Study on the potential impact of a future EU-RoK digital trade agreement

30 November 2024

EU-RoK Policy Dialogue Support Facility

Funded by
the European Union

ICF

ICF makes big things possible

ICF is a global consulting and technology services provider with more than 7,000 professionals focused on making big things possible for our clients. We are policy specialists, social scientists, business analysts, technologists, researchers, digital strategists and creatives. Since 1969 government and commercial clients have worked with ICF to overcome their toughest challenges on issues that matter profoundly to their success. Our five core service areas are described below. Engage with us at icf.com.

Disclaimer

This publication was funded by the European Union. Its contents are the sole responsibility of ICF S.A. and do not necessarily reflect the views of the European Union.

A report submitted by ICF SA

Date: 30 November 2024

Job Number: J 330300751

ICF SA
Avenue Marnix 17, Brussels
B-1000, Belgium

www.icf.com

Document control

Document title	Study on the potential impact of a future EU-RoK digital trade agreement
Job no.	J 330300751
Prepared by	Michael Mudd, Irina Korgun, Tony Michell
Checked by	Tony Michell, Irina Korgun, Eunjung Choi
Date	30 November 2024

Contents

Abbreviations and Acronyms

4IR	Fourth Industrial Revolution
ACCL	The Anti-Cyber Crime Law
APEC	Asia Pacific Economic Cooperation
API	Application Programming Interface
CPEA	Cross-Border Privacy Enforcement Arrangement
CBDC	Central Bank Digital Currency
CBDF	Cross-Border Data Flow(s)
CBPR	Cross-Border Privacy Rules
COE	Council of Europe
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
CSP	Cloud Service Provider
DEPA	Digital Economy Partnership Agreement (NZ/SIN/CHL/Korea)
D2B	Direct-To-Business
D2C	Direct To-Customer
DID	Digital ID
DLP	Data Loss Prevention
DPIA	Data Protection Impact Assessment
DPRK	Democratic People's Republic of Korea (North)
DFTA	Digital Free Trade agreement
DSA	Data Sharing Agreement
DPO	Data protection Officer
EC	European Commission (of the EU)
EHR	Electronic Health Record
eIDAS	electronic Identification, Authentication, and trust Services
EORI	Economic Operators Registration and Identification number
EDPB	European Data Protection Board
ESF	Enduring Security Framework
EU	European Union
EUD	Delegation of European Union
EU-KDTA	European Korean Digital Trade Agreement
FinTech	Financial Technology Services
FSS	Financial Supervisory Service (Korea)
G20	Group of 20 Largest Economies (G7 is a subgroup)
GDPR	General Data Protection Regulation (EU)
GCI	Global Cybersecurity Index (ITU)

GPT	Generative Pre-trained Transformer (AI),
GSMA	Association for Mobile Telecommunications
GRC	Governance, Risk management and Compliance
JSI	Joint Statement Initiative on e-Commerce (WTO)
IAM	Identity and Access Management
ICT	Information and Communications Technology
ICO	Information Commissioner's Office (UK)
IETF	The Internet Engineering Task Force
IOT	The Internet of Things
IPEF	Provisional Entry into Force - Investor-State Dispute Settlement (ISDS) (CPTPP)
IPEFP	Indo-Pacific Economic Framework for Prosperity
ISO	International Standards Organization
ITU	International Telecommunications Union
KISA	Korea Internet and Security Agency
K-SDPA	Korea-Singapore Digital Partnership Agreement
Korea	Republic of Korea
KPI	Key Performance Indicator
KYC	Know Your Customer (also eKYC)
MSIT	Ministry of Science, Information and Communication Technology (Korea)
OECD	Organization for Economic Co-operation and Development
NIST	National Institute of Standards and Technology (US)
PETs	Privacy Enhancing Technologies
PIPA	Personal Information Protection Act
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RCEP	The Regional Comprehensive Economic Partnership
ROK	Republic of Korea (South)
SME	Small and Medium Sized Business(es)
SSL	Secure Sockets Layer
SWIFT	The Society for Worldwide Interbank Financial Telecommunication
UNCTAD	United Nations Conference on Trade and Development
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNICITRAL	United Nations Commission on International Trade Law
VAT	Value Added Tax

Executive summary

This report sets out the team's approach to the parameters of the study authorised by PDSF AToR37 commenced in late April 2024.

The European Union (EU) and Korea are currently negotiating an EU-Korea Digital Trade Agreement (EUKDTA). This agreement seeks to build upon existing frameworks, including the EU-Korea Free Trade Agreement (FTA) and the 2020 EU-Korea Digital Trade Principles. These negotiations are taking place against the backdrop of a growing web of digital trade commitments for both the EU and Korea.

This study provides an overview of the underlying legislative frameworks relevant for the negotiations and existing digital trade commitments., and the broader context of global digital trade frameworks. As the EUKDTA talks remain in progress at the time of drafting this report, report, information from the negotiation rounds – which is confidential – is included. Instead, the report examines the initial negotiating landscape, identifies areas of overlap and gaps between existing and planned digital trade provisions, and explores the potential implications of likely outcomes for governments, businesses, and civil society.

This report will also examine necessary steps that would provide a basis to deepen relations between the EU and Korea, facilitate the EU's position as Korea's biggest foreign direct investor, and allow service providers from the EU and Korea to compete on a level-playing field.

Specifically, the report will review the current conditions in bilateral digital trade and regulations, conduct a survey of businesses to bring in their perspective on the matter, and try to estimate the potential impact of a possible future DTA between the EU and Korea.

This report is continuing the previous project PDSF AToR34 which concentrated on key issues such as regulation, data, localisation, cloud security and financial system network segregation and the more comprehensive approach of the present study.

As a result of studies conducted at the end of the work on AToR34, the team's conclusion is that Korea's digital economy is well-developed internally, but that its integration internationally is limited. For example, the integration of its information and communication technology (ICT) infrastructure is limited, possibly due to the country adopting standards that differ from the rest of the world. This may result from barriers created by internal regulation, as well as a lack of binding commitments in its digital agreements, or a lack of digital companies exploiting opportunities to expand internationally.

This study, AToR 37, pursues six main objectives.

1. Sketch out evolving initiatives in digital trade regulation at multilateral level – such as the World Trade Organization (WTO) Joint Statement Initiative on E-Commerce (JSI) – as well as regional and bilateral levels (standalone DTAs and trade agreements with chapters on digital trade).
2. Make a comparative analysis of Korea's digital trade chapters and DTAs - notably the Digital Economy Partnership Agreement (DEPA) and the recent Korea-Singapore Digital Partnership Agreement (KSDPA) – with existing forward-looking DTAs, some of the EU agreements, as well as the WTO JSI.
3. Conduct an in-depth investigation of Korea's regulation that is applicable to both a broader digitised economy and, more narrowly, digital trade.
4. Survey and analyse potential outcomes of the DTA for EU companies.

5. Construct an estimate or range of estimates of an overall economic effect of a future DTA on trade flows in goods and services between the EU and Korea and its importance to business and the wider community.

Section 1 of the study describes general trends in the development of digital trade regulation on multilateral and regional levels. It also establishes a relationship between the existing EU-Korea Digital Partnership and the DTAs as well as EU-Korea FTA and the DTA.

The second part of the study, Section 2, analyses Korea' existing DTAs and how they compare in terms of the issues covered, and binding with the WTO JSI and some of the EU trade agreements that have e-commerce/digital chapters. Section 3 presents an overview of Digitalisation trends in the Korean economy and explores various dimensions of the digital trade between the EU and Korea, including trade in digitisable products.

Sections 4 to 6 analyse Korea's internal regulation and certification standards with regard to data and other digital issues, and explain where some legislation may affect the direction of a future a DTA. They also identify areas that increase costs of operations for foreign businesses.

These sections draw attention to where foreign affiliates in Korea are limited in their ability to use and analyse data, which puts them in an inferior position in competition with domestic players. Korea's reluctance to harmonise payment authentication limits trade opportunities in digitally delivered services, and the participation of small businesses in bilateral digital trade, as well as causing other problems.

The report outlines the relationship between cybersecurity and the DTA in Section 7. It notes that some of Korea's domestic regulatory initiatives are aimed at creating the necessary conditions for sustainable development of digital trade, but that the country's overall security structure has shown weaknesses in the face of cybersecurity attacks.

Section 8 investigates the benefits of a future DTA. It draws on existing studies on the effect of digital trade on economic development and growth to estimate the potential effects on trade flows between the EU and Korea.

Section 9 presents interview and survey results of foreign businesses operating in Korea. It highlights some of the major digital trade related barriers that European companies face in the Korean market, and draws attention to some of the specific regulations that they have to deal with. Surveys verified that, overall, businesses view the ongoing negotiations on a DTA positively, as the agreement will likely help in harmonising certain standards and regulatory practices.

Finally, Section 10 concludes by highlighting that the DTA can be seen as an optimal policy choice that will foster EU Korea cooperation in digital areas by providing transparent, predictable and clear guidelines for businesses, civil society and other actors involved in cooperation, and prepare both parties for a more digitalised future.

Section 1. Background of the expansion of digital trade agreements

1.1 General trend

Multilateral organisations such as the WTO[1], the World Bank[2] and the Organisation for Economic Co-operation and Development (OECD)[3] all pursue active policies on digital trade. The G20 issued the 'Osaka Declaration on the Digital Economy' at the G20 Osaka Summit, 2019[4], with Korea as a signatory member. Following up on the April 2021 'Digital and Technology Declaration'[5], the G7 came out strongly in favour of secure and trusted digital commerce, with Korea as an signatory observer. Korea has also endorsed the declaration at a subsequent meeting in Japan[6].

However, moving from non-binding discussions at G-7/20 level, to binding multilateral trade agreements on digital trade at the WTO, has proved challenging. WTO members managed to agree on a political commitment not to impose customs duties on electronic transmissions, but it has to be renewed regularly. The recent extension at the 13th Ministerial Conference extends the moratorium to 2026 with future extensions jeopardised by opposition from a limited number of WTO members. In 2019, WTO Members initiated plurilateral negotiations under the JSI, which now includes 91 participants representing 90% of global trade. In July 2024, the co-conveners of the JSI announced on behalf of participants that, after five years of negotiations, they had arrived at a stabilised text (Annex 1).

The JSI's stabilised text represents a foundational step towards establishing global rules for digital trade. It aims to promote an open digital environment while addressing trust and facilitation issues that are essential for e-commerce growth. However, it lacks strong commitments on data flows, data localisation and the source code protection. Participants will now undertake domestic consultations with the aim of incorporating this outcome into the WTO legal framework.[7]

Slow progress and uncertainty in the e-commerce JSI negotiations have led to a series of bilateral and plurilateral trade agreements (PTAs) with chapters on e-commerce/digital trade, or standalone DTAs.

The Trade Agreement Provisions on Electronic-commerce and Data (TAPED) dataset, published by the University of Lucerne, seeks to trace developments in digital trade governance comprehensively.[8] Its most recent version covers 432 PTAs concluded or signed between January 2000 and November 2023. Of those, 214 contain provisions relevant for e-commerce and digital trade, and 122 have dedicated e-commerce or digital trade chapters. Of the PTAs concluded or signed from January 2020 to November 2023, 90% contain provisions on digital trade or e-commerce, reflecting a general trend towards regulating digital trade.

[1] WTO - Osaka declaration 2019

[2] The World Bank - The Regulation of Digital Trade 2020

[3] OECD - Digital Trade

[4] G-20 - Osaka declaration 2019

[5] G-7 - Digital and Technology Ministerial Declaration 2021

[6] G7 - G7+ Australia, India, Korea, and South Africa Digital Technology Ministers meeting 2021

[7] WTO e-commerce latest updates

[8] A Dataset on Digital Trade Provisions; The TAPED

PTAs and DTAs tend to cover several important topics such as: (1) cross-border data flows, including prohibitions of unjustified data localisation requirements; and (2) disclosure or transfer of the source code.

Meta-analysis from the TAPED indicates that 49 PTAs (or just over 11%) contain provisions on the free movement of data. Of these, 19 are not legally binding, while 30 are. Out of the 49 PTAs concluded or signed since January 2020, 19 (or 38% of the reference period PTAs) contain a provision on cross-border data flows. Of these, 16 are binding. Other relevant provisions include review clauses in which the parties agree to review data flow provisions after a certain amount of time. Such a clause is included in the EU-Japan agreement.

Only 32 PTAs out of 432 contain a provision on banning or limiting data-localisation requirements, with varying levels of ambition. This represents 7% of the total number of PTAs. Out of the 49 PTAs concluded or signed from January 2020 to November 2023, only 16 contain a provision banning or limiting data-localisation requirements. This indicates a tendency to agree on prohibitions of data localisation, and a more differential approach to data flows.

Of the total 432 PTAs, only 23 PTAs contain a provision on the disclosure or transfer of the source code. Of these, 22 are binding.[9] Since January 2020, a further 12 PTAs have contained a provision on the subject, and there has been some convergence between the US-led and EU models in this regard, although the EU still inserts several exceptions.[10]

Data protection is the issue on which most governments agree. In agreements concluded or signed since January 2020, 32 out of the 49 PTAs have included a relevant provision. However, half of them is non-binding. The trend is to converge on internationally accepted standards, principles, and guidelines.

Provisions on the facilitation of digital trade are also a rising trend, reflecting the parallel developments occurring in the context of the WTO JSI negotiations.

Korea geographically is an Asia – Pacific economy so it has pursued agreements with neighboring countries with regards to digital trade. The most active country in the region was Singapore, followed by New Zealand and Australia.[11] DEPA, of which Korea is a recent party, remains, one of the most prominent trade agreement addressing issues in cross-border digital trade regulation to date. Korea and Singapore were among the first regional players to implement a DTA, which includes a broad spectrum of regulatory initiatives in its text. Singapore has also signed Digital Economy Agreements (DEAs) with Australia, the UK and the EU.

Two other important agreements - the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Regional Comprehensive Economic Partnership (RCEP) - both include broad digital/e-commerce commitments such as rules to facilitate cross-border data flows, ban server localisation, and promote data privacy and consumer protection. However, only CPTPP addresses Intellectual Property of source code.

The 10 members of the Association of Southeast Asian Nations (ASEAN) are working on an upgrade to their 2018 E-Commerce Agreement to become the Digital Economy Framework Agreement (DEFA) in 2025. According to D. Elms the real benefit of DEFA might be found in an improved organisational structure to manage digital trade for the region. Importantly, DEFA is a commitment to getting a coherent structure in place and providing platforms for regular ongoing discussions on topics of importance.[12] DEFA could influence certain aspects of

[9] The Evolution of Digital Trade Law: Insights from TAPED.

[10] See e.g. Article 207 EU–UK TCA

[11] WTO Joint Statement Initiative on E-commerce: Statement by Ministers of Australia, Japan and Singapore

[12] Elms, D. 2024 Designing ASEAN's digital trade framework

Korea's digital trade policy and regulation, as the country is connected to participating countries through various agreements, including RCEP.

The Asia Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) system and the ASEAN Framework on Personal Data Protection (PDP) are two examples, addressing data privacy. The ASEAN Single Window Agreement, and the Framework Agreement on Facilitation of Cross-Border Paperless Trade in Asia and the Pacific, focus on the Digitalisation of trade documents.[13]

The latter agreement is particularly important for sustaining free movement of goods along value-chains, which are abundant in the region. Additionally, the UN Framework Agreement on Facilitation of Cross-Border Paperless Trade in Asia and the Pacific (CPTA) provides a neutral platform for testing cross-border paperless trade solutions among over 50 member states, enabling harmonisation of electronic trade data and document exchange rules and systems.[14]

Work by the United Nations Economic and Social Commission for Asia and the Pacific (ESCAP) on digital trade regulation at multilateral and regional levels cautions that despite convergence on certain issues and the emerging overlap in coverage, countries use different legal languages to adjust the level of commitment in different areas. This is indicative of different approaches to the governance principles for digital trade. Some countries are more concerned with creating incentives to innovate reserving a limited role for government, while others pursue digital protection. The protection of the rights of individuals, preservation of the democratic rights of society and more equitable distribution of gains from the digital economy are very central for European policymakers. [15]

1.2 The EU – Korea digital partnership and digital trade principles

Prior to entering into negotiation on the DTA, the EU and Korea signed two documents intended to set the tone for cooperation on issues related to digital trade – the EU-Korea Digital Partnership and the EU-Korea Digital Trade Principles. The Digital Partnership, a 16-page document signed on 28 November 2022, is an outcome of Korea-EU summit that took place on 30 June 2020. It serves to align their national strategies (Korean Digital Strategy' and the European Commission "2030 Digital Compass Communication) for dealing with the challenges of the Fourth Industrial Revolution and human-centric digitalisation.

