2 February 2023

BSA COMMENTS ON UNITED KINGDOM – REPUBLIC OF KOREA TRADE AGREEMENT NEGOTIATIONS

Submitted Electronically to the UK Department for International Trade

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to provide input to the United Kingdom's Department for International Trade (DIT) and the Department for Culture, Media and Sports (DCMS) on trade negotiations between the United Kingdom (UK) and the Republic of Korea (Korea).[2]

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA members are at the forefront of data-driven innovation that is fueling global economic growth, including cutting-edge advancements in artificial intelligence (**AI**), machine learning, cloud-based analytics, and the Internet of Things.

This submission will focus specifically on the digital trade component of the UK-Korea trade negotiations. BSA appreciates the UK's leadership in advancing regional and global frameworks for digital trade and cross-border movement of data.

The UK-Korea trade negotiations are an opportunity for UK to maintain and advance the high digital trade standards set forth in its recent agreements, such as the Australia-UK Free Trade Agreement, the UK-Japan Comprehensive Economic Partnership Agreement, and the UK-Singapore Digital Economy Agreement. These negotiations will also provide an opportunity for the UK to lead Government-to-Government (**G2G**) and Government-to-Business (**G2B**) projects that would bring tangible benefits to businesses. Accordingly, our submission covers:

1. Digital trade provisions to be negotiated;

2. "Early harvest" on cross-border data; and

3. Pilot projects and initiatives.

We have provided some proposed text for DIT's and DCMS's consideration in the Appendix at the end of this submission.

[1] BSA's members include: Adobe, Akamai, Alteryx, Atlassian, Autodesk, Bentley Systems, BlackBerry, Box, Cisco, Cloudflare, CNC/Mastercam, CrowdStrike, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intuit, Juniper Networks, Kyndryl, MathWorks, Microsoft, Okta, Oracle, Prokon, PTC, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trellix, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] Call for Input on trade negotiations with South Korea (publishing.service.gov.uk)

I. Digital Trade Provisions on Cross-Border Data Transfers and Digital Trust

BSA urges the UK to maintain a digital trade policy that: (1) safeguards cross-border data transfers and access to information, and (2) protects digital trust. BSA recommends that the UK propose the following digital trade provisions, which would build on prior UK digital economy agreements. Proposed text for these various provisions is found in the Appendix to this submission.

1. Provisions to safeguard responsible cross-border data transfers and access to information

- Cross-Border Transfer of Information by Electronic Means: Parties should not prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business.

- Location of Computing Facilities: Parties should not impose requirements to use or locate computing facilities in their own territory as a condition for conducting business.

- Custom Duties: Parties should not impose customs duties on electronic transmissions.

- Electronic Signatures: National laws should recognize electronic signatures in commercial transactions, including "smart" contracts.

2. Provisions to protect and build cross-border digital trust

- Protecting against Cybersecurity Risk: Parties should promote cybersecurity risk management frameworks based on internationally recognized standards and best practices**.** Parties should also refrain from imposing data localization mandates, data transfer restrictions, or other measures that exacerbate cybersecurity risk.

- Protecting Security Through Encryption: Parties should not undermine encryption in commercial products, and should not impose restrictions on security technologies used to safeguard against intrusions.

- Protecting Source Integrity: Recognizing the risks of malicious Parties should not require the transfer of, or access to, source code of software owned by a person of the other Party, as a condition of market access. Parties should also recognize that, in some cases, regulatory or judicial authorities may have a legitimate interest in such source code for a specific investigation or judicial proceeding.

- Protecting Privacy and Personal Data: Parties should commit to adopting or maintaining a framework that protects the personal data of those engaged in electronic commerce, while also striving to build interoperability between their respective protection frameworks.

- Protecting Procedural Limits on Government Access to Privately Held Data: Parties should ensure that law enforcement requests to access information are procedurally fair and transparent.[3] The Parties should also explore improved mechanisms for resolving differing legal requirements between jurisdictions.

- Promoting Trustworthy Artificial Intelligence**:** Parties should promote the AI risk management frameworks, prohibit unlawful discrimination through AI systems, promote AI-related R&D, and take other steps to promote trustworthy AI.

[3] *See e.g.*, OECD *Declaration on Government Access to Personal Data held by Private Sector Entities*, at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487

- Promoting Transparent and Non-Discriminatory Standards for Digital Services. Parties should support voluntary, internationally recognized standards on digital services and emerging technologies, and should refrain from imposing conflicting national standards in these areas.

