Comments on Korea's Accession to the Korea-Singapore Digital Partnership Agreement

April 2022

The Global Data Alliance[1] (**GDA**) welcomes the opportunity to provide these comments on the substantially concluded Korea-Singapore Digital Partnership Agreement (**KSDPA**).

I. Introduction

GDA is a cross-industry coalition of companies that are committed to high standards of data privacy and security and that rely on the ability to transfer data responsibly around the world. GDA members have significant operations based in Korea, invest hundreds of millions of dollars into the Korean economy, and have many thousands of Korean employees. Data transfers are critical to our activities across Korea in all sectors, from aerospace, healthcare, advanced manufacturing to transportation and telecommunications. Cross-border data transfers enable the digital tools and insights that are critical to enabling our Korean operations to create jobs, boost efficiency, drive quality, and improve output.

GDA congratulates Korea on the substantial conclusion of the KSDPA, which is a forward-looking and comprehensive Digital Economy Agreement (**DEA**). In relation to the KSDPA's international commercial aspects, some of the most important disciplines are those relating to cross-border data transfers and data localization.

II. Discussion

Trade barriers and digital protectionism are growing around the world at the very time that digital trade and connectivity are helping sustain economic activity, employment, and social well-being. The World Trade Organization (**WTO**) has reported that some 80 countries have imposed export and other trade restrictions in reaction to the COVID-19 epidemic, in addition to a growing number of digital trade barriers that impact the movement of information across borders.

Binding rules prohibiting unwarranted restrictions on cross-border data transfers and requirements to localize computing facilities are an important bulwark against this worrying trend. The KSDPA's Article 14.14 stipulates that neither Party shall prohibit or restrict the cross-border transfer of information by electronic means, including personal information, if this activity

[1] The Global Data Alliance 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. Alliance members are headquartered across the globe and are active in the advanced manufacturing, aerospace, automotive, consumer goods, electronics, financial services, health, media and entertainment, natural resources, supply chain, and telecommunications sectors, among others. GDA | The Software Alliance administers the Global Data Alliance. For more information on the Global Data Alliance, please see: https://www.globaldataalliance.org/downloads/aboutgda.pdf

is for the conduct of business of a covered person. Article 14.15 (Location of Computing Facilities) prohibits the Parties from imposing requirements to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory. GDA strongly supports the inclusion of these binding rules.

However, GDA also notes that the KSDPA's prohibition on computing facility localization does not apply with respect to a "financial institution" or a "financial service supplier of a Party".[2] In other words, financial institutions and service suppliers from Singapore may be required to use or locate their computing facilities in Korea as a condition for conducting business in Korea, and vice versa.

GDA recognizes that regulatory authorities in the financial sector require immediate and ongoing access to information of financial institutions and service suppliers, including information underlying their transactions and operations, to discharge their supervisory and monitoring duties.[3] It is a common concern among financial regulatory authorities that their ability to access financial data may be hampered if such data was stored outside of the country. Localization measures are thus seen as the solution for financial regulatory authorities seeking to maintain access to financial data.

However, requiring financial institutions/service suppliers to localize their computing facilities and data may increase security risks. As the capabilities of malicious actors in cyberspace continue to evolve, investments in data security have increased. This is especially so for the financial sector, where the effects of a cyberattack can be devastating. However, localization measures often compel financial institutions and service suppliers to use local data storage service providers in the country the imposes such measures. This by definition limits the options of such financial institutions and service providers when deciding where and with what entities they wish to entrust their data, including the option of using their own centralized data storage and processing centers, or those provided by third party service providers that may not have data centers in country. Local data storage service providers may not have the same security capabilities as global counterparts, many which invest enormous amounts of resources in their cybersecurity capabilities and constantly upgrade their security programs and controls to deal with the latest cyber threats.