The Digital Partnership is an overarching document that provides the masterplan for cooperation to address digital-related challenges. It is an expression of shared views on core issues of the digital economy, along with intentions to cooperate in areas of digital infrastructure, capacity building, relevant standards and cybersecurity, and to foster research and development in areas of artificial intelligence (AI), quantum and other future technologies. However, it is not legally binding and not intended to supersede national law or international obligations. In addition, the document emphasises that any outcomes produced as a result of the Digital Partnership shall fall under the domestic law of each side. The Digital Trade Principles signed on 30 November 30 2022, are an initial deliverable of the Digital Partnership and set the agenda for a future DTA.

[13] Runqiu Du, Yann Duval, Maria Semenova, Natnicha Sutthivana (2023). "Multilateral and Regional Cooperation Trends in Digital Trade in the Asia-Pacific Region", ARTNeT Working Paper Series No. 227, October 2023, Bangkok, ESCAP.

[14] Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific (CPTA).

[15] Bradford, A., 2023. Digital Empires: The Global Battle to Regulate Technology. New York: Oxford Academic. https://doi.org/10.1093/oso/9780197649268.001.0001

The Digital Trade Principles encourages adherence to the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce (1996), and UNCITRAL Model Law on Electronic Transferable Records (2017), signalling support for the existing multilateral agreements that can be applied to digital trade. Section 2 of the Digital Trade Principles deals with digital trade facilitation and includes such important areas for businesses, such as electronic contracts, e-authentication and e-signatures, e-invoicing, e-customs and transfer of records. Other issues covered include: the concept of 'data free flow with trust'; unjustified obstacles for data transfers; consumer trust; business trust; open internet access; cybersecurity; source code; and cryptography. The document instils an idea that the development of digital trade requires adequate governance to ensure that the core interests and rights of all digital trade actors are taken into account and protected.

The concept of 'data free flow with trust' is also part of the Singapore-EU Digital Trade Principles, and has been promoted by Japan and others in the context of the G7[16]. Similar to the Digital Trade Principles with Singapore, the Digital Trade Principles with Korea contain a commitment to open government data, calling for government data to be made publicly available in an anonymised, open, interoperable and machine-readable format, where appropriate. Considering that Korea has already concluded a DTA with Singapore, sharing similar commitments with the EU creates a basis for interoperability and common standards between Europe and key Asian partners, with the potential for these standards to be expanded further in the region.

1.3 EU-Korea FTA's applicability to digital trade

The EU Korea FTA in force does not include a modern ecommerce/digital chapter. However, some parts of the agreement could be applicable to digital trade.

The FTA includes a prohibition of customs duties on electronic transmissions. In addition, it has deep commitments on services market access and national treatment for the sectors needed for e-commerce/digital trade: computer and related services, telecommunications, and financial services, as well as a provision on the non-imposition of customs duties on electronic transmissions.

The dispute settlement mechanism applies to e-commerce/digital trade provisions and in particular the core provisions on non-discrimination and customs duties.

Certain areas of the agreement could be applicable to paperless trading, customs procedures, and automated or custom data exchange systems. It also recommends avoiding any unnecessary regulatory burden on e-commerce, and that e-commerce must not be more restricted than other trade.

Article 7.43 of the FTA includes a commitment on data processing, committing the parties to permit a financial service supplier of the other Party established in its territory to transfer data into and out of its territory for data processing.

The FTA does not include:

- provisions on e-invoicing, facilitation of e-payments, and other digital trade facilitation provisions;
- prohibitions of access to the source code of software;
- provisions on cybersecurity or open internet access/net neutrality;
- provisions on the free movement of data, other than for financial services.

[16] Data Free Flow with Trust.

Section 2. An overview of Korea's agreements on digital trade

This section is focused on several agreements: DEPA, the Korea-Singapore DTA, RCEP and the Korea-UK agreement. The focus is to identify core and new issues and provisions, as well as the level of ambition codified in the language of the agreements. More information of coverage on the digital trade-agenda issues in the e-commerce chapters of Korea's FTAs is given in Annex 1 A 1.2.

2.1 DEPA

DEPA is a plurilateral trade agreement focused on digital trade, founded by Singapore, New Zealand and Chile[17]. Korea became the first economy outside the founders to become a member in May 2024, supported by Singapore. [18]

Korea's participation is deemed very positive due to its role as a major producer of chips and other ICT products that are vital in the digital era, as well as the many political values and respect for the rule-based international trading system that it has in common with other DEPA members.

DEPA has a 'modular structure', which means that the different chapters include a glossary and have no cross-referencing between different chapters. The agreement adopts an open, plurilateral approach that allows other countries to join as whole, select specific modules or replicate the modules in other trade agreements.[19] It has modules on e-invoicing and e-payments and specified rules on non-discrimination for digital products, facilitation of e-commerce and cooperation on ICT. Other modules are forward-looking to cover regulatory sandboxes for testing new ideas in data innovation.

The key principles of DEPA[20] are as follows:

1. **Recognising the importance of the digital economy** and the need to harness technological advances to create new products and markets, and enhance daily life.
2. **Promoting open, fair and transparent digital trade** by establishing basic rules to facilitate the export of digital services and products.
3. **Exploring new technological subjects** that benefit society through inclusive economic development.
4. **Acknowledging the role of standards, and particularly open standards**, in facilitating interoperability between digital systems and enhancing value-added products and services.
5. **Promoting cooperation on emerging technologies** such as financial technology (FinTech), AI, and digital identities.

[17] All three economies are also members of the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP). CPTPP – a UK report 2024 for the Commons

[18] DEPA – Korea application 2021

[19] https://www.kommerskollegium.se/contentassets/d4c3fa9298384ca1b860169afb1bf732/the-digital-only-trade-agreements--what-is-new.pdf

[20] DEPA – Agreement text

6. **Fostering close cooperation between small and medium-sized enterprises (SMEs)** to enhance their participation in the digital economy.
7. **Emphasising digital inclusion** to ensure all people and businesses can participate in and benefit from the digital economy.
8. **Recognising the need to update global rules** in response to the growing range of barriers related to trade in the digital economy.
9. **The digital economy's impact on competition policy and government procurement is also recognised**. However, in these emerging areas, there are no binding commitments, simply 'best efforts' language to promote cooperation.
10. **Affirming the importance of promoting corporate social responsibility,** cultural identity and diversity, environmental protection, gender equality, labour rights, and sustainable development.

Some of the important provisions under DEPA include:

- prohibitions on requirements to store or process data locally;
- prohibitions on the transfer of or access to computer source code;
- prohibitions on requirements to use local computer facilities;
- prohibitions on requirements for local content in electronic transmissions;
- prohibitions on transfer of technology as a condition of foreign investment.

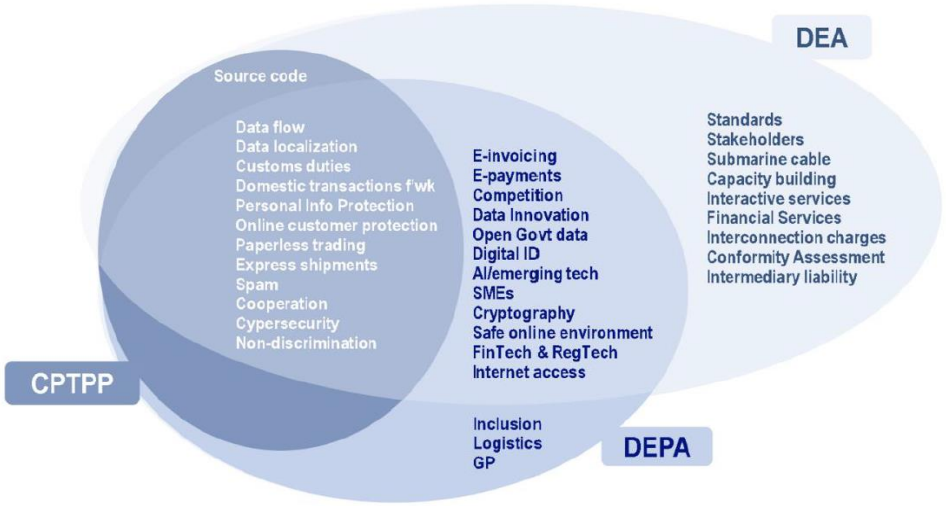
Although the commitments are mostly non-binding (granting governments the right to apply domestic law on data protection), and focused on cooperation and dialogue, they create a necessary platform for forging interoperability in member-countries' regulation of digital trade, covering issues such as AI, fintech and digital identity. For example, DEPA has recommended the recognition of data protection trust marks to verify conformance with privacy standards.

Importantly, the commitments included in this agreement do not apply to financial services or government procurement.

If DEPA is compared (figure 2.1 on the next page) with agreements such as CPTPP (one of the earliest FTAs to consider digital-trade related issues) and the Australia-Singapore DEA, it becomes obvious that later agreements go beyond the core issues included in CPTPP, tending to include more cross-cutting issues that span into emerging areas, such as cooperation on AI, digital identity and open government data.[21]

[21] Javier López González, Silvia Sorescu and Pinar Kaynak. Of Bytes and Trade: Quantifying the Impact of Digitalisation on Trade. TRADE POLICY PAPER May 2023 n°273.

Figure 2.1 Comparison of digital trade agenda issues coverage in DEPA, CPTPP and DEA



Sources:
Panel A: Based on TAPED database, agreements entered into force by 2022 considered.
Panel B: Honey (2021[11]), https://www.tradeexperettes.org/blog/articles/untangling-the-digital-noodle-bowl-the-case-for-depa.

2.2 Korea - Singapore DPA

The KSDPA[22] is an annex to Korea - Singapore FTA (KSFTA[23]) that replaces the provisions of Chapter 14 (Electronic Commerce), Chapter 12 (Financial Services) and Chapter 21 (Exceptions) of KSFTA.

The KSDPA aims to strengthen the KSFTA e-Commerce chapter by increasing bilateral cooperation in trade facilitation, digital identities, fintech and e-payments, AI and other areas of research and investment.

The key features of the KSDPA include:

1. **facilitating end-to-end digital trade** through e-payments and paperless trading;
2. **enabling trusted data flows** by allowing cross-border data transfers, prohibiting data localisation requirements, and ensuring open government data;
3. **facilitating trust in digital systems and participation in the digital economy** through cooperation on AI, protecting cryptography and source codes, ensuring online consumer protection, promoting SME cooperation, and enabling interoperability between digital identity regimes.

The KSDPA confirms the non-imposition of customs duties on electronic transmissions, explicitly referencing UNCITRAL and UN conventions to ensure consistency in the domestic legal transaction frameworks. The agreement contains provisions on: e-invoicing; the facilitation of e-payments; electronic authentication; electronic signatures and digital certificates; paperless trading; electronic transferable records; customs-procedures automation or custom data-exchange systems; consumer protection; and net neutrality. However, many of these provisions are written in a soft language, suggesting some flexibility in their interpretation (e.g. for national security measures).

[22] The KSDPA

[23] The KSFTA effective date 2006

In the realm of data, the agreement includes prohibitions to require the transfer of, or access to, source code of software owned by a person, as a condition for the import, distribution, sale or use of such software. It also includes provisions on cryptography and cybersecurity.

The DPA allows for exceptions to its general rules on data flows and localisation under specific circumstances related to legitimate public policy objectives:

- **National Security**: The DPA specifies that data flows can be restricted for national security purposes.
- **Public Health and Safety**: The DPA states that transfers may also be restricted if deemed essential for protecting public health or safety.
- **Law Enforcement**: The DPA specifically acknowledges that law enforcement agencies may require access to personal data across borders in order to investigate or prevent criminal activities.
- **Compliance with Local Laws**: If local laws mandate specific requirements for data handling that conflict with the DPA's provisions, those local laws take precedence.

However, article 14.15 of the agreement contains a carveout that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications. In Korea's context, such data include financial data, medical data (unless it has been randomised and is transmitted for research in accordance with agreed policies).

The agreement refers to the protection of data, recognising certain international standards; the free movement of data; and a provision banning or limiting data localisation. The text explicitly addresses the localisation of financial services data with a specific, legally non-binding provision. To be more precise, paragraph 4 of article 14.15 says that 'this Article shall not apply with respect to a "financial institution" or a "financial service supplier of a Party".

Of particular interest to the financial services industry, Paragraph (b) of the Article 14.16 specifies that each party shall identify, develop, and promote joint initiatives to facilitate covered financial persons to use or locate computing facilities outside of a Party's territory, as they may wish, for the conduct of business, as long as the Party's financial regulatory authorities, for regulatory or supervisory purposes, have immediate, direct, complete and ongoing access to information processed or stored on computing facilities that covered financial persons use or locate outside of the Party's territory."[24]

Korea-Singapore agreement includes a provision on open government data or open data and provisions referring to data innovation, allowing data to be shared and reused. Soft provisions are included on digital identities, digital inclusion, on fintech cooperation and AI.

Importantly, although the KSDPA is light on binding commitments, the three Memoranda of Understanding that accompany it are more specific and may be viewed as implementing guidelines for the DTA.

The three Memoranda of Understanding are on:

- implementing Korea-Singapore Digital Economy Dialogue[25];
- the Electronic Exchange of Data to Facilitate the Implementation of Korea-Singapore Digital Partnership Agreement[26];

[24] KSDPA

[25] Memorandum of Understanding between The Ministry Of Trade, Industry and Energy of The Republic of Korea and The Ministry of Trade and Industry of The Republic of Singapore on Implementing Korea-Singapore Digital Economy Dialogue

[26] MOU on the Electronic Exchange of Data to Facilitate the Implementation of Korea-Singapore Digital Partnership Agreement

- cooperation on Artificial Intelligence[27].

The agreement sets out non-binding guidelines to adopt internationally accepted standards and open application Programming Interfaces (APIs) to facilitate electronic data exchange between financial institutions and service suppliers to enable greater interoperability between electronic payments.[28]

In the most recent development, the Cyber Security Agency of Singapore (CSA) signed a Mutual Recognition Arrangement (MRAs) for the recognition of cybersecurity labels with Korea Internet & Security Agency (KISA) and Germany Federal Office for Information Security (BSI) on October 15, 2024.[29]

2.3 The regional comprehensive economic partnership (RCEP)

The RCEP[30] is a 15-member economic block in East Asia-Pacific including Korea which was created on 15 November 2020. It encompasses about 2.3 billion people and 30% of global trade, making it the world's largest trading area[31], eclipsing the former top spot held by the EU until the UK quit. There is considerable membership overlap with the CPTPP, but the main differentiator is the inclusion of China. Uniquely, this is the only trade agreement that includes Korea, China and Japan as member states. Hong Kong applied to join the RCEP on 23 February 2022, and is expected to accede in late 2024.[32]

The RCEP is a binding agreement that came into effect in January 2022. The e-commerce provisions are covered in Chapter 2 and share similarities to the CPTPP, although they are not as prescriptive.[33]

Overall, the RCEP has low level of ambition on digital trade as most of commitments are non-binding and written out in rather soft language.

Key features of Chapter 12 of the RCEP include the following:

1. **Data free flow and protection**: Prohibitions against requirements for localised computer facilities and localised data, ensuring the free flow of data across borders.
2. **Business facilitation and promotion**: Encouragement of paperless trading, electronic signatures, reduced regulatory burdens, duty-free electronic transmissions, and flexibilities in data storage and cross-border data transmission.
3. **Connectivity and interoperability**: Improvements in areas such as paperless trading, consumer protection, and data transfers to enhance the e-commerce environment and reduce cybersecurity risks.

[27] MOU on Cooperation on Artificial Intelligence

[28] Korea-Singapore DTA enters into force.

[29] Singapore Signs Mutual Recognition Arrangements with Republic of Korea and Germany on Cybersecurity Labelling for Consumer Smart Products

[30] RCEP Overview 2021

[31] RCEP Forms the World's Largest Trading Bloc. What Does This Mean for Global Trade?

[32] Hong Kong has ASEAN backing to join RCEP trade pact: John Lee

[33] Chapter X Electronic Commerce

4. **Confidence and safe environment**: Provisions related to consumer protection, cybersecurity cooperation, online safety and security, unsolicited commercial electronic messages, and online consumer protection.
5. **Cooperation on emerging technology and governance issues**: Focus on digital identities, financial technology cooperation, AI, public domain, data innovation, open government data, SMEs in the digital economy, stakeholder engagement, and digital inclusion.

The agreement does not include binding commitments in relation to customs duties/tariffs on electronic transmissions. Moreover, in comparison to other agreements on digital trade, rules in relation to cross-border flow and localisation of data are relatively non-committal and flexible, offering exceptions for member countries to adopt or decline.

With regard to cross-border data flows, Article 12.15 provides a specific exception for measures to achieve a legitimate public policy objective:

3. *Nothing in this Article shall prevent a Party from adopting or maintaining:(a) measures inconsistent with paragraph 2 that it considers necessary to achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; or (*b) *any measure that it considers necessary for the protection of its essential security interests. Such measures shall not be disputed by other Parties.*

2.4 Comparison of DEPA, KSDPA and RCEP with WTO JSI and EU-New Zealand FTA

When the three above agreements are compared to the WTO JSI and EU-New Zealand FTA (Table 2.1 below), several common themes emerge:

- a moratorium on customs duties on electronic transmissions and digital products;
- a ban on data localisation;
- free cross-border transfer of data of personal information;
- protecting consumers' personal information;
- consumer protection laws that define and prevent fraudulent and deceptive commercial activities;
- measures against spam or unsolicited messages.