- Promoting Online Consumer Protection: Parties should adopt or maintain laws that guard consumers from fraudulent or misleading conduct, which might be more prevalent when engaging in online commercial activities. Parties should also protect against unsolicited electronic communications.

- Promoting Technology Choice: Citizens and companies should be free to use the technology of their choice and should not be required to use local technology.

- Promoting Transparency and Access to Government Data: Parties should commit to making non-sensitive government-generated data freely available to the public, on a non-discriminatory basis, and in machine-readable formats.

- Promoting Non-Discriminatory Treatment of Digital Products: Parties should not accord less favorable treatment to a digital product created or produced by other parties than it accords to other like digital products.

- Promoting Digital Inclusion: Parties should work together to ensure that all people and businesses have what they need to participate in, contribute to, and benefit from the digital economy, to close the digital divide. This also includes creating an ecosystem that will enhance digital literacy and skilling.

II. "Early harvest" of cross-border data commitments

Out of the various digital trade provisions to be negotiated, those relating to cross-border data and access to information are particularly important critical for the efficacy and growth of the global digital economy. As such, the "early harvest" of these data-related provisions should be a priority in the digital trade negotiations.

Consistent with prior agreements, this "early harvest" should cover: 1) cross-border transfer of information by electronic means; 2) location of computing facilities; and 3) custom duties. There is widespread evidence of the benefits accrued from incorporating these commitments, which are set out in the Annex at the end of the submission.

These commitments focus on the impact that data regulations may have on trade among trading partners, and do not prevent governments from enacting rules to promote data privacy, data security, or other policy goals. To address the cross-border impacts of any data regulations that involve incidental restrictions on data transfers,[4] we urge the UK to clarify that such data regulations must:

- Be necessary to achieve a legitimate public policy objective;

[4] As connectivity and data have become integrated into every aspect of our lives, data-related regulation has become common in many areas: data privacy, cybersecurity, intellectual property, online health services – to name a few. Globally, the number of data regulations grew by over 800% between 1995 and 2015, and exceeds 250 today. *See* OECD, Trade and Cross-Border Data Flows, OECD Trade Policy Papers (2019), at: https://www.oecd-ilibrary.org/docserver/b2023a47-en.pdf?expires=1636811939&id=id&accname=guest&checksum=4D81CCF1C6E59168A9C5AE0E43F3F9FB

- Not be applied in a manner that would result in arbitrary or unjustifiable discrimination or a disguised restriction on trade;

- Not impose restrictions on transfers that are greater than required;

- Not improperly discriminate among different economic sector, such as the financial services sector;

- Not discriminate against other providers from either Party by modifying conditions of competition by treating cross-border data transfers less favorably than domestic ones;

- Be designed to be interoperable with other countries' legal frameworks to the greatest extent possible; and

- Be developed in a transparent and accountable manner.

The bulleted list above reflects longstanding tenets of international law and practice, namely: 1) the freedom to pursue necessary public policy objectives; 2) the renunciation of discrimination against non-national persons, products, services, or technologies; 3) the commitment to minimize trade-restrictive effects; and 4) due consideration for trading partner laws.[5]

III. Pilot projects and initiatives

Beyond its rule-setting function, the digital trade provisions of the UK-Korea FTA can provide an avenue for Parties to engage constructively with both other countries and the private sector, collaborating on G2G/G2B projects that would benefit both workers and businesses.

Our suggestions on possible projects and initiatives include the following:

- Working on data-driven innovation and collaborations, such as data sharing projects and regulatory sandboxes;

- Promote the development and use of internationally recognised standards in the fields of cross-border data transfers, cyber and data security, and AI;

- Agree on norms or best practices for the ethical use of AI and for AI risk management and co-create frameworks and guidance materials with industry on risk management tools and processes (e.g., how to conduct AI impact assessments);

- Explore the use of emerging technologies, such as blockchain and AI, to detect and combat forced labor practices in supply chains;

- Promote digitally focused development assistance activities and "earn-as-you-learn" programmes to help workers seize new opportunities in the digital economy;

- Collaborate on the use of digital technologies, including big data analytics, cloud, AI, and the Internet of Things, to reduce greenhouse gas emissions; and

[5] In the WTO context, these tenets – which trace back to the 1947 General Agreement on Tariffs and Trade – now apply to all multilateral trade rules, including those relating to goods, services, investment, technical regulations, and customs procedures. In the same spirit, UK and Korean should explicitly reaffirm the application of these core tenets to trade rules relating to the cross-border movement of data.

