GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

South Korea's Digital Trade Barriers

Status in Reciprocal Trade Negotiations

The Honorable Scott Bessent
US Secretary of the Treasury
1500 Pennsylvania Avenue NW
Washington, DC 20220

The Honorable Jamieson L. Greer
United States Trade Representative
Executive Office of the President
600 17th Street, NW
Washington, DC 20508

The Honorable Howard W. Lutnick
US Secretary of Commerce
1401 Constitution Avenue NW
Washington, DC 20230

The Global Data Alliance (GDA)[1] welcomes the efforts of the Office of the US Trade Representative and the Departments of Commerce and Treasury to resolve unfair and non-reciprocal trade barriers that hurt US strategic interests, US companies, and US workers. Building on our March 2025 submission, we take this opportunity to offer the following updated information on South Korea's progress in resolving digital trade barriers.

Notwithstanding ongoing negotiations, South Korea continues to advance severe trade restrictions on US digital exports and US services market access. The collective effect of these measures is to undermine economic opportunity for American workers and American enterprises, making it more difficult for Americans across all sectors to export digitally-enabled services and goods to South Korea.

South Korea's actions run directly counter to the Administration's efforts to advance a "production economy" built on "robust and realist trade policy [that] can create jobs, promote innovation, strengthen the national defense, raise wages, and foster [a] manufacturing renaissance" in the United States.[2] We urge you to ensure that South Korea addresses these barriers that undermine American workers' jobs in all sectors.

Sincerely yours,

Joseph Whitlock

Executive Director
Global Data Alliance

Annex

The GDA is a cross-industry coalition of companies that support tens of millions of American jobs and that are active across all 50 US states in every sector of the US economy. The GDA shares the US government view that the United States should be a "production economy" — that is "oriented around the production of manufactured goods, agricultural products, services, and knowledge."[3]

A strong production economy requires — first and foremost — access to knowledge, information, and data. Such access powers growth, innovation, jobs, and wage-growth for companies of all sizes — from small and medium-sized enterprises (SMEs) to large corporations. Such access also supports a strong cybersecurity posture, promoting threat visibility and the ability to detect security risks early. Such access is essential to the functioning of manufacturing plants, modern farms, and service providers in every sector,[4] including the agriculture,[5] automotive,[6] clean energy,[7] finance,[8] health,[9] logistics,[10] media,[11] pharmaceuticals,[12] and telecommunications[13] sectors.

Cross-Border Data Transfers and Server Localization: It remains very difficult for businesses to deliver services via the cloud in South Korea's very broadly defined public sector. This is, in part, due to onerous certification requirements imposed by the Korea Internet Security Agency (**KISA**) under the Cloud Security Assurance Program (**CSAP**) on CSPs that provide cloud services to public sector agencies and requirements for physical network separation. Similar guidelines and regulations requiring physical network separation or data onshoring apply to healthcare sectors.[14] Service providers are required to fulfill technical and administrative requirements, many of which are not in line with global standards and business practices, and which do not lead to improved cloud security. These include:

A) **Physical Network Separation.** Most public sector data systems are required to be hosted on infrastructure and networks that are physically separated from those used by other clients. This requirement diverges from international best practices, which recognize logical separation as a secure and effective method for isolating sensitive workloads in multi-tenant cloud environments. While a few countries retain physical network separation requirements for some highly sensitive areas (national security, defense), it is rarely applied throughout the public sector, including to institutions that handle non-sensitive or even public data, such as public universities.

B) **Data Localization.** All data associated with public sector data systems must be physically located in Korea. This is an unnecessary barrier for many US CSPs that store and process data in regional data centers outside of Korea. In some cases, the use of offshore data centers ensures redundancy and back-up. In cases of serious physical damage or cyberattack on one data center, data stored in physically remote data centers can be used to recover from the incident.

C) **Local Personnel Requirements.** CSPs must have operations and management personnel located within Korea to obtain CSAP certification. Local personnel requirements disadvantage US CSPs by significantly raising their compliance costs, as they must duplicate personnel and infrastructure already managed efficiently at scale elsewhere.

Korea Personal Information Protection Act: The Personal Information Protection Act (**PIPA**) also imposes restrictions on the transfer of personal data outside Korea. In 2023, the PIPA was substantially revised, and the Korean Personal Information Protection Commission (**PIPC**) adopted an Enforcement Decree that took effect in March 2024. These changes provide the PIPC with new authority to impose fines on service providers based on their global revenue rather than revenue in Korea, and order the suspension of cross-border transfers of personal data. The PIPA permits the transfer of personal data outside of Korea only in limited circumstances, such as when the service provider has obtained a separate consent from the data subject to transfer data outside of Korea, when the recipient of the data has obtained a privacy certification recognized by the PIPC, or when the data is transferred to a country that the PIPC has determined provides an equal level of data protection, among others. These

restrictions pose barriers to the cross-border provision of based services that depend on data storage and processing.

Cross-Border Data Restrictions in the Financial Services Sector: In the Korea-US Free Trade Agreement, South Korea committed to allowing financial institutions to transfer data to foreign affiliates and to permit certain data processing and other functions to be performed outside of Korea. Nevertheless, South Korea's Financial Services Commission (FSC) dictates that personal credit information cannot be processed overseas and, if processed in public cloud, the cloud computing systems must be maintained on servers located in South Korea.[15] Moreover, South Korea's network segregation rules, which require internal and external networks to be physically segregated,[16] effectively require the localization of network infrastructure and data sets. These policies expose financial institutions to greater cybersecurity risks by creating a more diffuse and decentralized cybersecurity environment with a greater cyber-attack surface and potential points of failure. South Korea's localization mandates also effectively inhibit central oversight and information sharing across borders, reducing cyber threat awareness and visibility.