Issues on which agreements diverge relate to e-insvoicing and e-signatures, cooperation on AI, digital inclusion, data innovations, etc. (See more in detail in **Table 2.1** on the next page).

Table 2.1 Gap analysis of DTAs to which Korea is party

	DEPA	KSDPA	RECP	WTO JSI	EU-NZ
Moratorium on custom duties on electronic transmissions and digital products					
Non-discriminatory treatment for digital products					
Cross-border transfer of data / ban on data localisation					
Free cross border transfer of data					
Consumer protection laws that define and prevent fraudulent and deceptive commercial activities					
Measures against spam or unsolicited messages					
Prohibit parties from forcing transfer of source code as a condition for market access					
Collaboration on cybersecurity management					
Open government data					
Interoperable electronic invoicing					
Interoperable electronic payments system					
Interoperable digital identities					
Cooperation in fintech sector					
Ethical governance of AI					
Data innovation					
Digital innovation and emerging technologies					
Logistics best practices					
Standards and technical regulations					
Open Internet access to consumers					
Cooperation on digital inclusion					
Adapted in part from The Asia Foundation/Authors.	Binding	Non-binding			

Section 3. Trends in digitalisation in Korea and the EU-Korea digital trade

3.1 How far has Korea come on its digital journey?

Like many advanced economies, Korea is moving from digitisation to Digitalisation at all levels including social, economic and cultural life. Digitisation serves as the foundation for digitalisation. Without digitised data, organisations cannot effectively implement digitalisation strategies. In essence, digitisation is about making information digital, while digitalisation is about using that information to drive change and improve business outcomes.

Due to the country's positioning at the heart of digital technology value chains, the process of adaptating digital innovations is happening at a rapid pace. In 2023, the IMD World Competitiveness Center ranked Korea in the 6th out of total 64, 2 places up from the previous year. In the World Digital Competitiveness Ranking[34], Korea is ranked 1st for future readiness in terms of adaptive attitudes, business agility, technological framework and IT integration.[35]

These results are somewhat contrary to Korea's own findings that 61,5% of its companies were not ready for the digital transformation in 2022[36] with only 19% of SMEs having the relevant plans in place.[37] Some other areas in which Korea underperforms are talent, regulatory framework and capital.

Digital adaptation is intensified by some unique social problems such as low fertility, relatively low rates of women's participation in economic life, and rapid ageing of the workforce - these trends combine to stimulate a wider use of automated processes and robotics in industries and business. Currently, Korea is the leader in industrial robot density. According to the International Federation of Robotics, Korea had 1,012 robots per 10,000 employees in 2023, followed by Singapore (730 units) and Germany (415 units).[38]

The functioning of these machines relies on massive use of data, often hosted in the cloud, and requires a high standard of protection from cybersecurity attacks.

Robotics is set to become a strategic industry of the future. The government has unveiled plans to train more than 15,000 professionals to lead the advanced robot industry in connection with the mobility industries (e.g., future cars and drones) and to foster over 30 specialised intelligent robot companies with sales of over KRW 100 billion.[39]

Another rapidly developing area in Korea is the Internet of Things (IoT), which interconnects machines and computers through sensors. The projected revenue in the IoT market is estimated to reach USD 12.22 billion in 2024, and projected annual growth to 2029 is expected to exceed 6%, reaching USD 17.10 billion.[40] Since 2021, the market has been adding KRW 2 trillion (USD 1.45 billion) annually. At the end of 2023 the Korean government announced plans to invest KRW 123.5 billion jointly with the private sector to promote digital transformation in key processes across five industries: the automotive industry, battery sector, innovative materials, industrial machinery and shipbuilding. Under this program, there are plans to set up factories based on international standards, which can partially resolve Korea's deviation in

[34] World Digital Competitiveness Ranking

[35] Ibid.

[36] Digitalization of businesses [In Korean]

[37] Digital readiness of SMEs [In Korean]

[38] Global Robotics Race: Korea, Singapore and Germany in the Lead

[39] Korean government plans to invest in robotics [In Korean]

[40] Internet of Things in Korea

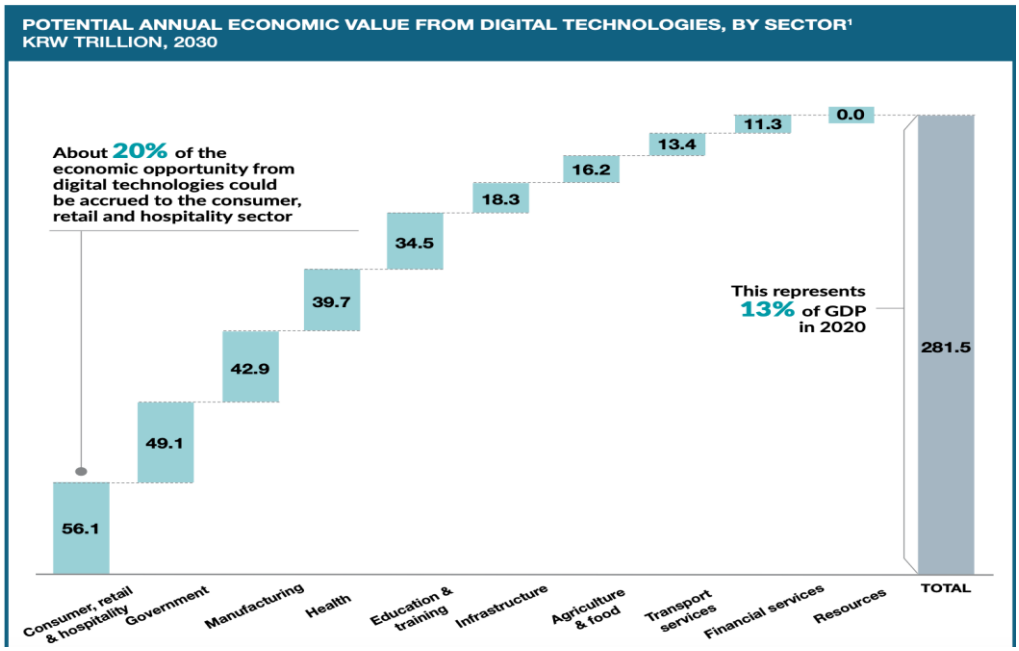
certain digital-related standards (an issue covered in this report further).[41] The plan also includes growing three Korean e-platforms with global outreach: buykorea[42]; gobizkorea[43]; tradekorea[44], with a combined sales of USD 10 billion.

There are challenges in estimating the total value of economic benefits generated by the use of automated process. However, data available on certain aspects give an idea of the magnitude of the effect. Korean businesses are estimated to derive annual economic benefits from Google's products worth KRW 10.5 trillion (USD 8.8 billion) and the estimate for the Korean consumers is KRW 11.9 trillion (USD 10 billion).[45]

As of 2021, the economic value generated by the digital transformation in Korea by 2030 would be USD 236 billion. Annually, this figure includes GDP increments, productivity gains, cost savings, time savings, increased revenues, increased wages and increased tax collection. Sectors that would enjoy the largest benefits are retail, hospitality, manufacturing, and government sectors.

The consumer, retail and hospitality sector is projected to be technology's largest economic beneficiary in Korea (Figure 3.1). This sector is estimated to be able to gain annual economic benefits of up to KRW 56.1 trillion (USD 47 billion) in 2030 – amounting to about 20 percent of the country's total digital opportunity. Other top sector beneficiaries include: government (KRW 49.1 trillion or USD 41.1 billion); manufacturing (KRW 42.9 trillion or USD 36 billion); health (KRW 39.7 trillion or USD 33.3 billion); and education and training (KRW 34.5 trillion or USD 28.9 billion).[46]

Figure 3.1 Potential annual economic value from digital technologies in Korea by 2030, by sector (KRW trillion) (Source: Access Partnership[47]).



To sum up, it is worth noting that the continued rapid digital transformation of Korean economy will create considerable value in various parts of the economy both in terms of cost optimisation

[41] Korea to invest into industrial digitalisation

[42] Buykorea

[43] Bizkorea

[44] Tradekorea

[45] Unlocking Korea's Digital Potential

[46] Ibid.

[47] Access Partnership.

and new business opportunities. However, the pace of the digital transformation varies considerably by sectors and types of company. Korea's global giants are leading this trend while SMEs face certain challenges that are linked to problems with access to capital, the talent pool and other things.

3.2 Digital trade between the EU and Korea

Digital trade refers to trade in goods and services that are either digitally ordered or digitally delivered. According to the recent calculations by the United Nations Conference on Trade and Development (UNCTAD), as of 2022, world total exports for services stood at around USD 7.1 trillion. Of that, more USD 3.94 trillion, or 54 % were digitally deliverable services.[48]

While statistical methods of accounting for the digital trade are still evolving, in literature there are several approaches for capturing the following international digital trade flows:

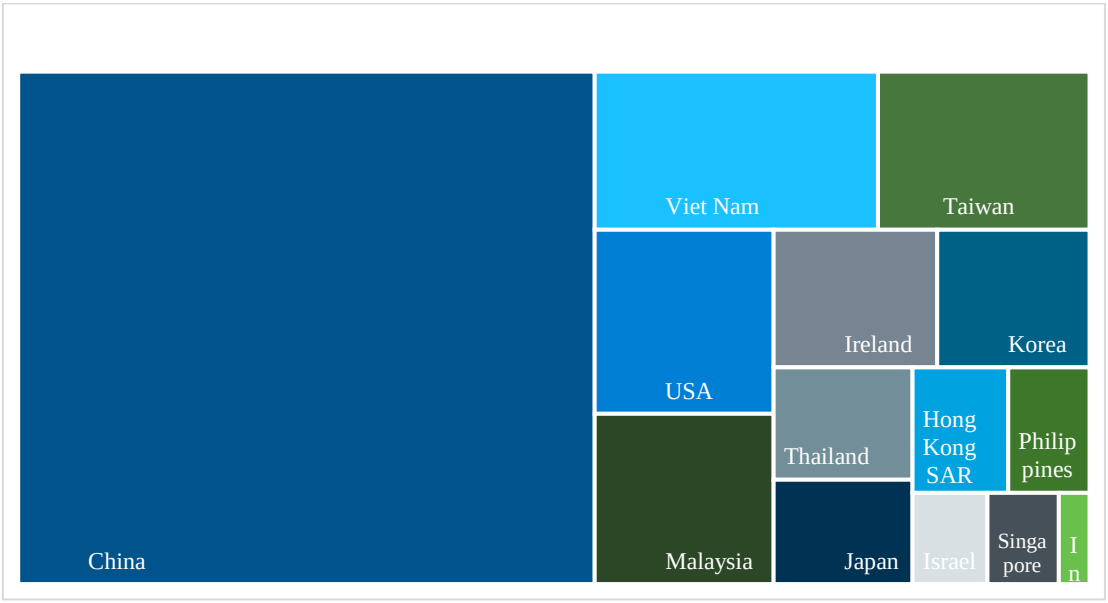
1) cross-border e-commerce;
2) trade in services with a digital component;
3) trade in ICT products, which make up the infrastructure for that enables e-commerce and trade in services (including semiconductors, computers, telecommunication devices and digital infrastructure, such as the internet and fibre-optic cables);
4) trade in digitally delivered content (sometimes referred to as digitisable products).

If the EU-Korea digital trade is estimated according to the above components, the following pattern emerges.

3.2.1 EU-Korea trade in ICT products

Trade in ICT goods between Korea and the EU reached USD 9.8 billion in 2021, with Korea maintaining a substantial surplus as its exports to the EU amounted to USD 7.1 billion, while imports reached USD 2.7 billion. In 2021, Korea ranked as the seventh-largest supplier of ICT goods to the EU, following China, Vietnam, Taiwan, the US, Malaysia, and Ireland (Figure 3.2).

Figure 3.2 EU sources of ICT imports (Source: data from UNCTAD)



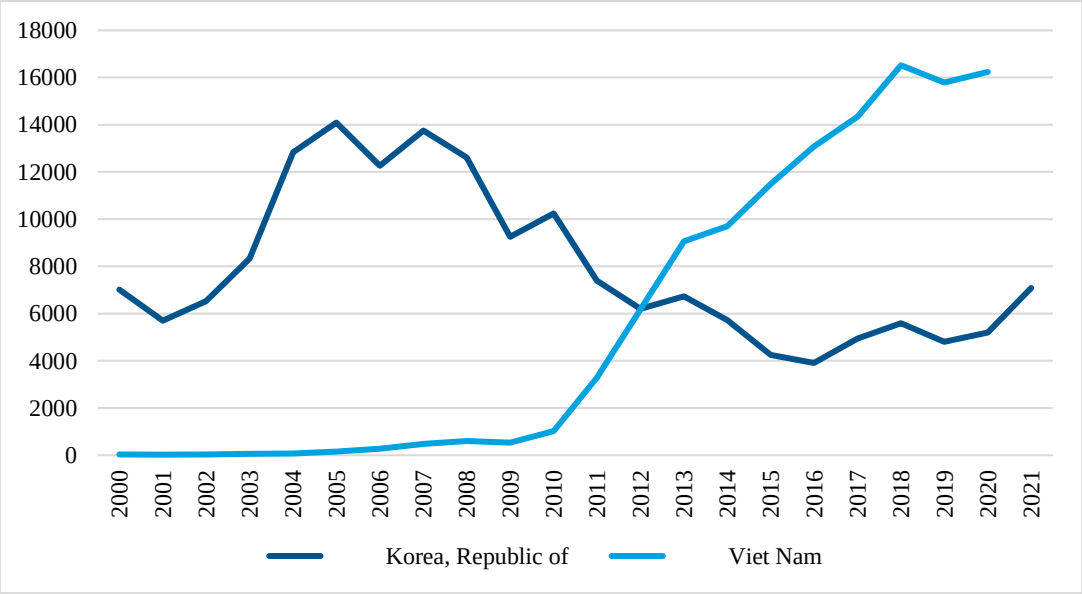
[48] UNCTAD – Digitally Deliverable Services Boom Risks Leaving LDCs Behind

The relatively low volume of Korea's direct shipments of ICT products to the EU is due to the effect of the regional value chains. Major Korean producers of semiconductors and electronic goods such as Samsung and LG have relocated parts of their production to Vietnam.

As Figure 3.3 shows, the decline in Korea's ICT exports to the EU in the late 2000s coincided with a steady increase in Vietnam's exports of ICT products to the EU. In 2012, there was a turning point where Vietnam's ICT exports surpassed those of Korea in value. By 2020, Vietnam was shipping four times the value of ICT products to the EU compared to Korea.

The impact of Samsung on the Southeast Asian economy remains significant, with the company accounting for 25% of Vietnam's total exports and 80% of its electronics exports in 2020[49]. Other Korean producers, such as SK Hynix[50], have also established a presence in Vietnam.

Figure 3.3 Korea and Vietnam ICT exports to the EU, 2000-2021, USD million



Source: constructed based on UNCTADstat

3.2.2 EU-Korea cross-border e-commerce

Korea's purchases through European and UK online platforms (disaggregated statistics not available) have shown steady growth since 2016 (see Table 3.4). During the COVID-19 pandemic, sales were up more than 20% to reach a record of USD1.15 billion in 2021. In 2023 Korea's online purchases went down to pre-pandemic levels to USD 874 million due to a combination of factors: the end of revenge buying; inflation putting pressure on Korean customer budgets; the start up of travel making Koreans prioritise their budgets; and the popularisation of Korean culture which made customers to look more to domestic brands. This declining trend was observed in most of the markets, with the exception of China. Many

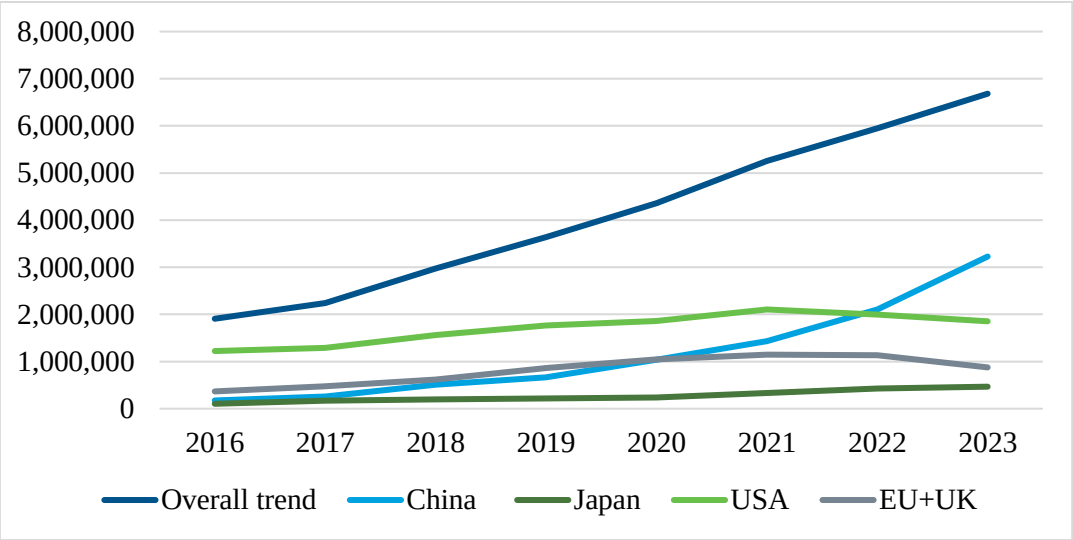
[49] Contribution from Samsung to the economy is still "unknown", or in other words, the regulatory agencies are not able to calculate. The official information on the financial situation is published by Samsung Vietnam on its website, citing the Financial Statements of the parent corporation in Korea, saying that the first three quarters of 2019 revenue and operating profit reached USD 51-53 billion and USD 6.4-6.6 billion respectively. There are no separate financial statements for Vietnam market, which is Samsung's largest global production base. // Vietnam Credit. (2020). Samsung: Driver of Vietnam's Economic Growth?; Business Korea (2019). Samsung Electronics Accounts for 28% of Vietnam's GDP.