- Establish an annual or biannual public forum, where workshops and discussions can be conducted to share best practices and build capacity.

IV. Conclusion

We hope that our comments will assist the United Kingdom in its trade negotiations with Korea. **BSA would welcome the opportunity to engage with DIT or DCMS staff on these matters.** Please do not hesitate to reach out to us if you have any questions or comments.

Sincerely,

Thomas Boué
Director General, Policy, EMEA
BSA | The Software Alliance

Appendix

Proposed Digital Trade Provisions

Selected Provisions on Cross-Border Data and Access to Information

Article __: Supporting Cross-Border Access to Information

The Parties recognize that the ability to access, store, process, and transmit information across borders supports:

- The legitimate policy objectives of the Parties, including those relating to the protection of the environment, health, privacy, safety, security, and regulatory compliance;
- Sustainable economic development and shared economic prosperity, including through greater cross-border connectivity, including for Micro-, Small-, and Medium-Sized Enterprises;
- Financial inclusion and security, including for those lacking access to banking resources, as well as fraud prevention, anti-money laundering, and financial transparency;
- Healthcare delivery, research and development of new healthcare treatments, cross-border healthcare regulatory collaboration, and global medical humanitarian assistance;
- Scientific progress, including through cross-border access to knowledge and information, cross-border data analytics, and cross-border research and development (R&D) needed to develop technological solutions to meet global challenges;
- Cybersecurity, including through an enhanced ability to detect cybersecurity risks, respond to cybersecurity threats, and recover from cybersecurity incidents through real-time cross-border data access and visibility; and
- Climate change response, including through improved cross-border carbon emissions tracking and predictive climate modeling based on multi-regional data sets that can help communities to prepare for climate-related risks and identify mitigation and remediation strategies.

Article ___: Cross-Border Transfer of Information by Electronic Means

1. No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person.

2. In the case of transfers of financial information, no Party shall prevent a covered person from transferring information, including personal information, into and out of the Party's territory by electronic or other means when this activity is for the conduct of business within the scope of the license, authorization, or registration of that covered person.

3. This Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 that is necessary to achieve a legitimate public policy objective, provided that the measure:

   a. is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade;[6] and
   b. does not impose restrictions on transfers of information greater than are necessary to achieve the objective.

[6] A measure does not meet the conditions of paragraph 2(a) if it accords different treatment to transfers of information solely on the basis that those transfers are cross-border and if it does so in a manner that modifies the conditions of competition to the detriment of service suppliers of another Party.

Article ___: Location of Computing Facilities

1. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.

2. In the case of financial information, no Party shall require a covered person to use or locate computing facilities in the Party's territory as a condition for conducting business in that territory, so long as the Party's financial regulatory authorities, for regulatory and supervisory purposes, have immediate, direct, complete, and ongoing access to information processed or stored on computing facilities that the covered person uses or locates outside the Party's territory.[7]

3. Examples of measures that would breach paragraphs 1 and 2 include those that:
    a. require the use of computing facilities or network elements in the territory of a Party;
    b. require the use of computing facilities or network elements that are certified or approved in the territory of a Party;
    c. require the localization of information in the territory of a Party;
    d. prohibit storage or processing of information outside of the territory of the Party;
    e. provide that the use of computing facilities or network elements in its territory, or the storage or processing of information in its territory, is a condition of eligibility relating to:
        i. technical regulations, standards, or conformity assessment procedures;[8]
        ii. licensing requirements and procedures;[9]
        iii. qualification requirements and procedures;[10] or
        iv. other governmental measures that affect trade; or
        v. condition market access upon the use of computing facilities or network elements in its territory or upon requirements to store or process information in its territory.

4. This Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 that is necessary to achieve a legitimate public policy objective, provided that the measure:
    a. is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade;[11] and
    b. does not impose requirements that are greater than are necessary to achieve the objective.

[7] The Parties recognize that immediate, direct, complete, and ongoing access by a Party's financial regulatory authorities to information of covered persons, including information underlying the transactions and operations of such persons, is critical to financial regulation and supervision, and recognize the need to eliminate any potential limitations on that access. Each Party shall, to the extent practicable, provide a covered person with a reasonable opportunity to remediate a lack of access to information as described in paragraph 2 before the Party requires the covered person to use or locate computing facilities in the Party's territory or the territory of another jurisdiction.