Besides data localization, the network segregation requirements prevent the Korea subsidiaries from leveraging on the global IT and cybersecurity service and expertise, and negatively impact financial institutions' adoption of cutting edge cybersecurity services delivered through SaaS and AI-enhanced tools. A recent interpretation provided by Financial Supervisory Service (FSS is the FSC's supervisory arm) deems global support as violation of network segregation rule, which poses non-compliance risk to all global FIs and cybersecurity risk.[17]

Cross-Border Data Restrictions in the Insurance Sector: US reinsurance companies continue to face significant restrictions on transferring personal information outside of Korea in the ordinary course of business. These restrictions persist despite statements by Korea's FSC in 2022 and 2024 indicating a revised interpretation of the Personal Information Protection Act that would permit the cross-border transfer of primary insurance policyholder data for purposes such as data processing, risk management, and underwriting. In September 2024, Korean government officials verbally provided clarification related to the use of a revised consent form and possible changes to Korean law, no public written documentation has been issued to confirm these changes. In the absence of legal certainty, US reinsurers remain unable to transfer data outside of Korea.

Location Data: South Korea's restrictions on the transfer of location-based data have led to a competitive disadvantage for international suppliers seeking to incorporate such data into services offered from outside of South Korea. Among major markets, South Korea maintains a uniquely restrictive licensing framework for such data transfers. To date, Korea has never approved a license to transfer cartographic or other location-based data, despite numerous applications by US enterprises.

---

[1] The Global Data Alliance (globaldataalliance.org) is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. The Alliance supports policies that help instill trust in the digital economy while safeguarding the ability to transfer data across borders and refraining from imposing data localization requirements that restrict trade. Alliance members are headquartered across the globe and are active in the advanced manufacturing, aerospace, automotive, consumer goods, electronics, energy, financial services, health, supply chain, and telecommunications sectors, among others. The Business Software Alliance administers the Global Data Alliance. See Global Data Alliance, About the Global Data Alliance (2020), https://www.globaldataalliance.org/downloads/aboutgda.pdf

[2] USTR, 2025 Trade Agenda (March 2025), at: https://ustr.gov/about-us/policy-offices/press-office/press-releases/2025/march/us-trade-representative-announces-2025-trade-policy-agenda

[3] USTR, 2025 Trade Agenda (March 2025), at: https://ustr.gov/about-us/policy-offices/press-office/press-releases/2025/march/us-trade-representative-announces-2025-trade-policy-agenda

[4] Global Data Alliance, The Cross-Border Movement of Data: Creating Jobs and Trust Across Borders in Every Sector (2020), https://globaldataalliance.org/wp-content/uploads/2021/07/GDAeverysector.pdf

[5] Global Data Alliance, *GDA Website – Agriculture* (2022), at: https://globaldataalliance.org/sectors/agriculture/

[6] Global Data Alliance, *GDA Website – Automotive* (2022), at: https://globaldataalliance.org/sectors/automotive/

[7] Global Data Alliance, *GDA Website – Energy* (2022), at: https://globaldataalliance.org/sectors/energy/

[8] Global Data Alliance, *GDA Website – Finance* (2022), https://globaldataalliance.org/sectors/finance/

[9] Global Data Alliance, *GDA Website – Healthcare* (2022), https://globaldataalliance.org/sectors/healthcare/

[10] Global Data Alliance, *GDA Website – Supply Chain Logistics* (2022), https://globaldataalliance.org/sectors/supply-chain-logistics/

[11] Global Data Alliance, *GDA Website – Media and Publishing* (2022), https://globaldataalliance.org/sectors/media-publishing/

[12] Global Data Alliance, *GDA Website – Biopharmaceutical R&D* (2022), https://globaldataalliance.org/sectors/biopharmaceutical-rd/

[13] Global Data Alliance, *GDA Website – Telecommunications* (2022), https://globaldataalliance.org/sectors/telecommunications/

[14] On June 1 of 2020, a new certification framework that includes CSAP requirements was applied to electronic medical records. *See* Enforcement Decree of the Medical Service Act (Article 10-5: Standardization of Electronic Medical Records) (indicating that "matters subject to standardization to be determined and publicly notified by the Minister of Health and Welfare pursuant to Article 23-2 (1) of the Act shall be as follows: "2. Facilities and equipment necessary for the safe management and preservation of electronic medical records under Article 23 (2) of the Act").

[15] Article 17 under the Credit Information Use and Protection Act. Under RSEFT Article 14-2-8 (Usage process of cloud computing service), finance companies and electronic finance service providers shall use domestically located information process systems and apply Article 11-12 to process personal credit information or identification information.

[16] RSEFT Article 14-2-8 (Usage process of cloud computing service), finance companies and electronic finance service providers shall use domestically located information process systems and apply Article 11-12 to process personal credit information or identification information.

[17] FSC. No Action Letter: Whether it violates Article 15, Paragraph 1, Item 5 of the Electronic Financial Supervision Regulations when an overseas trustee directly accesses the server in the domestic computer room to perform entrusted tasks (system operation), https://better.fsc.go.kr/fsc_new/replyCase/OpinionDetail.do?stNo=11&muNo=86&muGpNo=75&opinionIdx=2261