[50] Korea IT News. (2022). Hana Micron, to hire 3,000 employees at a new plant in Vietnam

customers started using Chinese platforms more often to manage budgets under tightening economic conditions.

On the other hand, Korean sales to EU and UK increased in 2023 compared to 2023, more than doubling from USD 17 million to 36 million, but still could not reach pre-pandemic levels. Overall, the balance in the online trend remains favourable for Europe.

Figure 3.4 Volume of Korea's purchases from foreign online platforms (USD million)



Source: KOSIS

3.2.3 EU-Korea trade in services with the digital component

According to OECD data, trade in services with the digital component include such sectors as Insurance and pension services, Financial services, Charges for the use of intellectual property, Telecommunications, computer, and information services, Other business services, Commercial services, Other commercial services. The table 3.1 below showcases trends in total exports of these services by EU countries during 2011-2020 (the last year when statistics is available). The general trend was a positive one with countries like Denmark, Finland, Germany, Ireland, Netherlands, and Sweden improving their positions as providers of services with the digital component.

Table 3.1 EU countries export of services with the digital component to Korea, in Mn USD

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Austria	172,2	216,5	209,8	163,2	184,8	199,9	287	344,8	276,4	230,6
Belgium	110,5	166,1	212,6	248,5	219,2	162,7	176	191,4	204,4	143,2
Czechia	12	15,9	21	11	24,5	16,9	27,6	42,8	26	22,3
Denmark	1313,3	1301,2	1236,7	960,4	1093,8	970,4	1211,5	1178,2	1134	1707,6
Estonia	0,6	8,5	16	28,9	27,9	27,2	24,4	17	1,6	14,9
Finland	0	476,8	843,5	1151,7	1618,2	898	1870,7	1785,5	871,5	1163,9
France	1694,6	4649,8	6040,7	2663,9	2609	1730,5	2307,6	1239,2	1137,6	1200,5
Germany	3400,9	3887,4	6220,1	5783,8	6006,1	3593,6	4769,8	1391,5	1211,9	5088,1
Greece	333	365,6	384,1	239,4	197	276,9	326,2	307,5	250	492
Hungary	485,7	626,2	355,9	336,7	340,7	367,6	318,7	180,1	68	79
Ireland	265,9	241,7	286,9	316,3	422,9	467,7	548	724,3	3910,9	720,2
Italy	345	787,1	484,1	257,5	491,4	108,2	573,5	160,4	373,6	159,8

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Lithuania	0,6	0,4	0,5	0,6	0,8	0,8	0,7	1,2	0,7	3,8
Latvia	2,6	1,3	0	0	0	0	0	1,1	0	0
Luxembourg	93,8	134,1	109	276,3	177,1	123,1	146,5	201,5	178,2	181
Netherlands	0	0	238,3	885,7	505,3	600	531,5	809,4	2052,9	2121,4
Poland	206,4	64,1	153,8	147,3	143,3	151,2	177,8	354,2	174,5	181,6
Portugal	42,4	51,8	29,2	33,3	41	57,6	69,7	85,1	33,1	17,7
Slovak Republic	0	7,4	5,4	8,3	5,5	8,2	6,2	3,6	4,8	3,8
Slovenia	9,5	12,1	11,4	13,2	10,2	9,4	9,7	8,5	10,1	14,4
Sweden	626,7	1943,7	1996,8	1395,9	1544	1674,1	1685,5	1744,8	1627,7	1542,4
Total EU	**9115,7**	**14957,7**	**18855,8**	**14921,9**	**15662,7**	**11444**	**15068,6**	**10772,1**	**13547,9**	**15088,2**

Source: OECD

Of note however, is that the total numbers for the EU reached a peak of USD 18.9 billion in 2013, and in later years fluctuated between USD 10-15 billion. Starting from 2019, Korea's Services Trade Restrictiveness Index for digital services, published by the OECD was growing, indicating an increase in regulatory barriers. The overall index for digital services went up from 0.180731133 in 2018 to 0.202699021 in 2022 with the biggest increase observed in the component 'Other barriers affecting trade in digitally enabled services', which increased twofold from 0.021967886 in 2018 to 0.043935772 in 2022.[51]

3.2.4 EU-Korea trade in digitisable products

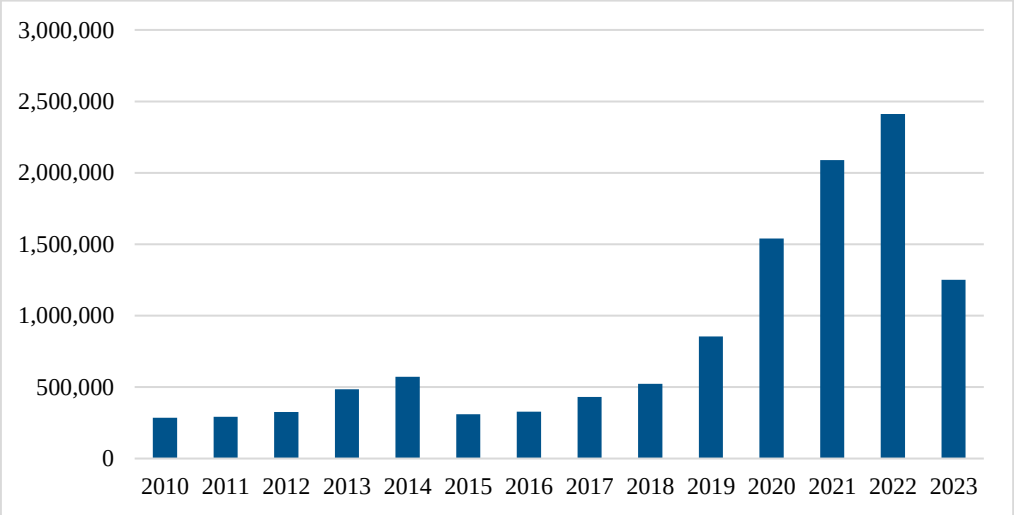
In a 2020 study by the WTO[52] there were 49 named digitisable products at the HS 6-digit level in four categories at the forefront of the technological transformation: photographic and cinematographic film; print matter; media for sound, video, software and video games. Consumption of these products has shifted increasingly from physical goods to digital equivalents, traded over the internet. For example, books, physical recordings of music and films, and games are being substituted by consumers for digital products provided through electronic transmissions.

EU-Korea bilateral trade in digitisable products has been growing steadily over the past decade reaching a maximum high of USD 2.4 billion in 2022 (Figure 3.5). In 2023 the numbers went down to USD 1.25 billion. While this is a very approximate measure of digitisable products, it still gives an idea of the trade volume that will be directly affected by the trade agreement. It is worth noting that those products are often in the cultural space - an area where the EU has always had a strong foothold.

[51] The OECD Going Digital Toolkit, based on the OECD Digital Services Trade Restrictiveness Index, https://qdd.oecd.org/subject.aspx?Subject=STRI_DIGITAL.

[52] World Trade Organization (WTO). 2020b. "Moratorium on Electronic Transmission: Economic and Tariff Revenue Effects." Geneva.

Figure 3.5 EU-Korea bilateral trade in digitisable products (USD thousand) (Source: KITA)



Note: HSK categories included: 9504; 8524; 8523; 4911; 4910; 4909; 4908; 4907; 4906; 4905; 4904; 4903; 4902; 4901; 4821; 3706; 3705.

3.3 General conclusions on the effect of digitalisation and digital trade agreements on economic growth

It is challenging to estimate the effect of the policy actions due to a limited amount of data on the general effects of such agreements. However, it is possible to estimate the impact of Digitalisation, assuming that the agreement will facilitate further Digitalisation of trade in goods and services between the EU and Korea.

Evidence from existing expert and academic research suggests a range of Digitalisation-associated benefits for trade and domestic economies.

- digitalisation promotes overall services tradability[53];
- trade growth in digitally deliverable business services has a positive impact on domestic value added embodied in exports[54];
- improved online protection for consumers increases trust in digital transactions;
- SMEs, which particularly benefit, now have access to an affordable entry point to digital commerce through trusted platforms;
- digitalisation and adoption of digital technologies induces more companies to become exporters.[55]

Data localisation requirements act as a drag on digital development and disproportionally affect SMEs. This has been articulated in a recent paper from the Centre for Information Policy Leadership (CIPL). In Asia-Pacific, which is tightly bound by well-developed regional value chains, full implementation of binding and non-binding WTO FTA measures, together with

[53] Benz, S., A. Jaax and Y. Yotov (2022), "Shedding light on the drivers of services tradability over two decades", OECD Trade Policy Papers, No. 264, OECD Publishing, Paris, https://doi.org/10.1787/d5f3c149-en

[54] Andrenelli, A. and J. López González (2019-11-13), "Electronic transmissions and international trade – shedding new light on the moratorium debate", OECD Trade Policy Papers, No. 233, OECD Publishing, Paris. http://dx.doi.org/10.1787/57b50a4b-en

[55] López-González, J. (2017), "Mapping the participation of ASEAN small- and medium- sized enterprises in global value chains", OECD Trade Policy Papers, No. 203, OECD Publishing, Paris, https://dx.doi.org/10.1787/2dc1751e-en.

other paperless and cross-border trade facilitation measures (digital trade facilitation) can result in cost reductions of more than 26%.[56]

In Asia-Pacific, the adoption of specific digital trade provisions was found to increase the flows of digitally ordered and digitally deliverable trade by between 11% and 44% in successive years.[57]

A 2023 study by the APEC Committee on Trade and Investment presents evidence that adoption of digital trade provisions increased the volume of digitally deliverable trade in the observed countries.

Digital trade provisions that came into force between 2000 and 2018 are estimated to have added USD 40.1 billion, or 2.9%, to the overall value of digitally deliverable trade between APEC economies in 2018.[58] The strongest effect was observed the year after provisions entered into force. The study also managed to capture that an increase in consumer trust and the adoption of provisions for cybersecurity had a statistically significant impact on digital trade.

Some findings also suggest that digital trade facilitation provisions in trade agreements significantly increase trade for high-income exporters, especially for services trade.[59] At the time of negotiating the United States-Mexico-Canada Agreement (USMCA), a report by the United States International Trade Commission found that including a digital trade chapter, along with provisions related to investment and e-commerce, would contribute significantly to the model's estimated 0.17 % increase in U.S. services sector output and 1.2 % increase in services exports to the world.[60]

Several studies have tested the impact of digital trade provisions on trade, concluding that the implementation of digital trade provisions tends to enhance digital trade, and particularly trade in services (Ma et al. 2023[61]; Suh and Roh 2023[62]; and Wu et al. 2023). The impact is stronger when deeper agreements are established between the parties.

Two other potential areas where positive effects could be achieved are trade in digitisable products' and exports of services with a digital component. Several studies identified 49 product lines under HS 6 digit that are being used to estimate the impact of digitalisation on trade in goods.[63] Section 9 of this study looks into available data on Korea-EU flows in these products for the purposes of better understanding digitalisation's impact on trade.

The most recent data derived from the OECD (presented above) confirm a significant rise in the EU's export of services with a digital component during 2010-2020. Considering that this period also saw an acceleration in the use of digital technologies across various industries, it is highly plausible that the growth was partly induced by digitalisation. The growth occurred despite existing barriers

[56] Duval, Y., Utoktham, C. and Kravchenko, A (2018). "Impact of implementation of digital trade facilitation on trade costs", ARTNeT Working Paper Series, No. 174, January 2018, Bangkok, ESCAP. http://artnet.unescap.org

[57] APEC Committee on Trade and Investment 2023. Economic Impact of Adopting Digital Trade Rules: Evidence from APEC Member Economies. APEC Project: CTI 05 2022S.

[58] APEC Secretariat (2023), Economic Impact of Adopting Digital Trade Rules: Evidence from APEC Member Economies.

[59] Peter R. Herman, Sarah Oliver (2023) Trade, policy, and economic development in the digital economy Journal of Development Economics 164 103135

[60] United States International Trade Commission U.S.-Mexico-Canada TradeAgreement: Likely Impact on the U.S. Economy and on Specific Industry Sectors April 2019 Publication Number: 4889 Investigation Number: TPA 105-003

[61] Ma, Shuzhong, Yuting Shen, and Chao Fang (2023). Can data flow provisions facilitate trade in goods and services?-Analysis based on the TAPED database. Journal of International Trade & Economic Development, pp. 1-26.

[62] Suh, Jeongmeen and Jaeyoun Roh (2023). The effects of digital trade policies on digital trade. The World Economy. Available at https://onlinelibrary.wiley.com/doi/10.1111/twec.13407

[63] Tibor Hanappi ; Adam Jakubik ; Michele Ruta. Fiscal Revenue Mobilization and Digitally Traded Products: Taxing at the Border or Behind It? September 7, 2023

to data flows and non-tariff barriers. Minimising of those will further stimulate export expansion, due to the digitalisation benefits identified by the studies mentioned above.

It should be noted that effects are not linear and may change, depending on the evolution of the technologies themselves and the depth of their adaptation by respective societies.

It has been observed that the nature of products and services, and the relationships between them, are changing. The McKinsey Global Institute[64] points out that the technology component of some goods can fundamentally affect the value of the good. The so-called “digital wrappers,” as digital add-ons, can enable or raise the value of other activities. Therefore, being able to incorporate products with high value-added digital components into trade will be part of the evolution of trade patterns.

[64] James Manyika, Susan Lund, Jacques Bughin, Jonathan Woetzel, Kalin Stamenov & Druv Dhingr, Digital Globalization: The New Era of Global Flows (2016)

Section 4. Overview of the EU and Korea's legal ICT/Digital framework

This section further examines the legal structure surrounding data, data partnerships, cross-border data requirements and cybersecurity in the EU and Korea. It starts with a brief overview of major regulations in the EU and then proceeds to Korea. To avoid repetition, this section should be read in conjunction with Section 7 on 'Technical standards, certification and compliance', and Section 8 on 'Cyber security', with respect to the various agencies that are legally responsible.

4.1 The EU legislation (2011-24) with a digital component and its impact on Korea's regulatory initiatives

The EU is a large market for digital products and its policy priority has been to promote its right to regulate to ensure citizens' consumer and digital rights. This has been most pronounced in the area of data privacy, where the EU updated its earlier privacy regime for personal data, with the stronger General Data Protection Regulation (GDPR). The EU has also been at the forefront of initiatives to curb anti-competitive practices of large technology companies, and EU Member States have been leading the charge on the introduction of digital services taxes at the point of consumption.

The EU has continued to issue landmark digital legislation since the EU - Korea FTA that came into effect in 2011. The table below presents major legislative acts passed by the EU, which form an important part of the negotiation process, as none of them can be compromised in the final agreement.

Table 4.1 the EU's regulations with a digital component

Name	Impact on EU-Korea FTA	Comments
EU Declaration on Digital Rights	Serves as a guiding principle for subsequent legislation, including the Digital Services Act, Digital Markets Act, Data Governance Act, and AI Act.	Not a legal norm but was recognised in the EU-Korea FTA - the EU's first trade agreement with environmental and labour components.[65] May be viewed as guidance for digital human rights in the EU – KOR Digital FTA.
General Data Protection Regulation[66] (GDPR)	Contains specific provisions for transfers of personal data to countries outside of the EEA.	Korea was granted GDPR adequacy by the EU in December 2021.
EU Network and Information Security Directive (NISD) 2016 and NIS 2 2022	Forms part of the EU cybersecurity policy; May be viewed as a modern series of cybersecurity controls, which manages risk and incident reporting	This is quite different to how cybersecurity is addressed in Korea.