[8] "Technical regulation," "standard" and "conformity assessment procedure" have the meaning set forth in the WTO Agreement on Technical Barriers to Trade, Annex 1, at: https://www.wto.org/english/docs_e/legal_e/17-tbt_e.htm

[9] "Licensing requirement and procedure" has the meaning set forth in the WTO Reference Paper on Services Domestic Regulation, at: https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/L/1129.pdf&Open=True

[10] *Id.*

[11] A measure does not meet the conditions of paragraph 4(a) if it modifies conditions of competition to the detriment of service suppliers of another Party by according different treatment on the basis of the location of computing facilities used, or on the basis of the location of data storage or processing.

Article __: Customs Duties

No Party shall impose customs duties[12] on electronic transmissions, including content transmitted electronically, between a person of a Party and a person of the other Party.

Selected Provisions on Cross-Border Digital Trust

Article __ : Supporting Digital Trust

The Parties place a high value on building and strengthening public trust in the digital environment, and in that regard, recognize that:

1. Promoting personal information protection, consumer protection, and safeguards against unsolicited electronic communications can help enhance confidence in digital trade and can facilitate the delivery of economic and social benefits to citizens;
2. Protecting the integrity of source code and algorithms from malicious cyber-related compromise or theft necessitates limits on forced technology transfer and access mandates, but – at the same time – regulatory bodies and judicial authorities can have legitimate regulatory or judicial reasons to require that source code or algorithms be preserved or made available for a specific investigation, inspection, examination, enforcement action, or judicial proceeding;
3. Protecting cybersecurity through cyber-incident detection, response, and recovery depends in part upon effective cybersecurity risk management and real-time cross-border access to cybersecurity-related technologies and cyber threat indicators; and
4. Adopting Artificial Intelligence (AI) risk management frameworks can help ensure that AI is developed and deployed to produce benefits for the health and well-being of citizens, to safeguard democratic values, and to help enterprises map, measure, manage, and govern high-risk uses of AI, including those that may result in unlawful discrimination.

Article __: Protecting Personal Information

1. Each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade.[13] In the development of this legal framework, each Party should take into account principles and guidelines of relevant international bodies, such as the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013).

2. The Parties recognize that pursuant to paragraph 1, key principles include: limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability. The Parties also recognize the importance of ensuring compliance with measures to protect personal information and ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented.

[12] "Customs duty" includes any duty or charge of any kind imposed on or in connection with the importation of a good, and any surtax or surcharge imposed in connection with such importation, but does not include any:

(i) charge equivalent to an internal tax imposed consistently with paragraph 2 of Article III of the GATT 1994;

(ii) fee or other charge in connection with the importation commensurate with the cost of services rendered; or

(iii) antidumping or countervailing duty.

[13] For greater certainty, a Party may comply with the obligation paragraph 1 by adopting or maintaining measures such as comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy.

3. Each Party shall adopt or maintain non-discriminatory practices in protecting users of digital trade from personal information protection violations occurring within its jurisdiction.

4. Each Party shall publish information on the personal information protections it provides to users of digital trade, including how:

   (a) a natural person can pursue a remedy; and

   (b) an enterprise can comply with legal requirements.

5. Recognizing that the Parties may take different legal approaches to protecting personal information, each Party shall encourage the development of mechanisms to promote compatibility and interoperability between these different approaches. These mechanisms include:

   (a) broader international and regional frameworks, such as the APEC Cross Border Privacy Rules;

   (b) mutual recognition of comparable protection afforded by their respective legal frameworks, national trustmarks or certification frameworks; or

   (c) other avenues of transfer of personal information between the Parties.

6. The Parties shall endeavor to exchange information on how the mechanisms in paragraph 6 are applied in their respective jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility and interoperability between them.

7. The Parties recognize that the APEC Cross Border Privacy Rules System and/or APEC Privacy Recognition for Processors System are valid mechanisms to facilitate cross-border information transfers while protecting personal information.

8. The Parties shall endeavor to jointly promote the adoption of common cross-border information transfer mechanisms, such as the APEC Cross Border Privacy Rules System.

Article __: Protecting Source Code Integrity

1. No Party shall require the transfer of, or access to, a source code of software owned by a person of another Party, or to an algorithm expressed in that source code, as a condition for the import, distribution, sale or use of that software, or of products containing that software, in its territory.

2. This Article does not preclude a regulatory body or judicial authority of a Party from requiring a person of another Party to preserve and make available[14] the source code of software, or an algorithm expressed in that source code, to the regulatory body for a specific investigation, inspection, examination, enforcement action, or judicial proceeding, subject to safeguards against unauthorized disclosure.

