GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

GDA COMMENTS ON NETWORK SEPARATION IN ELECTRONIC FINANCIAL SUPERVISON REGULATIONS

FINANCIAL SERVICES COMMISSION (FSC)

February 2026

The Global Data Alliance (GDA)[1] would like to provide our recommendations to the FSC on its proposed amendments to the Enforcement Rules of the Electronic Financial Supervision Regulations (**Rules**) regarding network separation.

About GDA

The GDA is a cross-industry coalition of companies, headquartered in different regions of the world, that are committed to high standards of data privacy and security. Global Data Alliance members share a deep and long-standing commitment to supporting economic development, building trust in the digital economy, and protecting personal data across regions, technologies, and business models. Alliance member companies rely on the ability to transfer data responsibly around the world to create jobs and make industries at home and abroad more competitive. Cross-border data transfers power growth across the globe and all sectors of the economy — from agriculture; to financial services; to the manufacturing industries. Data transfers are critical for companies of all sizes, fostering innovation and economic development, creating jobs, and promoting productivity, safety, robust cybersecurity, and environmental responsibility.

Discussion

The GDA welcomes certain aspects of the FSC's efforts to ease the network separation requirements set out in the Rules, with a view to facilitate the use – in the financial services sector – of the most globally secure and competitive software-as-a-service (SaaS) offerings.[2] GDA is encouraged that the proposed amendments to the Rules would allow financial institutions to adopt and deploy a broader range of cloud-based SaaS solutions for internal and back-office functions without being subject to blanket network separation requirements. This shift away from the prior reliance on case-by-case approvals under the regulatory sandbox framework appropriately recognizes the maturity, stability, and security of widely deployed software solutions that support the financial services sector. This is an important step toward aligning Korea's financial regulatory framework with modern IT architectures and global practices.

[1] The GDA is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to access and transfer information across borders to innovate and create jobs. GDA member companies are active in the accounting, agriculture, automotive, aerospace and aviation, biopharmaceutical, consumer goods, energy, film and television, finance, healthcare, hospitality, insurance, manufacturing, medical device, natural resources, publishing, semiconductor, software, supply chain, telecommunications, and transportation sectors. For more information, see https://www.globaldataalliance.org

[2] Financial Services Commission, "*Network Separation Rule to be Eased in Financial Industry to Facilitate Use of Cloud-Based Software-as-a-Service*", January 2026, https://www.fsc.go.kr/eng/pr010101/86100 (**"FSC Press Release"**). Per the FSC Press Release, SaaS programs specified under the Enforcement Decree of the Act on the Development of Cloud Computing and Protection of Its Users will be exempted from the network separation rule pursuant to the Electronic Financial Transactions Act and the supervisory regulation on electronic financial services.

However, the GDA is very concerned with the other aspects of the proposed amendments, which significantly limit the practical impact of the easing of network separation requirements.

First, GDA is concerned that the new exemptions from network separation will *not* apply to the handling of personal identification information or personal credit information.

We note that this restriction is motivated by security considerations over the protection of personal identification information and personal credit information. However, maintaining network separation for systems handling personal or credit information does not, in itself, result in stronger security outcomes. Modern cloud environments employ layered security controls, including strong encryption, access management, continuous monitoring, and rapid threat detection, which are widely recognized as more effective than physical or logical isolation alone. Retaining network separation requirements for these systems may therefore reduce, rather than enhance, overall security by limiting access to advanced security capabilities that are natively delivered through cloud-based services.

In addition, network separation can introduce operational complexity that increases the risk of misconfiguration, delays the deployment of security patches, and constrains real-time visibility across systems. These factors can weaken an institution's ability to detect and respond to evolving cyber threats in a timely manner. Restricting their use for systems involving personal or credit information may therefore reduce access to best-in-class security capabilities and runs counter to internationally recognized, risk-based approaches to protecting sensitive financial data.

Relatedly, this restriction also means that commonly used SaaS tools, such as customer relationship management systems, internal analytics platforms, or AI-enabled customer support solutions, cannot be used where they process customer identifiers or credit-related data, even for routine internal operations. In particular, it inhibits the adoption of advanced data analytics and AI-enabled services that are designed to operate securely on cloud infrastructure, including use cases that directly enhance customer outcomes such as real-time fraud detection and more personalized financial services. This significantly constrains financial institutions' ability to modernize core business processes, limiting the practical value of easing network separation requirements and, in turn, slowing down Korea's financial digital transformation and undermining policy objectives to promote cloud adoption and innovation in the financial sector.[3]

Second, GDA cautions against implementing onerous information control measures requirements that, in practice, would continue limit the utility of the broader network separation exemptions for financial institutions.[4]

In particular, requirements relating to the pre-screening or prior approval of SaaS programs, highly prescriptive technical controls, and rigid encryption or operational specifications risk creating significant compliance burdens for both financial institutions and SaaS providers. While security oversight is essential, such requirements are not aligned with the operational realities of SaaS delivery models, where services are continuously updated, improved, and secured through standardized processes applied at global scale.