[65] EU - European Union–South Korea Free Trade Agreement 2011

[66] EU - The General Data Protection Regulation 2016

Name	Impact on EU-Korea FTA	Comments
	across the European market under a single agency, working with all EU Member States to a common set of criteria against threats.	
The EU Cybersecurity Act[67]	Seeks to achieve a high common level of cybersecurity across the EU by giving support to national authorities and EU institutions, bodies, offices and agencies in improving cybersecurity.	Cybersecurity makes up a part of the EU-Korea Digital Partnership.
The EU Cyber Resilience Act[68]	Focuses on regulating cybersecurity for digital products and services through common standards, including mandatory incident reports and security updates for digital products. Sets stringent cybersecurity requirements for all products with digital elements their components, and other digital services that are offered in the EU market, with the objective of enhancing consumer protection and digital rights.	Cybersecurity makes up a part of the EU-Korea Digital Partnership.
The Digital Markets Act[69] (DMA)	Protects EU consumers by ensuring that they have more control over their data and can choose from a variety of services and platforms by putting restrictions in place on how user data is stored and used by the platforms.	Korea follows the EU in imposing stringent domestic regulation around consumer protection.
The Digital Services Act[70] (DSA)	Designed to regulate digital platforms and services, particularly those with significant societal impact, to protect users' fundamental rights and combat the spread of illegal content and disinformation.	Korea aligns with the EU on the right to regulate digital platforms.
Data Governance Act[71] (DGA)	Supports the European strategy for data[72]; Seeks to increase trust in data sharing, drive data-driven innovation, strengthen mechanisms to increase data availability, and overcome technical obstacles to the reuse of data.	There is no comparable equivalent legislation in Korea.

[67] EU - Cybersecurity Act 2019
[68] EU - Cyber Resilience Act 2022
[69] EU - Digital Markets Act 2022
[70] EU - Digital Services Act 2022
[71] EU - Digital Governance Act 2022
[72] EU - European strategy for data

Name	Impact on EU-Korea FTA	Comments
The EU Artificial Intelligence Act (EU AI Act)[73]	The first of its kind in the world, and may set a global standard for AI regulation; Incorporates guidelines on data, AI and judicial use issued in 2018 and early 2019[74], as well as 'Ethics Guidelines for Trustworthy AI.'	Korea's AI Act shares many of the elements of the EU AI Act, in particular for high-risk models.[75]
The EU Common Criteria-based cybersecurity certification scheme (EUCC)	Coalesces a set of existing rules with the objective of ensuring a high level of cybersecurity for ICT products, services, and processes in the European market by setting common rules, technical requirements, and evaluation procedures.	
European Digital Identity[76] (EDI)	Aims to provide a secure, easy-to-use, user-controlled means of identification and authentication, ensuring that citizens have control over their personal data and can access various services seamlessly.	Korea has MyData which performs similar functions to the proposed EDUA. However, this is built on closed standards as opposed to open standards, which are mandated under the EU.

4.2 Korea's major digital laws

Laws discussed further in this section are summarised in table 4.2 below.

Table 4.2 Korea's major laws governing digital trade issues

Name of legislative act	Entry into force year/ amended	Comments
'Personal Information Protection Act' (PIPA) 2011	2020, 2023	Brings Korea into line with GDPR adequacy. It has: (i) integrated the previously binary regulations on data controllers and online service providers; (ii) introduced new data subject rights, including the right to request transmission of personal information and the right to object to automated decision-making; (iii) shifted the focus of sanctions to fines; (iv) established regulations on the operation of mobile visual data processing devices; (v) introduced more grounds for transferring personal information overseas

[73] EU - AI Act becomes Law 2024

[74] European Commission For The Efficiency Of Justice (CEPEJ)

[75] Korea: an overview of AI bills

[76] EU – Proposal for a framework for a European Digital Identity

Name of legislative act	Entry into force year/ amended	Comments
		and the right to order the suspension of overseas transfer of personal information; and (vi) expanded the bases for processing personal information other than consent.
'Use and Protection of Credit Information Act' (UPCIA) 2013	2020, 2023	
Act on the Establishment, Management, etc. of Spatial Data		Prohibits mapping data from being stored outside the country
Network Act 2001	2014, 2016	
Act on Promotion of Cloud Computing and Protection of Users	2022	Prohibits cloud computing service providers from disclosing user information to third parties without consent
Cloud Security Assurance Programme (CSAP)	2023	Based on international standards like ISOIEC 27001, with additional requirements. Provides the basis for the Personal Information and Information Security Management System (ISMS-P).
Act on the 'Consumer Protection in Electronic Commerce (e-Commerce Act', (Act. 17799,)	2021	Polices the internet platforms and guards against monopolies
Digital Signature Act/Electronic Signature Act (Act No. 5792)	2020 2022	Allows authorised organisations to issue private identifiers using mobile phone number for verification.
At on the Promotion of Information and Communications Network Utilisation and Information Protection	2016	Provides legal background for the Korea Information Security Management System (K-ISMS).
'Infrastructure Protection Act No. 18871	2022	
Financial Investment Services and Capital Markets Act (Act No. 19263)	2023	
The Electronic Financial Transaction Act (Act No. 17354)	2020	Stipulates that financial companies or electronic financial business operators' systems for processing (i) unique identification information or (ii) personal credit information cannot be located outside of Korea in the course of using cloud computing services.[77] Major regulation that mandates network separation for financial institutions.
Act on the Promotion of AI Industry and Framework for Establishing Trustworthy AI" (the "AI Act")	Proposed to the National Assembly in 2022	Unlike the EU's AI Act, it is based on the principle of "adopting technology first and regulating later", aiming to support the development and industrial activation of AI technologies.

[77] Data Protection and Privacy 2024. Korea.

Name of legislative act	Entry into force year/ amended	Comments
Unfair Competition Prevention and Trade Secret Protection Act	Last amended up to Act No. 19289 of 28 March 2023	Amendments address issues around data use and AI-generated content.
Telecommunications Business Act		Prevents app store operators with dominant positions from forcing payment systems on app developers and 'inappropriately' delaying app reviews or blocks. The law also gave the Korean government the power to mediate disputes regarding payment, cancellations and refunds in the app market
Medical Services Act		Prohibits storing Electronic Medical Records (EMR) outside of Korea. According to PIPA, personal information controllers may process pseudonymised medical information without the consent of data subjects for the purposes of statistics, scientific research and archiving in the public interest.

Korean laws related to ICT were developed primarily to be inwardly focus on internal security. Korea's data-related legal frameworks include the 1995 Act on Informatisation - the first legal foundation for data in Korea. There were also a number of complimentary acts, including Act 14080 on the Promotion of Information and Communications Network Utilisation and Information Protection[78], and the Infrastructure Protection Act and the Public Agency Data Protection Act, which also addresses cybersecurity.

The primary law governing data protection in Korea is the Personal Information Protection Act 2023 (PIPA Act No. 19234). Originally passed on 30 September 2011, it was substantially updated as Act No. 16930 on 4 February 2020[79] to bring it into compliance for adequacy under the EU GDPR. Further extensive updates were promulgated in February 2023 to develop adequacy, and although the two systems still have many differences, they have 'the same DNA'[80].

Another important piece of legislation, 'the Use and Protection of Credit Information Act' (UPCIA) 2013 was amended in 2020 and 2023.[81] These amendments were quite significant in removing overlaps with the GDPR amendments to the PIPA.

The Act on the 'Promotion of Information and Communications Network Utilization and Information Protection, the Network Act 2001 as amended 2016 and the 2014, 'Act on the Establishment, Management, Etc. of Spatial Data', prohibits mapping data from being stored outside the country.

[78] Korean Act on Real Name Financial Transactions and Guarantee of Secrecy

[79] Korean Personal Information Protection Act

[80] Detailed explanations of 2023 are given in: Korea passes extensive amendments to data privacy law.

[81] Korea CREDIT INFORMATION USE AND PROTECTION ACT

Korea is the only advanced country in the world that maintains data localisation requirements specifically for mapping data. This is one of the reasons why certain international services (such as Google Maps or Find my iPhone or iPad) either do not work in Korea or have limited application.

Korea has defended its prohibitions on data mapping as it wants to limit the availability of high-resolution commercial satellite imagery of Korea for national security reasons.[82]

4.3 Korean cloud laws and regulations

The first set of laws covering cloud computing in Korea was the 2015 Act on Promotion of Cloud Computing and Protection of Users. This has since been updated several times in 2018[83] and 2022[84]. This is in part, to enable Korea's Third Master Plan for Cloud Computing, which was issued by the MST in 2019. The act also contains provision to certify cloud service provider under the CSAP[85] created by KISA in 2016.

The most recent plan for cloud incorporates goals to promote the use of commercial cloud services in the public sector, stating that by 2025 cloud will be the basis of all information systems of national, local and public institutions. The act expands the CSAP[86] from guidance to a legal requirement.

The legal background for the K-ISMS is provided in Article 47 of the Act on the Promotion of Information and Communication Network Utilisation and Information Protection (Certification of ISMS)[87].

In late 2018, the CSAP was updated with the issuance of the ISMS-P. This is based on international standards, including ISOIEC 27001, but has additional requirements when compared to a general ISO/IEC 27001 security assessment.

Certification is valid for three years, and certified entities must pass an annual audit to maintain it. The law is currently being reviewed[88], and changes being contemplated include revising cybersecurity policies for data classification in the cloud.[89]

Korea classifies public data into three categories, and only the lowest level may be hosted in the cloud.[90] However, the moving of public data into the cloud has been slow and regulations unclear. Since January 2023, cloud service providers must locate cloud computing systems within Korea to comply with the CSAP if they provide services to 'public institutions.

[82] Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?

[83] Korea - The Cloud Act as amended 2018.

[84] Korea - The Cloud Act as amended 2022.

[85] Korea CSAP

[86] Korea CSAP

[87] Korea Article 47

[88] Korean Government Announces Cloud Computing Promotion Plan, Repealing the "Information Classification System"

[89] The Readable. Korea revises cybersecurity regulations: Satellite, cloud included

[90] The 2015 and 2018 system retained 3 categories of data of which only the lowest form could be handled by private organizations. / Korean Government Announces Cloud Computing Promotion Plan, Repealing the "Information Classification System".

This data localisation obligation extends to associated data, backup systems and personnel.[91] The amended Cloud Computing Act prohibits cloud computing service providers from disclosing user information to third parties without consent.[92]

Furthermore, it empowers the Ministry of Science and ICT (MSIT) to evaluate compliance with the cloud computing standards and provide security certification.[93]

4.4 Korean digital ecosystem laws and regulations

Korea has a well-developed digital economy, overseen primarily by Korea Fair Trade Commission (KFTC), its competition watchdog covering non-financial institutions. Consumer protection is covered by the 2021 Act on Consumer Protection in Electronic Commerce (e-Commerce Act, Act. 17799).[94] The KFTC also polices the internet platforms and guards against monopolies with a new Platform Act strengthening its powers.

Complimentary to the above laws and cloud, a number of specific pieces of legislation have been passed since 2016 to foster growth in e-commerce and the digital economy. These have focused on enhancing or clarifying the laws on e-commerce/e-transactions, identity and authentication, online trade documentation, and e-invoicing, underpinned by a secure digital ID system that enables individuals and corporations in Korea to access e-services and paperless trade with digital authentication and verification.

In June 2022, the 2020 Digital Signature Act (Act No. 5792)[95] was amended by the MSIT as the 'Electronic Signature Act' to allow authorised organisations to issue private identifiers using a mobile phone number for verification.

Early e-commerce transactions were legally covered by the Act on the 'Promotion of Information and Communications Network Utilisation and Information Protection[96], and the 'Infrastructure Protection Act, updated as Act No. 18871 in 2022[97]. KISA maintains an up-to-date summary of digital laws.[98]

Intermediary liability is covered specifically in Article 44-2 of the revised Consumer Protection Act, that generally limits service providers to takedown notices, without having to admit liability or pay compensation. This has been challenged on censorship grounds, particularly when it relates to content on political figures.[99]

4.5 Korean data laws and regulations

[91] Tommaso Giardini, Maria Buza DPA Digital Digest: Republic of Korea. 25 Apr. 2023.

[92] Korea – consent ruling

[93] Korea - security certification

[94] Korea E-Commerce Act.

[95] Korea Digital Signature Act 2020.

[96] Korean Act on Real Name Financial Transactions and Guarantee of Secrecy,

[97] Korean Network Act.

[98] Korea KISA Laws.

[99] More on Network act, Article 44-2 and censorship questions can be found here: Intermediary liability: Not Just Backward but Going Back.

As previously stated, there are plethora of laws that have evolved to cover the protection of personal data. The movement of data, in particular commercial data across borders has been a challenge for a number of economies, Korea is no exception.

In Korea, the legal basis for data transfers, including cross-border, relied primarily on prior consent, and until 2023, Korea data privacy law lacked the flexible alternative mechanisms available in other advanced jurisdictions. Many modern data protection laws acknowledge that the legal basis for processing personal data is transaction specific, and should be determined with reference to various considerations, including the type of transaction, the relationship between the parties, and other material issues.

The 2023 amendments to the PIPA have gone some way to address this but still do not specify standard contractual clauses nor binding rules as the basis for cross-border transfers without consent.

From September 2023 the amended PIPA allows cross-border data transfers if either 1) the recipient country has a level of data protection similar to Korea 's, 2) the recipient country has an international data transfer agreement with Korea, 3) the transfer fulfils a contract with the data subject that discloses storage details, or 4) the recipient organisation is certified by the Personal Information Protection Commission (PIPC).[100]

On the international level, in April 2022, Korea joined the Asia-Pacific Economic Cooperation's (APEC) Cross-Border Privacy Rules (CBPR) system together with Canada, Japan, the Philippines, Singapore, Chinese Taipei, and the US. The CBPR system centres around a voluntary privacy code of conduct for participating member economy businesses that are operating in the APEC region based on the nine APEC Privacy Principles developed in the APEC Privacy Framework: preventing harm, notice, collection limitation, use, choice, integrity, security safeguards, access and correction, and accountability.[101]

In addition, Korea has received data privacy adequacy decisions from the European Union and the United Kingdom.

4.6 Korean finance laws and regulations

As noted above, these acts do not cover financial companies, securities or banking transactions online, which are covered by the 2023 Financial Investment Services and Capital Markets Act (Act No. 19263)[102].

All financial institutions are required to abide by Korea's Electronic Financial Services Act, and are governed by the Financial Service Commission (FSC). The Financial Supervisory Service (FSS)[103] is Korea's integrated financial regulator, which examines and supervises financial institutions under the broad oversight of the FSC.

The FSS is the compliance agency, which legally sits under FSC but is virtually independent. The Bank of Korea, FSC and FSS all report independently to the Bank for International Settlements, for example[104]. The FSS website provides an overview of its activities[105].

[100] Ibid.

[101] Korea joins APEC cross-border privacy rules system

[102] South Korea – Financial Investment Services and Capital Markets Act.

[103] South Korea – Financial Supervisory Service.

[104] Official website of the Financial Supervisory Service in Korean.

[105] Ibid. (as is common in South Korea, the English website looks nothing like the Korean website).

The Electronic Financial Transaction Act (Act No. 17354, 2020) was first enacted in 2006 and updated in 2020[106]. The act addresses new financial models, such as Buy Now, Pay Later, as well as introducing protections for consumers' funds held on deposit[107].

Any business licence-holders engaging in online commerce involving a payment – from the smallest micro-SME to the largest chaebol – are subject to a set of limitations on their digital financial business accounts, which are policed by the banks under regulations written and unwritten by the FSS[108].

The Electronic Financial Transaction Act (Act No. 17354) requires all financial institutions to separate all financial transaction data into a private network with robust security measures within Korean territory. In principle, this prohibits any transfer of domestic financial transaction data overseas.

However, this controversial practice of network separation for financial institutions might undergo a considerable overhaul in the coming months, as the FSC is seeking to upgrade the rules on financial data security. It plans to ease the relevant regulations gradually, in stages, through a sandbox program, with the aim of balancing innovation and security appropriately. The FSC also plans to revise the supervisory regulation on electronic financial services until the end of 2024, to facilitate financial companies' research and development projects.

On 22 January 2024, the FSC held a meeting with foreign financial institutions, and pledged to create a favourable environment through regulatory improvements that are more in line with global standards[109].

4.7 Korean artificial intelligence laws and regulations

In 2023, the Korean National Assembly's Science, ICT, Broadcasting and Communications Committee passed a proposed Act on the Promotion of AI Industry and Framework for Establishing Trustworthy AI (AI Act)[110].

If passed into law, the AI Act would be the first comprehensive law to govern and regulate the AI industry in Korea. The act aims not only to support the AI industry and technology, but also to protect users of AI-based services by ensuring the trustworthiness of AI systems. Similar to the EU AI Act, it includes provisions for:

- requiring high-risk AI to meet certain trustworthiness standards;
- providing support for innovative AI businesses;
- establishing ethical guidelines for AI;
- creating a Basic Plan for AI and an AI Committee to oversee AI development.

However, the passage of the AI Act has faced some opposition from civil society groups, who argue that the bill lacks proper regulatory framework and does not adequately address risks to human rights and safety. The act therefore has not yet passed into law.

[106] Korea Electronic Financial Services Act: https://www.fsc.go.kr/eng/pr010101/22471.