Article ___: Managing Cybersecurity Risk

1. The Parties shall endeavor to:

   (a) build the capabilities of their respective national entities responsible for cybersecurity incident response; and

   (b) strengthen existing collaboration mechanisms for cooperating to identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks, and use those mechanisms to swiftly address cybersecurity incidents, as well as for the sharing of information for awareness and best practices.

2. Given the evolving nature of cybersecurity threats, the Parties recognize that risk-based approaches may be more effective than prescriptive regulation in addressing those threats. Accordingly, each Party shall endeavor to employ, and encourage enterprises within its jurisdiction to use, risk-based approaches that rely on consensus-based standards and risk management best

[14] This making available shall not be construed to negatively affect the software source code’s status as a trade secret, if such status is claimed by the trade secret owner

practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity incidents.

3. Given that cybersecurity certification requirements and other measures may increase risk when they contain elements that impair cross-border coordination or access to cybersecurity technologies, each Party's cybersecurity certification standards and other measures shall treat service suppliers from other Parties no less favorably than domestic service suppliers, including in respect of the domicile, nationality, or degree of foreign affiliation or ownership of the service supplier; in respect of the country of origin of the technology; and in respect of the location of computing facilities and the cross-border transfer of information.

Article ___: Promoting Trustworthy Artificial Intelligence

1. Each Party recognizes the importance of developing governance frameworks for the trusted, safe, and responsible development and use of AI technologies. To that end, each Party should take into account the OECD Principles on Artificial Intelligence. The Parties endorse the OECD's five recommendations to policymakers pertaining to national policies and international co-operation for trustworthy AI, namely: (2.1) investing in AI research and development; (2.2) fostering a digital ecosystem for AI; (2.3) shaping an enabling policy environment for AI; (2.4) building human capacity and preparing for labor market transformation; (2.5) and international co-operation for trustworthy AI.

2. Consistent with OECD Recommendations 2.2 – 2.3, the Parties acknowledge the benefits of supporting interoperable legal frameworks and voluntary consensus-based standards and best practices relating to AI. Each Party shall encourage organizations within their jurisdiction that develop and deploy AI systems to risk-based approaches that rely on consensus-based standards and risk management best practices to map, measure, manage, and govern high-risk uses of AI.

3. Consistent with OECD Recommendation 2.5, each Party recognizes that AI systems should not result in unlawful discrimination on people based on their race, color, religion, sex, national origin, age, disability and genetic information or any other classification protected by the law of the Party. Each Party also recognizes that existing nondiscrimination laws remain enforceable in instances involving the use of AI.

4. Consistent with OECD Recommendation 2.4, and recognizing the importance of workforce development for AI-related technical skills to empower and enable current and future generations of workers and to improve the quality of life of our people, the Parties shall, subject to the availability of resources, upon request, and on mutually agreeable terms and conditions, exchange information and best practices, and otherwise cooperate, to:

   (a) Develop programs to train and reskill workers for AI and other high-demand technology skills;
   (b) Invest in apprenticeship programs and other alternative pathways to future employment that require AI and other high-demand technology skills;
   (c) Explore public-private partnerships to expand the availability of real-time labor data that can improve employer and worker visibility into the AI and other digital skillsets that are most in-demand in their markets, allowing them to make informed choices about the types of reskilling efforts that will generate the most opportunity; and
   (d) Invest in inclusive science, technology, engineering and math education, with an emphasis on computer science, at all levels of the educational system.

5. Consistent with OECD Recommendation 2.1, each Party shall promote sustained investment in AI R&D and public-private collaboration across the IPEF region. The Parties shall, subject to the availability of resources, upon request, and on mutually agreeable terms and conditions, collaborate to:

   (a) take stock of and utilize existing science and technology cooperation and multilateral cooperation frameworks involving IPEF Parties;
   (b) recommend priorities for future cooperation, particularly in R&D areas where the Parties

share strong common interests, face similar challenges, or possess relevant expertise;

(c) coordinate as appropriate the planning and programming of relevant activities, including promoting collaboration among government entities, the private sector, and the scientific community;

(d) promote AI R&D, focusing on challenging technical issues, and protecting against efforts to adopt and apply these technologies in the service of authoritarianism and repression; and

(e) explore the development of sharing best practices on public data sets to unlock AI innovation and exchanges of information on regulatory frameworks to remove barriers to innovation.