Delays in uploading threat incident information to cybersecurity companies' global networks due to regional data restrictions could also expose customers in that region to new threats spreading from other parts of the world, reducing information privacy and security for those customers. For example, effective fraud mitigation as provided by banks, card networks and other players in the financial services sector demands sophisticated monitoring and rapid detection at the time of transaction to interpret and weigh the risk of fraud of each payment transaction as weighed by the facts of that payment transaction as against norms for all payment transactions and that account. Fraud detection models are typically built on global transaction data or transaction data collected from multiple countries since fraud patterns are not limited by national boundaries. Fraud trends which appear in one region or country may apply in others as cardholders travel to different countries, cardholders transact online with merchants in different countries, and the perpetrators of fraud do not respect any national boundary lines. Thus, to build effective fraud models and to gain the necessary insights into fraudulent activity in order to help prevent them, these models must be built off of global or multi-country data sets, based both on the location of

[2] KSDPA, Article 14.15 (4)

[3] KSDPA, Article 14.16 (2)

the merchant and the location of the cardholder.

Information sharing across jurisdictions could also be limited, undermining efforts from both financial institutions/service suppliers and regulatory authorities to combat money-laundering and financing of terrorism.

Localization requirements in the financial sector are also not necessary for regulatory oversight. In a globalized economy, financial institutions and service suppliers often must provide services internationally to their customers in other countries, requiring the international transfer of significant amounts of financial data daily. Regulators have several mechanisms to ensure that they may maintain access to necessary data from financial institutions and service suppliers regardless of where the data may be stored, such as entering contractual agreements with financial institutions/service suppliers to have immediate and ongoing access to information processed or stored on computing facilities out of the country. As a general principle, there is no reason to impose localization requirements on financial institutions/service suppliers if regulatory authorities have immediate and ongoing access to their data. **This is the approach taken in Singapore's DEAs with both Australia and the United Kingdom (UK), which GDA strongly supports:**

- In the Singapore-Australia DEA, Article 25(2) states that neither Party shall require a financial institution/services supplier to localize their computing facilities and data, so long as financial regulatory authorities "have immediate, direct, complete and ongoing access" to the information processed or stored on computing facilities used by the financial institution/service supplier located out of the country.
- Similarly, the UK-Singapore DEA amends Article 8.54 of the UK-Singapore Free Trade Agreement to state that a Party may only impose localization measures on a financial service supplier if it is "not able to ensure appropriate access to information required for the purposes of financial regulation and supervision". The Article further requires the Party imposing the localization measure to: (1) provide the financial service supplier "a reasonable opportunity to remediate any lack of access to information"; and (2) to consult with the other Party's regulatory authorities before imposing the localization measure.

The United States-Singapore Joint Statement on Financial Services Data Connectivity[4] is also a useful reference point. While non-binding in nature, both countries agreed to:

- Ensure that financial service suppliers can transfer data, including personal information, across borders by electronic means if this activity is for the conduct of the business of a financial service supplier.
- Oppose measures that restrict where data can be stored and processed for financial service suppliers as long as financial regulators have full and timely access to data needed to fulfill their regulatory and supervisory mandate.
- Ensure that financial service suppliers have the opportunity to remediate the lack of access to such data before being required to use or locate computing facilities locally.

GDA urges Korea to work towards the high watermark set by the Singapore-Australia and UK-Singapore DEAs in its future DEAs. We also urge Korea's financial regulatory authorities to collaborate closely with their Singaporean counterparts, including through non-binding joint statements or Memorandums of Understanding, so that this issue may be addressed in future upgrades to the KSDPA.

[4] United States-Singapore Joint Statement on Financial Services Data Connectivity, February 2020, https://www.mas.gov.sg/news/media-releases/2020/united-states-singapore-joint-statement-on-financial-services-data-connectivity

III. Conclusion

GDA appreciates this opportunity to provide comments on the KSDPA. We reiterate our support for the binding rules in KSDPA that prohibit unwarranted restrictions on cross-border data transfers and requirements to localize computing facilities. We also hope that the KSDPA's prohibition on location of computing facilities can be applied to financial institutions and financial service suppliers in the near future.

Sincerely yours,

Tham Shen Hong
Manager, Policy-APAC
Global Data Alliance