[107] Korea Joongang Daily. 2022. Buy now, pay later gains ground in Korea as marketing tool.

[108] When questioned about some regulations, bank officers merely say it is required by FSS and cannot cite a law or published regulation.

[109] AI companies: Uphold Your Privacy and Confidentiality Commitments US FTC Comment.

[110] South Korea – the AI Act proposed in 2023.

Korea has also introduced other related legislation, such as amendments to the PIPA and Unfair Competition Prevention Act, to address issues around data use and AI-generated content, in particular for elections[111].

Korea has also issued National Guidelines for AI Ethics[112], which follow the OECD AI Principles. The MSIT issued the first National Strategy for AI in 2019 – a policy document outlining a vison for AI in Korea, which was substantially updated in 2023[113]. Section 7.5.3 of this report outlines AI and ethical considerations for AI in Korea.

A table in Annex 2 A 2.1 shows the steps taken to formulate the act in its current form.

4.8 Korea digital platform regulation

4.8.1 App store legislation

In August 2021, Korea became the first country to enact legislation on app stores, which primarily addresses unfair competition issues regarding in-app payment. The bill that amended the Telecommunications Business Act aimed to prevent app store operators with dominant positions from forcing payment systems on app developers, and 'inappropriately' delaying app reviews or blocks. The law also gave the Korean government the power to mediate disputes regarding payment, cancellations and refunds in the app market[114].

The app store regulation primarily targeted the dominant position of Apple and Google, but did not achieve the desired effect. According to the Korea Communications Commission, the two tech giants abused market dominance to force local app developers to use their in-app payment methods rather than competitors' payment systems, and unfairly delayed app reviews to enforce the specific billing system.

In October 2023, the Korea Communications Commission warned Google and Apple of potential fines totalling up to USD 50.5 million, alleging enforcement of certain payment methods by Google and Apple, and 'discriminatory charging of fees to domestic app developers' by Apple.

Beyond app markets, there is ongoing broader discussion about whether it is necessary to introduce a separate *ex ante* competition legislation for digital platforms, similar to the EU DMA.

In 2023, as the DMA was entering the implementation stage, the KFTC revived its efforts to introduce *ex ante* regulation concerning digital platforms through the Online Platform Act. Specifically, the KFTC established the Online Platform Regulatory Improvement Task Force, while adopting the Guidelines for Review of Abuse of Market Dominance by Online Platform Operators (the Online Platform Review Guidelines), which took effect on 12 January 2023.

However, it faced criticism that the regulation is 'excessive' as a regulatory measure, and represents reverse discrimination against Korean digital platforms. The National Economic Advisory Council – an advisory body directly under the president – communicated these concerns to the presidential office through its Annual Report in October 2023.

The KFTC has to decide whether Korea's *ex ante* regulation of digital platforms would be modelled on the EU's DMA or Germany's 10th amendments to its competition law *Gesellschaft für Wirtschaftsbestimmung* (GWB 10). This choice was previously deliberated by the platform taskforce, and it was reported that the taskforce was leaning towards GWB-10-style

[111] South Korea – AI legislative update 2024.

[112] South Korea – The National Guidelines for AI Ethics.

[113] South Korea – MSICT AI Policy 2023.

[114] South Korea passes bill limiting Apple and Google control over app store payments.

regulation[115]. However, there are major concerns regarding over-regulation and stifling of competition.

On 14 November 2023, a partial amendment to the Telecommunications Business Act was announced. The amendment aimed to establish and spread a legal basis for platform self-regulation to respond quickly and actively to the needs of platform users.

The amendments allow digital platforms to conduct activities – such as creating a balanced trading environment, promoting innovation, protecting users and promoting cooperation – through private-platform self-regulatory organisations, or self-regulation by digital platforms themselves. The amendments also focus on the government's support for such self-regulatory activities.

The government has been discussing how to handle digital platform matters at the Pan-government Platform Policy Council, which involves all relevant ministries, including the Ministry of Economy and Finance, KFTC, MSICT and Korea Communications Commission.

In February 2024, the KFTC announced a proposal called the Platform Competition Promotion Act, aimed at regulating the dominant online and mobile platform players. If passed, it will likely target domestic companies, such as Naver and Kakao, as well as global corporations, including Google, Apple and Meta. Opinions on the Korean Platform Act are sharply divided domestically (not just among big firms, but startups too) and abroad.

The American Chamber of Commerce in Korea released a statement expressing concerns about Korea rushing passage of the act[116]. But the KFTC strongly believes that the act is essential to combat monopolisation in the platform market, which tends to grow and become entrenched rapidly.

[115] Recent developments in South Korea's digital platform regulations.

[116] South Korea speeds up to regulate platform giants such as Google or Apple; KFTC vows to push for controversial platform act despite growing criticism.

Section 5. Korea ICT infrastructure

5.1 4G, 5G and 6G, internet service providers, cables and DTS satellite proposals

5.1.1 Korea's 5G and 6G development plans

Korea started 4G service in 2011 and continued to work on 5G. Standardisation for 5G was completed in 2012, and relevant research and development started in 2013. It was the first country in the world to roll out the 5G service, in 2019. As of December 2023, 48 sites in Korea have built private 5G networks, including companies such as LG Electronics, Samsung Electronics, Naver Cloud and Hyundai Motor[117].

Currently the country is actively preparing to launch 6G by 2028 – two years earlier than originally planned under the K-Network 2030 programme.

In November 2023, the MSIT unveiled its KRW 440.4 billion (USD 324.5 million) research and development plan for future 6G networks. And in July 2024, it announced the launch of the '6G Society'. This initiative should be seen as a standardisation project, as it aims to promote communication and interchange between the satellite communication and 6G mobile communication fields[118].

Korea is a major world holder of 5G technology patents, accounting for 25.9% of 5G patents, while China holds 26.8%[119]. The government aims to raise Korea's share to 30% with 6G patents. Korean 6G technologies were selected by the International Telecommunications Union (ITU) as global-standard candidates, signalling the high intensity of Korean efforts to win the race. Korea had proposed four 6G frequency ranges and three of them were selected as global-standard candidates: 4.4-4.8 gigahertz (GHz); 7.125-8.5 GHz; and 14.8-15.35 GHz[120].

To promote global collaborative networks, Korea conducted joint studies on core 6G technologies and 6G spectrum with the US (2021-2025, 11 studies, KRW 9.8 billion budget); China (2021-2023, 1 study, KRW 3.3 billion); and Finland (2020-2024, 2 studies, KRW 3.5 billion), and collaborates with the US and European countries on technologies for 6G.

5.1.2 Internet service providers (ISPs)

In 2023, about 40.8% of high-speed internet users in Korea used internet services provided by KT Corporation. KT Corporation, SK broadband, LG U+ and other system operators such as CJ HelloVision and t-broad are the main telecommunication companies that provide high-speed internet services in Korea.

Korea has a 'sender-pays' model, in which ISPs must pay for traffic they send to other ISPs, breaking the worldwide norm of 'settlement-free peering' – voluntary arrangements whereby ISPs exchange traffic without cost.

---

[117] Private 5G in Korea 2023

[118] '6G Society' will promote communication and interchange between the satellite communication field and the 6G mobile communication field

[119] S. Korea plans to launch 6G network service in 2028

[120] Korea's 6G frequency bands picked as standard candidates

It started in 2016, when the Ministry of Science, ICT and Future Planning (predecessor of the MSIT) began enforcing the revised Interconnection Standards for Telecommunication Facilities, requiring ISPs to charge for the traffic that they receive from each other.

The sender-pays model is attractive, because stakeholders such as governments and telecommunications operators would like internet giants such as Facebook, Google and Netflix to pay for telecommunications infrastructure.

The sender-pays policy was reinforced in 2020, when the country's National Assembly amended the Telecommunications Business Act to require video-sharing platforms – specifically, content providers that meet certain thresholds – to take measures to ensure that their services remain stable in the country. These include securing enough server capacity, ensuring an uninterrupted internet connection, and notifying ISPs before they change their traffic routes.

A number of bills introduced since 2021 seek to mandate local and foreign content providers to enter into contracts with ISPs in Korea to be able to use their networks. A contract would need to specify the ISP's usage fees, period of use and available capacity, among other terms[121].

With Korea's sender-pays interconnection rules, it is very costly to operate data-intensive services in

Korea. These rules strongly encourage ISPs not to host popular content. So, although there are no official rules that content providers must pay network fees, there are unofficial mechanisms that encourage deal-making. Streaming site Twitch pulled out of

Korea in February 2024, with its CEO saying it was 'prohibitively expensive' to operate there[122].

5.1.3 Undersea cables

Korea is almost wholly dependent on its undersea communications cable infrastructure for international communications. As of 2019,

Korea had nine undersea communications cables in operation, and one cable in the survey phase of the project. Nevertheless, as the EAC-C2C cable has segments landing at Taean and Busan, Korea has 11 onshore cable landings.

To accommodate these 11 landings, there are four cable landing stations: two in Busan on the southeast coast, one on the southern island of Keoje, and one in Taean on the west coast. Importantly, every cable landing in Korea also lands in either Japan or Taiwan, and all cables but one – the Korea-Japan Cable Network – land in China (see map below).

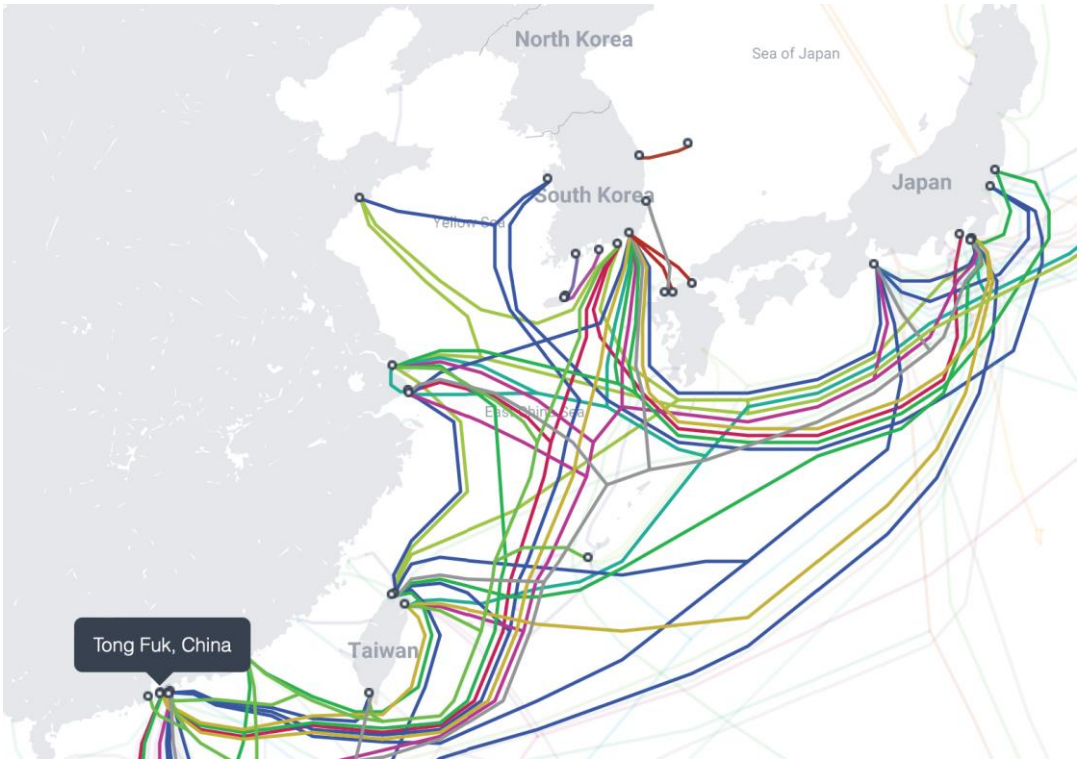
Korea invested USD 700 billion between 2008 and 2023 to build its undersea cable infrastructure, led by LS Cable & System – its largest cable company. In August 2023, LS Cable announced it would invest USD 117.5 million in manufacturing undersea cables to meet the increased market demand for cables carrying data for email, bank transfers, etc. across the seas. Even during the COVID-19 pandemic, LS Cable signed contracts for undersea cables with the Netherlands, the US, Singapore and Bahrain[123].

[121] South Korea Interconnection Rules.

[122] When Regulation Encourages ISPs to Hack Their Customers.

[123] South Korea: A Catalyst for Fixing Laws on Undersea Cables.

Figure 5.1 Map of Korea's undersea cables



Source: Submarine consultancy

From a national security perspective, the transnational nature of the undersea-cable physical infrastructure, and the far-reaching effects of any communications disruptions, must be a concern. Broadband subscriptions, high export volumes and foreign bank claims together indicate that the country does tens of billions of dollars' worth of financial transactions per day via undersea communications cable infrastructure – in addition to data and voice traffic that is not financial in nature. This means that Korea's social and economic fabric is vulnerable to disruption if the state's cables are compromised[124].

The top three Korean ISPs are major players in the country's content space: in 2022, they collectively controlled an 86% market share in the Korean pay TV market.

5.2 Network charges and fees and their impact on market conditions and competition

Recent years have seen some debate over the low network usage fees paid in Korea by global IT firms, such as Google and Facebook, compared to what they pay in other countries (e.g. in the EU). This resulted in proposed regulations aimed at correcting the situation. These proposals have been consolidated into the seventh piece of legislation on this matter – the Netflix Free-Ride Prevention Act – introduced by Rep. Young-chan Yoon on 8 September 2022.

The legislation effectively mandates local and foreign content access providers to enter into contracts with ISPs in Korea to be able to use their networks. A contract would need to specify the ISP's usage fees, period of use and available capacity, among other terms.

[124] Assessing Threats to South Korea's Undersea Communications Cable Infrastructure.

One bill[125] in particular instructs ISPs to calculate network usage fees based on: (a) capacity and usage period; (b) the content provider's size, based on its subscriber base or market share; (c) a discounted wholesale rate; or (d) the agreed method of calculation in the existing contract.

Another bill[126] prohibits content providers from using an ISP's network without paying 'fair consideration' for use of the network, whereby the non-complying content provider's service can be shut down by the authorities. This bill implicitly allows ISPs to refuse to carry traffic from content providers who fail to pay the 'network usage fees'.

The Sending Party Network Pays model resulted in higher costs for interconnectedness in Korea. The cost of transit in Seoul is typically 8–10 times that of major European network hubs like London and Frankfurt. Elsewhere in Asia, technological improvements in optical fibre network technology and vigorous competition are leading the cost of transit to fall by about 20% a year.

The prices demanded by Korean ISPs for delivering traffic make it impossible for new online services and applications to be created, homegrown and developed successfully in the country. Also, the Sending Party Network Pays model has increased the fragility of the Korean interconnectedness system by incentivising peering abroad. Only about 1.3% of

Korean traffic is exchanged locally, which is a small fraction compared to the domestic traffic exchange in other developed countries. A large portion of Korea's domestic traffic – at least 17% – is exchanged abroad. Korea's ISPs exchange traffic with each other in Japan and Hong Kong, as a result of the structure of its undersea cables (discussed above). Peering abroad creates both increased latency for Korean end-users, as well as an incredibly fragile network architecture.

5.3 Challenges for digital trade within Korea

Korea's policy on digital trade aims to secure both 'digital sovereignty' and the right to regulate. This results in a range of practices that has raised objections, in particular in the US.[127]

Korea has imposed several requirements that effectively restrict companies from exporting geolocation data, leaving international firms providing mapping and other location-based internet-enabled services at a significant competitive disadvantage. Another concern is the provision of cloud services for the public sector. Current regulation makes compliance for foreign firms technically challenging and favours local firms, effectively closing the market to foreign service providers.

The requirements included: physical isolation of cloud facilities for government workloads; Korea-specific security certifications and encryption algorithms that preclude the use of internationally standardised solutions; and personnel and resource localisation requirements. The NIS guidelines introduce stricter cybersecurity requirements than the CSAP guidelines, as well as other cybersecurity validation programmes that impact the CSAP, including requiring that cloud facilities, equipment and personnel be under the exclusive legal jurisdiction of Korea.

The amended PIPA grants the Personal Information Protection Commission the authority to order the suspension of cross-border transfer of personal data, based on a generalised risk of breaching privacy protections, without any evidence of specific violations.

On 14 February 2023, the National Assembly's Science, ICT, Broadcasting and Communications Committee advanced the Law on Nurturing the AI Industry and Establishing

[125] ICT laws.

[126] ICT laws.

[127] US industry views on Digital trade in Kore: Korea

a Trust Basis, after 12 different bills related to AI were introduced in the previous three years. While the bill does not discriminate based on nationality or size, it includes increased and unclear obligations on AI systems that are determined to be 'high risk', including methods for detailing how an AI system reaches its final decision.

In late 2022, in response to a fire at a major data centre, the National Assembly passed amendments to the Broadcasting Communications Development Act, the Telecommunications Business Act, and the Act on the Promotion of Information and Communications Network Utilisation and Information Protection (the Network Act) to improve the resilience of data centres.