From the perspective of SaaS providers, these requirements can make it difficult or impractical to offer services to financial institutions, as they may require bespoke configurations, static versions of software, or repeated local

[3] Cloud adoption is widely recognized for driving efficiency, security, and innovation in the financial services sector – benefits that the financial sector in South Korea could better capitalize on. According to the Asian Development Bank, South Korea's spend on cloud services in 2023 was only 0.29% of its GDP, trailing behind counterparts like Singapore and New Zealand, whose total cloud spend was 0.8% of their GDP, and similarly, Australia and Japan dedicated 0.3%-0.5% of their GDP to cloud services. See: Asian Development Bank, "*Cloud Computing Policies and Their Economic Impacts in Asia and the Pacific*", January 2024, https://www.adb.org/publications/cloud-computing-policies-and-their-economic-impacts-in-asia-and-the-pacific.

[4] Per the FSC Press Release, financial companies are required to: "(a) have their SaaS programs pre-screened by the Financial Security Institute, (b) maintain strict IT security protocols (certification, authorization, etc.) for access devices (computers and mobile devices), (c) monitor and control input, processing, and transfer of critical information, (d) prevent the sharing and processing of unnecessary information within SaaS programs and block access to unauthorized internet services, and (e) adopt encryption for networks where SaaS programs are being utilized."

approvals each time a service is updated. This undermines the core SaaS model, which depends on uniform service delivery, rapid deployment of security patches, and continuous improvement across a shared platform. As a result, providers may be unable to guarantee timely updates or consistent security protections or may be forced to limit functionality for financial sector customers, reducing the value and effectiveness of the services offered.

These challenges are increasingly pronounced as enterprise SaaS offerings now commonly incorporate embedded AI-enabled functionalities delivered as an integral part of the service. Clear confirmation that such AI-enabled SaaS capabilities fall within the scope of the exemption will provide financial institutions and service providers with the regulatory certainty needed to adopt these capabilities through ordinary SaaS deployments, without triggering duplicative approval processes. In the absence of such clarity, these requirements risk further narrowing the range of secure and innovative solutions available to the financial sector. In some cases, providers may determine that the compliance burden outweighs the commercial viability of offering their services to financial institutions, further narrowing the range of secure and innovative solutions available in the market.

In view of our concerns above, GDA recommends that the FSC further refine the proposed amendments by adopting a more risk-based and outcome-focused approach to the treatment of SaaS and network separation. In particular, the FSC should:

- Permit the use of cloud-based SaaS solutions for systems that handle personal identification information and personal credit information, particularly where supported by robust technical and organizational measures proportionate to the sensitivity of the data;
- Provide blanket exemptions for SaaS solutions without requiring pre-screening or prior approval from the incident response agency, such as the Financial Security Institute, as long as the firm has conducted sufficient internal security review and obtained internal approval;
- Confirm that requirements around bespoke configurations, static versions of software, or repeated local approvals each time a service is updated, will no longer be required under the revised rule;
- Recognize international best practices and certifications that are widely recognized by the industry;
- Provide clear confirmation that the scope of the SaaS exemption includes AI-enabled functionalities embedded within SaaS offerings, so that financial institutions and service providers have the regulatory certainty needed to adopt these capabilities as part of ordinary SaaS deployments, without triggering duplicative or ad hoc approval processes;
- Avoid prescriptive or inflexible information protection control measures that are misaligned with SaaS delivery models and instead recognize internationally accepted security practices that support continuous improvement, centralized security management, and rapid deployment of security updates.

Taking these steps would better enable financial institutions to adopt secure, innovative, and AI-enabled SaaS solutions, strengthen cybersecurity outcomes, and advance Korea's financial digital transformation objectives while maintaining strong protections for sensitive financial data.

Thank you for the opportunity to share these comments. Please do not hesitate to reach out with any questions or comments.

Sincerely yours,

Joseph Whitlock
Executive Director
Global Data Alliance