Protection Control Tower

(a) Focus on vulnerable areas

The Commission will conduct proactive inspections of in the three major privacy-vulnerable sectors: (i) sectors closely related to people's daily lives,¹ (ii) emerging technologies and industries,² and (iii) the public sector³ and incorporate its findings for policy and regulatory improvements.

(b) Enhance investigation capabilities through digital technologies

To enhance the Commission's investigative capabilities, the Plan includes: (i) establishing a forensic lab for collecting and analyzing digital evidence, (ii) operating an investigation management system to ensure systematic oversight throughout the entire process, (iii) training specialized investigators, and (iv) forming a dedicated team to manage lawsuits.

(c) Rationalize investigation and penalty system

The Commission will implement enforcement mechanisms for foreign businesses, requiring such companies to submit relevant documents (such as revenue statements) and work on improving the domestic representative designation requirement. It will also adjust penalty rates to ensure proportional sanctions based on the severity of violations, including those involving sensitive data (e.g., images that could be misused to create deepfakes). Exemptions will be considered for minor violations or small businesses.

► **Takeaways:** The Commission is expected to play a more active role in strengthening privacy protection through legislative reform and enhanced investigative capabilities. Businesses must thus be more proactive in adopting privacy protection controls and reducing the risk of violations. Particularly for foreign businesses, it is important to monitor developments in regulations related to document production and domestic representatives and ensure compliance in advance. Furthermore, businesses in the three privacy-vulnerable sectors identified by the Commission should conduct preliminary compliance assessments to review their current data handling practices and prepare for future inspections.

6. Build a Robust Privacy Safety Net

(a) Address privacy concerns that arise in digital transformation

To tackle privacy concerns arising from digital advancements, the Commission will (i) expand privacy-by-design certifications for widely used IT devices, (ii) enhance the management framework for the collection and use of behavioral data, critical for personalized advertising, (iii) conduct in-depth evaluations of privacy policies for 50 major companies across the AI, home IoT, edtech, broadcast, and telecommunications industries, and (iv) explore policy options for post-mortem privacy and digital legacies.

(b) Strengthening public sector privacy management

To bolster privacy management in public institutions, the Plan includes: (i) a policy requiring public disclosure of violations and follow-up inspections within three years for public entities affected by significant data breaches, (ii) inspections of adopted safeguards (e.g., retention of access logs for major public institution systems), (iii) expansion of the scope of entities subject to annual assessments on the level of personal information protection applied by public institutions, and (iv) analysis and evaluation of potential privacy risks for local governments that wish to have their local regulations reviewed.

(c) Raise privacy protection standards in the private sector

For the private sector, the Commission will: (i) enhance the expertise and skills of CCTV and control room operators by introducing a national certification program (also applicable to the public sector), (ii) develop tailored support systems for self-regulatory organizations of different sizes and types, and (iii) enhance privacy education for digitally vulnerable groups, including children, seniors, and small businesses.

► **Takeaways:** For businesses offering a variety of digital services, addressing emerging privacy concerns will require a privacy-centric design approach. Keeping an eye on the Commission's policy trends and continuously adapting to the rising standards of privacy protection would be crucial. Notably, since the privacy policy evaluation first conducted in 2024 is likely to expand in its scope, businesses are advised to conduct internal assessments of their respective privacy policies.

¹ Shared platforms, digital finance, and real estate and construction.

² Edtech, AI agents and other AI application services, and legal tech.

³ Critical management systems and universities.

[\[Korean version\]](#) 『2025년 개인정보보호위원회 주요 정책 추진계획』 발표 및 시사점

Key Contacts

Sinook Kang

Senior Partner

+82-2-316-4059

sokang@shinkim.com

Joe Juneyoung Jang

Partner

+82-2-316-4985

jyojang@shinkim.com

Jeong Ho Ahn

Partner

+82-2-316-2891

jhahn@shinkim.com

Jieun Lee

Senior Researcher

+82-2-316-1720

jeunlee@shinkim.com

Soonyoung Heo

Foreign Attorney

+82-2-316-1837

syheo@shinkim.com

Ho Sang Yoon

Partner

+82-2-316-2584

hsyoon@shinkim.com

Eugene Kim

Senior Foreign Attorney

+82-2-316-4770

eugenekim@shinkim.com