The legislation entered into force on 3 July 2023. This law includes extensive requirements for data related to data-centre security that could jeopardise companies' cybersecurity and non-disclosure agreements, and make sensitive data related to infrastructure, security and commercially sensitive trade secrets vulnerable to exposure.

While there is no general legal prohibition on exporting location-based data, it does require a licence. To date, Korea has never approved a licence to export cartographic or other location-based data, despite numerous applications by foreign suppliers[128].

In October 2021, Korea's National Assembly introduced several bills to strengthen local agent requirements for foreign ICT firms operating in the country. The bills seek to designate the Korean offices of foreign ICT firms as the local agents representing their headquarters.

Foreign firms generally prefer to set up limited liability companies to avoid Korea's criminal liability laws, which hold CEOs personally liable for all actions of their company and associated infractions.

The Korean government is preparing further regulation, with a bill for a Partial Amendment to the Telecommunications Act currently pending in the National Assembly. This amendment expands the scope of prohibited acts to include adding unfair or discriminative restrictions to network usage or provision agreements.

It also grants the Korea Communications Commission the authority to conduct factual surveys to assess the current status of network provision or usage, and to help establish fair competition in network usage and provision[129].

[128] National Trade Estimate Report.

[129] Network usage fees, consumer protection from foreign online platforms.

Section 6. Technical standards, certification and compliance

Accelerating the technical harmonisation of standards and certification is discussed in the Digital Partnership between the EU and Korea, which provides a framework for advanced cooperation on the full spectrum of digital issues. From a digital trade perspective, issues to be addressed include technical standards to enable interoperability, data transfers and regulatory harmonisation that are not hindered by unique domestic technical standards in Korea that inhibit trade between the country and the EU. This would reduce the cost of compliance, creating additional value for both software and hardware manufacturers in Europe and Korea.

In general terms, interoperability describes the capability of two or more hardware devices or software routines to work together. With regard to software specifically, interoperability is a feature, in the same way that functionality, ease of use, security and reliability are features.

To enable interoperability, data management may be principle-driven, interoperable by design (using international standards) and implemented by government, in order to lead with policies that are regularly reviewed based on technological advances and innovation (including regulatory interoperability).

UNCITRAL has established standards for the interoperability of trade by providing legal certainty in international commercial transactions, through the creation and dissemination of international trade standards.

UNCITRAL's Regional Centre for Asia and the Pacific of is in Korea[130]. However, it appears disconnected from the United Nations Network of Experts for Paperless Trade and Transport in Asia and the Pacific (UNNExT)[131], which is driving the implementation of electronic trade and paperless transport systems to facilitate trade.

UNNExT has an expert Advisory Committee, with representatives from countries including Japan, China, India and Singapore. However, Korea does not have an advisor on the board, and is seen as being behind Singapore in this respect[132].

6.1 EU-Korean ICT technical standards – how do they compare?

The EU has long recognised a need to build upon common ICT technical standards. At a practical level, from discussions with EU companies operating in Korea, it seems that some ICT standards in the country create barriers to EU companies doing business there.

For example, it appears to be possible to send Korean-sourced data overseas legally. However, it is the understanding of the European Chamber of Commerce in Korea and others in the market that, without using a Korean cloud, a foreign company cannot obtain a certificate of compliance with the CSAP for their Korean operations. This adds to their costs of doing business.

Encryption is a key pillar of the CSAP. Korea has developed its own encryption algorithm: ARIA KS X 1213:2004. The standard in common use internationally is the Advanced Encryption

[130] UNCITRAL Regional Centre for Asia and the Pacific.
[131] Aligned Trade Forms.
[132] Commission Staff Working Document, p.12.

Standard (AES) algorithm to ISO/IEC 29167-10:2015. Harmonisation with the international standard would enhance interoperability (see Annex 3 A 3.1.).

The NIS requires cloud service providers (such as Microsoft and Amazon Web Services) to use ARIA mandatorily to obtain CSAP. Although ARIA – a cipher derived from the more widespread AES cipher – has been standardised in the Internet Engineering Task Force, its use is virtually non-existent outside of Korea. By contrast, manufacturers, software developers and governments around the world have increasingly adopted the de facto global standard, AES (a cipher originally developed in Belgium, and adopted in the US only after a rigorous competition between competing ciphers)[133].

Microsoft and Amazon Web Services use AES, which is the global standard. The issue of CSAP must be resolved to ensure that there is: a clear understanding of any remaining restrictions on data that can be transferred freely from the cloud in Korea to authorised clouds in Europe; and essential interchange, possibly through the facilitation of sharing arrangements.

This appears to come down to differing cybersecurity standards, which have yet to be defined. However, a paper by Hangoo Jeon and others recommended the adoption of ISO standards as the basis for cloud security[134]. Cybersecurity is discussed in more detailed in a separate section below.

The net effect of this is that foreign cloud providers will be unable to comply with the mandatory CSAP without creating a separate product, unique to Korea, that meets the requirements for: physically segregated facilities for government customers; in-country backup systems; and operations and management personnel located within the territory of Korea. This may be considered data localisation, which is prohibited in most DTAs. The US-Korea Business Council recently sent a letter to the MSIT outlining the above as possible NBTs[135].

Korea plans to promote the use of commercial cloud services in the public sector, stating that cloud will be the basis of all the information systems of national, local and public institutions by 2025. The act expands the CSAP from guidance to a legal requirement.

6.2 Certification regulations for technology and compliance

The technical harmonisation of standards reduces the cost of certification compliance for ICT hardware manufacturers and service suppliers exporting from Europe to Korea, and vice versa.

A number of issues with the recognition of CC certifications issued outside of Korea were raised in a 2018 Business Software Alliance Cloud Survey[136]. The report stated that some ICT products that have already passed international Common Criteria Recognition Arrangement (CCRA) are required to undergo additional local testing in Korea.

Additional testing for high-security applications (e.g. in defence or intelligence gathering) is not unusual. However, interviews with EU businesses operating in Korea have confirmed that it is widespread, even for applications that will only access low-level data, and particularly for the use of cloud services.

Korea is one of the 18 Certificate-Authorising Members of the CCRA. The National Security Research Institute (NSRI) is the body responsible for the CCRA, which specialises in encryption and is the certification body of Korea. The extent of interaction between the NSRI and other standards bodies within Korea is not clear.

[133] Revision of Notice on Security Certification of Cloud Computing Services.

[134] Hangoo Jeon, Young-Gi Min and K. Seo. Improvement Framework of Korean Certification System for Cloud Service Focus on Security. DOI:10.14257/IJSIA.2016.10.2.07.

[135] US Korea Business Council Letter November 2020.

[136] Business Software Alliance Cloud Survey.

The adoption and recognition of EU CC certification by Korea will remove a substantial non-tariff barrier. It would also reduce costs for Korean companies that export to the EU, as they would only need to get their products certified once within Korea.

6.3 Korean context for ethical standards in AI

To steer AI to become a key driver of the fourth industrial revolution, Korea developed an AI strategy in December 2019, not long after helping to negotiate the OECD AI Principles[137]. The OECD AI Principles, adopted in 2019[138], are an OECD legal instrument for 46 adhering countries, including Korea. At international level, Korea is playing an active role in AI governance, having recently hosted the second AI Summit in Seoul, in May 2024[139].

The use of AI has become a headline concern around the world since ChatGPT was made public. However, with the rapid growth in generative AI in particular, there has been recognition in Korea that it poses significant risks that need be addressed in a risk management framework. In June 2023, the MSIT announced its plan to invest USD 364 million in a five-year development of AI-driven tech projects for global leadership[140].

The draft law on AI is still in the National Assembly. Reuters reported that it is less restrictive than EU regulation and guarantees freedom to release AI products and services, only restricting them if regulators deem any product to be harming the lives, safety and rights of people[141]. For a list of bills on AI that are currently going through the legislative process, please see the Annex 2.

The joint statement following the first meeting of the Korea-EU Digital Partnership Council reaffirmed that:

> *both sides intend to discuss their respective definitions of high-risk AI applications and establish a permanent communication channel to regularly update each side on respective legislative and non-legislative frameworks aimed at realizing trustworthy AI. Both the EU and South Korea sides also intend to coordinate approaches in the Global Partnership on Artificial Intelligence (GPAI), e.g., to new member candidates and project proposals*[142]*.*

[137] National Strategy for Artificial Intelligence
[138] Recommendation of the Council on Artificial Intelligence
[139] Seoul declaration on AI May 2024
[140] South Korea to invest $364 million in AI-driven tech projects for global leadership
[141] OpenAI CEO encourages South Korea to supply chips in AI boom
[142] Republic of Korea – EU Joint Statement

Section 7. Cybersecurity

There is no single cybersecurity law in Korea. Cybersecurity governance is directed by three agencies: the National Cybersecurity Centre (NCSC) under the National Intelligence Services for the government and public sector; the MSIT for the private sector, which includes the Korea Internet & Security Agency (KISA) that administers Korea's computer emergency response team (CERT) is the defacto enforcer of cybersecurity in Korea under the control of MSIT[143]; and then individual response systems for a diverse group of agencies, such as the one at the Ministry of National Defence for the military sector, and the National Security Research Institute (NSR).

All report to the National Security Office (NSO), Secretary to the President for Emerging and Critical Technologies and Cybersecurity (since 2021), and the National Security Council (NSC), under the President.

Korea's first National Cyber Security Strategy (NCSS) was released in 2019 by the NSO.[144] With the stated vison of creating a free and safe cyberspace to support national security, promote economic prosperity, and contribute to international peace. Like similar policy documents, it is built around a number of core pillars, goals and principles. The NCSS was updated in February 2024, with a greater focus on threats from the Democratic People's Republic of Korea (DPRK, North Korea).[145]

One key security control administered by KISA is the CSAP certification, which requires: 1) physical network separation; 2) a local CC certification; and 3) use of unique Korean encryption modules.

In connection with the CSAP, Korea's NIS has overseen domestic cybersecurity certification requirements through its National Security Evaluation Scheme since October 2014. Korea has broadly imposed the Security Evaluation Scheme for internationally CC-certified information technology products to be sold to the public sector.

In October 2022, the NIS introduced a three-tiered scheme dividing all public institutions into sensitivity tiers, 1 to 3, with 1 being the lowest and least sensitive. This includes some public institutions such as universities and public schools, which may still use internationally CC-certified ICT products without additional domestic security verification.

Feedback from EU companies indicates that only a few institutions are on the lowest level that permits the use of foreign services. This is estimated to be less than 10% of the total information market, effectively shutting out the majority of the public market to non-Korean companies, including those based in the EU. Concerns are that, with the next revision, government institutions not currently included in this triple classification will become classified.

According to a recent assessment issued by the international Computer and Communications Industry Association, the three-tiered system introduced by the Korean government represents very modest changes, as numerous other restrictions were left in place. As a result, not a single foreign supplier has so far succeeded in qualifying to offer cloud services, even at the lowest tier of risk level possible.

Therefore, the National SES still applies to most major public institutions, which account for over 90 percent of the public sector market, including all central administrative institutions such as ministries and metropolitan local governments.

[143] Korea - The Korea Internet & Security Agency
[144] Korea - National Cyber Security Strategy 2019
[145] Korea - Updates the NCS Feb. 2024

The NIS requires cloud service providers to use the Korean domestic encryption algorithm, KS X 1213:2004 ARIA. The international and widely used algorithm is the AES to ISO/IEC 29167-10:2015. Harmonisation on the international standard would enhance interoperability and security. The NIS requires cloud service providers to use ARIA to obtain CSAP. Microsoft and Amazon Web Services use AES, which is the global standard.

One major regulation in the CSAP is that it demands the physical separation of public data when the internationally accepted standard is for all, but the most sensitive (level 3) data is to utilise logical network separation of non-sensitive information. This is a barrier to foreign companies entering the public sector cloud-services market. No foreign operator had achieved CSAP accreditation at the time of writing[146].

Security certificates for public cloud management are issued by KISA[147]. The K-ISMS is a country-specific information security management standard operated by KISA. It defines a stringent set of control requirements, designed to help ensure that organisations in Korea consistently and securely protect their information assets.

These procedures have a significant overlap with ISO/IEC 27001 ISMS control objectives, but are not identical. K-ISMS provides a more detailed investigation against requirements than a general ISO/IEC 27001 assessment[148]. Under the supervision of the MSIT, KISA is the K-ISMS certifying authority. Certification is valid for three years, and certified entities must pass an annual audit to maintain it, which is costly. The specifications for K-ISMS certification are based on ISO/IEC 27001, ISO/IEC 27018, and other international standards that govern information security.

Amazon[149], Microsoft[150] and Google Cloud[151] services in Korea all claim to be K-ISMS compliant. Since the PIPA came into force, the K-ISMS has evolved into a new certification system – ISMS-P – to comply with PIPA mandates. ISMS-P keeps the original 80 controls of the K-ISMS and adds an additional 22 related to PIPA compliance[152]. It is unclear whether any foreign cloud service provider has achieved full ISMS-P certification.

7.1 Cyber security: EU and Korea

The size of the Korean cybersecurity consulting market in 2022 encompassed 200 companies and 15,000 employees, with an estimated turnover of KRW 4.5 trillion (EUR 3 billion). This is for the public and private market. Currently, foreign companies – including those from the EU – can only access the private sector component.

Many of the cybersecurity services offered by EU companies are delivered via cloud services that are usually also used by their clients. For example, if a major bank is using a particular cloud vendor, then their cybersecurity service would also be hosted within that cloud to serve that client. Offering such services to the public sector in Korea would require CC certification.

However, according to recent discussions with EU companies in Korea that provide cybersecurity services, not all foreign products/services that have CC certification in their country of origin are accepted by the NIS – particularly if they are delivered via one of the global cloud providers – and the NIS imposes onerous conditions on them to comply.

[146] Presumably reference to sections on the cloud and barriers.

[147] South Korea – ISMS-P.
[148] South Korea – ISMS-P.

[149] South Korea – Amazon Web Services K-ISMS.
[150] South Korea – Azure K-ISMS.
[151] South Korea – Google K-ISMS.
[152] South Korea – ISMS-P Thales.

For example, the certification renewal period required for a cybersecurity product in Korea is one third or half as long as the international standards. Cybersecurity firms also have to pay tens of millions of won just to take the test for renewal, as well as paying for the international CC certification[153]. Korean local standards impose excessive security requirements and veer significantly from global standards, with no proven benefit of increasing cybersecurity. Estimates are that a USD 290 billion market is effectively closed to EU companies[154].

7.2 Need for more stringent security controls

Recent major cybersecurity breaches in Korea, plus public service outages, indicate that the current level of controls and service continuity/backup are inadequate.

For example, a two-day outage of the e-government system, which is based at a single data centre in a rural area, meant that no government office could issue the documents needed regularly as part of Korean life[155]. An investigation by the Ministry of the Interior and Safety revealed that a router had failed, and stated that the ministry would 'self-correct to build a stable, digital government to prevent the recurrence of such issues that inconvenience the public under any circumstances.'

The main criticism, however, was that there was no redundancy or effective backup/failover for continuity of such a critical system as there are in financial data systems, for example. There was no mention of vendor service level agreements or adherence to recognised standards for business continuity, such as ISO 22301[156]. That it also took over two days to locate and correct the problem would be inconceivable for a commercially owned, private sector DC. A 2024 leak of personal information also indicated a lack of controls[157].

This is without the persistent threat of cyberattacks from North Korea. Of the 1.62 million hacking attempts made against Korean companies and public bodies last year, more than 80% have been traced back to North Korea, according to the NIS[158]. Successful cyberattacks were recently detected against Korean defence contractors[159] and the courts[160] in 2024. The use of generative AI has also been observed in some of these events[161].

One benchmark of effective cybersecurity is the ITU Global Cybersecurity Index. Korea ranked equal fourth with Singapore and Spain in the most recent 2020 index (the 2023 index is being compiled)[162]. The report noted that 'organisational measures' could be improved, including backup and continuity, which appear to be a major shortcoming.

This was identified in discussions with EU companies in Korea, where the general view was that Koreans have an overreliance on technical defences and do not have sufficient 'plan B or C' contingency plans in the event of a failure.

The ITU also recommend that the NCS be updated at least every five years to take evolving threats into account. For example, generative AI has only emerged as a persistent threat in the hands of bad actors in the last two years, but is being rapidly adopted.

---

[153] South Korea – Revises its cybersecurity regulations.

[154] Interviews. It is understood that this figure compiled tender totals over three years 2021-2023.

[155] South Korea – public data centre failure. November 2023.

[156] ISO – ISO 22301. Security and resilience – Business continuity management systems – Requirements.

[157] South Korea – May 2024 leak of personal documents.

[158] South Korea – DPRK cyberattacks in 2024 against South Korea.

[159] South Korea – DPRK Targets South Korean Defence Firms. April 2024.

[160] South Korea –Targets South Korean Courts. February 2024.

[161] South Korea – Generative AI being used in DPRK attacks. January 2024.

[162] ITU – Global Cybersecurity Index, 2020.

