

Data privacy laws in Korea's fintech landscape

As South Korea's financial sector undergoes rapid digital transformation, the government has prioritised data utilisation through policies that balance innovation with consumer protection. Central to this effort are the MyData licensing regime under the amended Credit Information Use and Protection Act (Credit Information Act) and reforms to the network separation policy to accommodate AI and cloud technologies. This article highlights key legal and policy developments in personal credit information protection, the MyData system, and network separation reforms.

Key policies

Strengthening personal data protection. The Credit Information Act operates as a special law supplementing the Personal Information Protection Act, taking precedence in matters involving the use of credit information in financial transactions. Where not specified, the general provisions of the Personal Information Protection Act apply.

To protect data subjects, the Credit Information Act requires prior consent for collecting credit information, mandates clear purpose statements and limits data use to what is necessary. Third-party sharing requires separate, specific consent.

The act also requires financial institutions to simplify and visualise the consent process, providing a "data usage consent rating" that outlines potential privacy risks and consumer benefits. This aims to support "informed consent" by financial consumers.

The act acknowledges the rise of automated data processing, such as AI-based credit evaluations and insurance calculations, and gives consumers the right to request explanations or object to profiling. It also allows individuals to request the transfer of their credit information between institutions. The act further requires an

ongoing review of data practices to enhance security and permits punitive damages of up to five times the actual loss in case of data breaches.

Improvements to MyData policies. The 2020 amendment to the Credit Information Act established a licensing system for MyData businesses, which consolidates individuals' financial data to provide services like product recommendations and financial advice.

To encourage small and mid-sized fintech firms' participation, the act sets a low capital requirement of KRW500 million (USD352,399) and exempts them from capital contribution rules for financial institutions. Operators must still meet staffing, infrastructure and business plan standards for approval by the Financial Services Commission (FSC).

To operate a MyData business in South Korea, a foreign corporation must establish a local subsidiary, which must obtain a MyData business licence. As a major shareholder, the foreign corporation must also meet requirements under the Enforcement Decree, including financial soundness, credibility, operational integrity and capital capacity.

Launched on 5 January 2022, Financial MyData services have since seen regulatory enhancements to support industry growth and strengthen consumer protection. By the end of 2022, the scope of information provided through Financial MyData significantly expanded from 492 to 720 items across all sectors, including banking, insurance, credit cards, financial investments, and public institutions.

On 21 January 2025, the government further amended the Supervisory Regulations on Credit Information Business, a subordinate rule under the act. Through this amendment: (1) MyData operators are

now permitted to conduct face-to-face sales activities; (2) the use of MyData services by minors has been improved; (3) standards for data combination by MyData operators have been clarified; and (4) when MyData operators sell information to third parties with the consent of the data subject, they are now required to use the "MyData Secure Provision System" established at the Financial Security Institute.

Network separation

The Regulation on Supervision of Electronic Financial Transactions, a subordinate rule under the Electronic Financial Transactions Act, requires physical network separation to protect systems from hacking and external threats. Internal business systems must be blocked from external networks like the internet and data centre systems, along with terminals used for operations, development, or security, must also remain physically isolated.

Although initially effective, Korea's physical network separation regulations have become less suitable in today's fast-evolving IT environment. Strict disconnection from the internet has restricted the use of SaaS, AI and security tools, delaying updates and weakening defences. The financial sector has voiced concerns about these inefficiencies, their impact on innovation and R&D, and the growing gap with global standards, prompting continued calls for reform.

In response, the government announced a three-phase network separation reform plan in August 2024 and is implementing phase 1, focusing on:

- (1) Permitting the use of generative AI (GenAI): Most GenAI services are in cloud-based internet environments; however, due to network separation regulations, their use has been significantly restricted. In addition, it is currently impossible to process or store personal credit information through overseas AI models that do not have servers located in Korea. To address these limitations, the government plans to allow exemptions

via a regulatory sandbox, allowing financial institutions to process even pseudonymised personal credit information using GenAI. Under this framework, the FSC reviews applications on a case-by-case basis, assessing factors such as purpose of AI use, data scope and security measures before approval for sandbox designation.

- (2) Expanding the use of cloud-based apps (SaaS). In September 2023, SaaS use within internal networks was approved via the regulatory sandbox. Recent reforms have since broadened its scope to include pseudonymised credit data and allowed applications beyond collaboration tools and ERP systems to cover security, customer management, and business automation programs. Devices authorised for SaaS access have also been broadened to encompass not only wired PCs but mobile devices as well.

The FSC reviews each application based on the scope of SaaS usage, the nature of business operations and the level of security measures before approval for sandbox designation. Considering the expanded scope of SaaS use, the FSC is also requiring the implementation of strengthened security measures.

- (3) Easing network separation for R&D. Although exceptions for R&D networks were introduced in November 2022, their impact was limited due to difficulties in physically separating R&D and business networks. The ban on using personal credit data also hindered service development. The government is now promoting reforms allowing logical separation and the use of pseudonymised credit data in R&D, fostering the development of new services based on customer data analysis.

Reform outlook

With the rollout of network separation reforms, many companies have gained sandbox approval to use GenAI and SaaS within internal networks via cloud solutions. The regulatory sandbox designations are not limited to financial institutions or electronic financial business operators established with domestic capital; subsidiaries of foreign companies incorporated under Korean law have also been eligible.

On 3 February 2025, as part of the

promotion of network separation policy reforms, the Regulation on Supervision of Electronic Financial Transactions was amended. As a result, financial institutions and electronic financial business operators are now permitted to use pseudonymised personal credit information within R&D networks.

The reform of network separation policies in the financial sector is expected to continue. The FSC plans to evaluate the performance and security implications on using GenAI and SaaS within internal networks, currently permitted under the regulatory sandbox. If these initiatives are assessed as highly effective and present no significant security risks, the FSC intends to amend the existing regulations and institutionalise these measures permanently. Additionally, the FSC is also considering expanding permissible data in R&D networks to include actual personal credit information, beyond pseudonymised data.

Meanwhile, amid growing reliance on cloud services and data centres, concerns remain over inadequate third-party risk management. In response, the government plans to strengthen its regulatory framework to address risks tied to the expanding use of SaaS, GenAI, and related technologies following the easing of network separation regulations.

The FSC has announced its commitment to advancing network separation reforms in a phased manner to build a new security framework based on autonomous protection and outcome-based accountability. In the long term, it plans to introduce a new law, tentatively titled the "Digital Financial Security Act", to shift from rules-based to principles-based regulation.

Takeaway

The Korean government is working to both foster the data economy and protect personal information. However, challenges such as hacking and data breaches require continued technological improvements. Clarifying service provider responsibilities, improving remedies for consumer harm and strengthening protections for vulnerable groups remain priorities. As data grows more central to value creation, public debate on data policy is expected to increase, prompting the government to continually refine its approach.



Hyun-il Hwang
Partner at Shin & Kim
in Seoul

Tel: +82 2316 4453
Email: hihwang@shinkim.com



Sang Hwan Han
Partner at Shin & Kim
in Seoul

Tel: +82 2316 1973
Email: shwhan@shinkim.com



Daniel Woojin Chang
Senior Foreign Attorney at Shin & Kim
in Seoul

Tel: +82 2316 7285
Email: wjchang@shinkim.com

SHIN & KIM

SHIN & KIM
23F, D-Tower (D2), 17 Jongno 3-gil,
Jongno-gu, Seoul 03155, Korea
Tel: +82 2316 4114
Email: shinkim@shinkim.com

www.shinkim.com