The protection of children has also emerged as major challenge since the COVID-19 pandemic, when many were forced online for education, exposing very young children to content that is inappropriate for developing minds. These issues need to form a specific part of the NCS.

It had been five years since Korea's NCS was issued, so it was duly updated in February 2024[163]. Although AI is mentioned as an emerging threat in the strategy, the protection of children was not mentioned

So, there is much work to be done, and it is clear that allowing EU-based cybersecurity companies to participate fully in the public and private sector will enhance Korea's cyber defences and increase resilience.

7.3 Standards for managing cybersecurity risk

ICT security standards are summed up in Annex 4 A 4.1. The MSIT Framework Act on Intelligent Informatisation was published in 2020[164]. In 2020, KISA stepped in to establish interoperability standards specifically for decentralised identity, as there are plethora of competing and non-interoperable applications in Korea[165].

The Ministry of the Interior and Safety was charged with a digital government innovation plan to implement e- government, which included a section on security standards[166].

The NSRI[167] – a government-funded entity that does cybersecurity research and training – also runs the CCRA, which was administered by the NIS, before being transferred to the NSRI in 2012. The NSRI is therefore the standards body for certification in Korea.

In 2021, the G7 – of which Korea is an observer – issued a declaration on creating 'a trusted, values-driven digital ecosystem', at the meeting of the G7 Digital and Technology Ministers in the UK[168]. Trusted cross-border data flows featured strongly in the declaration, with the G7 endorsing a Roadmap for Cooperation on Data Free Flow with Trust[169] as one of four annexes for action. This has also been endorsed by Korea and Australia (which are not G7 members) and is one of the strongest statements yet on a high-level, cohesive policy to enable secure global digital commerce.

The adoption of global standards that enable interoperability will further enhance Korea's ICT sector capabilities while managing cybersecurity risk, especially when engaging in e-commerce and cross-border digital trade.

[163] South Korea – Analysis of the NCS 2024 Update.

[164] South Korea – ICT Framework Act on Intelligent Informatisation.

.[165] South Korea – Decentralised identity.

[166] South Korea – Ministry of the Interior and Safety digital government innovation plan.

[167] South Korea – National Security Research Institute.

[168] UK G7 – Ministers Declaration.

[169] G7 – Roadmap for Data Free Flow with Trust.

Section 8. Benefits of the envisioned Korea-EU digital trade agreement

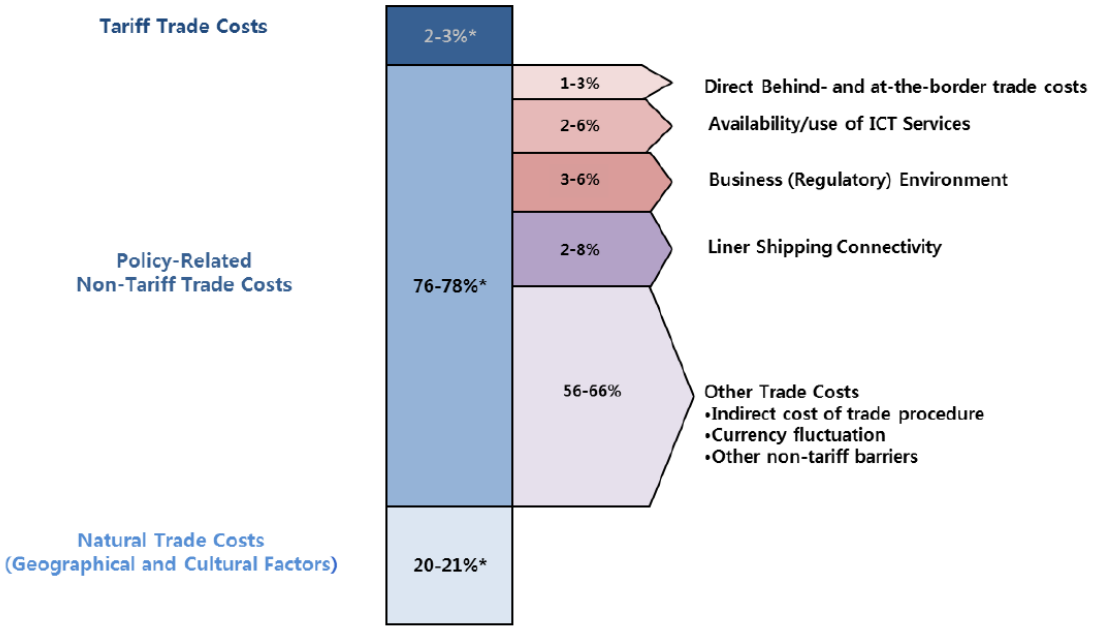
This section discusses the potential effects of a future EU-Korea DTA, based on available estimations of the general effect of DTAs (discussed in Section 3), and projections of some of those estimates on trade flows between the EU and Korea.

8.1 Reductions in policy-related trade costs

Data has become a big part of value-added chains for production of both products and services. Among other things, data help to produce new combinations of goods and services traded across borders, facilitate customs and payments, generate market analytics, improve communications, and optimise business processes. Any regulation concerning data will therefore ripple through value chains of multiple industries, affecting thousands of businesses and millions of consumers.

Available estimates project that the DTA will impact policy-related, non-tariff trade costs that are linked to data management and use. Generally, such non-tariff trade costs make up more than 70% of digital-trade-related costs incurred by businesses (see Figure 8.1 below). Businesses involved in trade between Korea and the EU could therefore see impacts on a range of tariffs involving a digital component.

Figure 8.1 Structure of trade-related costs incurred by businesses



Source: Duval, Y., Utoktham, C. and Kravchenko, A (2018). "Impact of implementation of digital trade facilitation on trade costs", ARTNeT Working Paper Series, No. 174, January 2018, Bangkok, ESCAP.

Automation, coordination, transparency and traditional trade in goods

Automation, coordination and transparency together are another overarching issue that is significant for trade in goods in the digital era. Regulatory alignment around data will enable 1–4% gains in trade in goods. EU- Korea bilateral trade in 2021 surpassed USD 107 billion. Applying 1–4% to this figure gives a potential increase in bilateral trade of USD 1.073–4.292 billion, coming only from harmonisation of data-related rules.

8.2 Data and parcel trade

Digitalisation affects parcel trade more profoundly, as it is closely connected to e-commerce, which is fully driven by digital technologies and data innovation. The effect of digitalisation on parcel trade is thought to be around 4%. In the context of EU-Korea trade, parcel trade is seen in the statistics on cross-border e-commerce. Korean online purchases from the EU totalled USD 1.1 billion in 2022, and USD 874 million in 2023. Applying 4% to these figures yields an additional USD 34.96–44 million in online sales from the EU to Korea.

When it comes to parcel trade, there is a second-order effect to consider too. Regulation on data and the use of AI for parcel screening will help to fight trade in counterfeited goods – a problem that has been aggravated since the COVID-19 pandemic and has the biggest negative impact on European firms in the form of intellectual property right infringements. According to recent OECD findings, France, Germany, Italy, Switzerland and Denmark are most adversely affected[170], and a future DTA could therefore impact online trade between these countries and Korea.

8.3 AI and growth in exports

Wider use of AI will generate multiple effects on international trade. The following insights from eBay show how significant the trade-enabling potential of AI could be. As a result of eBay's machine translation service, eBay-based exports to Spanish-speaking Latin America increased by 17.5% (value increased by 13.1%). This growth can be compared with the effect that a reduction of distance has on trade. It was found that a 10% reduction in distance between countries is correlated with increased trade revenue of 3.51%. A 13.1% increase in revenue from eBay's machine translation is equivalent to reducing the distance between countries by over 35%[171].

The above example shows that the use of AI-developed services in trade between the EU and Korea could potentially help more European firms overcome language and information barriers, and participate in bilateral trade. Coordinating rules on the use of AI will create a more predictable environment for businesses and help them manage risks better, facilitating the use of AI in trade.

As interviews with representatives of European businesses in Seoul have shown, changing regulation is one of the biggest challenges to navigate the Korean market. If that regulation is aligned with European rules, perceptions of predictability will increase and perceptions of risk will go down.

[170] Global Trade in Fakes : A Worrying Threat.

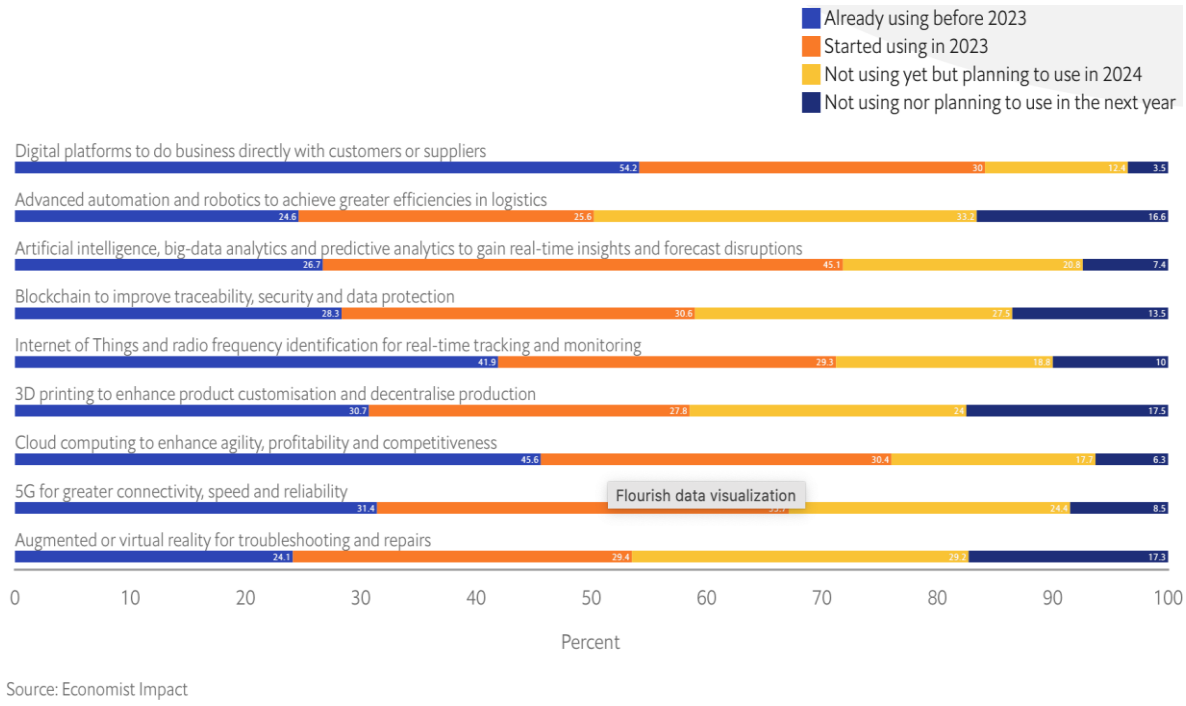
[171] The impact of artificial intelligence on international trade.

8.4 AI, costs and value chain management

According to research by McKinsey, companies will see a meaningful cost reduction from the use of generative AI and analytical AI in areas such as human resources, supply chain management, service operations and software engineering. Simultaneously, many sectors will see improvements in profitability of more than 5% – including marketing and sales, legal services and compliance, supply chain management and IT[172].

A survey carried out by *The Economist* suggests gains from use of AI will be in excess of 30% for cost optimisation and supply chain management. It also concluded that, overall, in the next couple of years, wider application of digital technologies in trade (Figure 8.2) will increase governments' intention to regulate their use out of concerns for privacy, security and fair competition[173].

Figure 8.2 Extent of technology adoption in trade operations



Source: Economist impact. Trade in transition 2024.
https://impact.economist.com/projects/trade-in-transition/technological-leaps

Interoperable rules and standards are essential for companies to enjoy the benefits of international trade. While the figures above may seem hypothetical, interviews with companies working in the Korean market showed that they have some basis. For example, due to Korean regulations, foreign companies can currently store data for one year only, while Korean companies can store customer data for up to five years. For companies in the human resources industry, this is a serious impediment, because they lose 30% of the customer data stored in their databases every year as a result of this rule. This means that they cannot enjoy the benefits of AI data analytics on a level playing field.

Regulatory alignment acknowledging both the opportunities and risks of AI-use would help to create a level playing field for European companies in the Korean market. Without adequate

[172] The state of AI in early 2024: Gen AI adoption spikes and starts to generate value. McKinsey Survey.

[173] Supply chains in sync.

rules, companies will be limited in using their AI models in the Korean market, which could initially put them in an inferior position to their Korean competitors.

Greater participation of SMEs, women and young people in international trade

The available data suggest that small and micro-businesses, and businesses set up by women and young people, export more as internet access improves and other services that help them to overcome communication and cultural barriers evolve. In Korea, there is a notable trend towards a growing number of young people under the age of 35 engaging in international trade between the EU and Korea.

Based on data for Europe, the disparity between small and large firms in export participation is much smaller for sales over digital networks than for overall trade. In addition, as firm size increases, the reliance on e-commerce marketplaces decreases, while the use of the firm's own website or app increases[174]. Smaller firms therefore rely more on digital tools for their operations, and are particularly sensitive to regulation in this realm.

While it is challenging to estimate the immediate effect of a future DTA on the participation of European SMEs in trade with Korea, a stable and predictable regulatory environment that clearly defines rules could help in terms of cost optimisation and better planning.

[174] Digital Trade for Development.

Section 9. Digital trade agreement from a business perspective - Stakeholders Interview results

A team of experts ran a series of in-depth interviews with representatives of foreign businesses and business councils in Korea. The interview questionnaire can be found in Annex 5 A 5.1. During the interviews, several issues that deserve attention emerged. Some of these have been mentioned throughout this report in relevant sections, and others are summed up below.

1) Most of the EU businesses feel the need for standards alignment with regard to interoperability between Korea and the EU because Korea has some specific standards that differ from internationally accepted standards.

2) Most of the businesses entering the Korean market are prepared to bear costs to work around existing regulations on data localisation, data transfer, etc., if they see market potential. Perceptions of market potential and risk vary greatly depending on the type of company: big businesses are in a slightly more advantageous position than SMEs or startups.

3) Digital rules in Korea can differ depending on whether companies operate in the public or private sector. The public sector has stricter rules for using Korean local digital certificates, and this requirement often locks foreign companies out of participating in tenders in certain public sectors.

5) Korean marketplaces (such as Naver or Coopang) do not disclose analytical data about customers to business users as international ones do. This significantly limits competitive capabilities.

6) National security is the reason most often given to foreign companies to justify access to the source code, and Korea's main regulatory act, PIPA, serves as grounds for that. It should be noted, however, that a similar rule can be applied to Korean companies if their activities conflict with national security considerations, because PIPA applies to the processing of personal information of data subjects based in Korea, regardless of their nationality or residency status.

7) Korea is more open to the idea of recognition of e-certificates, e-signatures and e-identities with certain Asian countries than with European countries, because it perceives them as being more digitally advanced.

8) Some Korean companies find loopholes and register as logistics companies while actually operating as e-platforms. In certain instances, this creates difficulties for European importers that have invested to develop the market.

9) Cybersecurity, AI, robots and data centres are seen as having the highest potential for export growth from the EU to Korea.

10) Clarification of the rules on value added tax for digital products and services is needed.

11) Foreign companies in Korea are required to store data for no more than one year, which is a considerably shorter period than the five years given to domestic companies. For some companies, this regulation means losing 30% of their database every year. Much of this data can never be retrieved.

In addition to the interviews, the team administered an online survey through Google Forms, with the help of the European Chamber of Commerce in Korea and individual foreign businesses operating in the digital trade space in Korea. The survey questionnaire can be found in Annex 5 A 5.2, and the results are summarised below.

Most of the respondents – which were medium, small and micro-businesses – see potential for expansion in the Korean market in the next 2–3 years, with 77% considering themselves to be involved in digital trade in some way. The reasons that respondents gave for growth are as follows.

- High and growing digital penetration.
- In my industry, Korea is a mostly untapped market that has expressed interested in the product. It is growing exponentially here, but the market is still small and has a lot of room for opportunities, growth and being one of the first 'players'.
- Korea seems to have a generally positive perception towards Northern Europe (particularly Denmark and its culture).
- Monetary support.
- As a service provider, expected deregulation and new regulations would be the points of services.
- FTA agreement in case of export.
- Strong government support and buy-in.
- Good talent pool, need to revamp the economy.
- Fully developed ICT industry sectors, infrastructure, etc.

Parts of the digital supply chain that business are involved in are as follows.

- Digital ordering but physical delivery (44%).
- Digital payments (33%).
- E-invoicing (55%).
- Data storage (55%).
- Data transfer (33%).
- E-signatures (44%).
- Digital customs (44%).
- Encryption (33%).
- Privacy (44%).
- Cybersecurity (33%).
- Digital marketing consulting (11%).

In terms of regulatory scrutinity, businesses cited data storage, data transfer and cybersecurity as the areas with the strictest regulations. Overall, 30% of respondents think Korean digital-trade barriers are mild (5 out of 10 on a 10-point scale), while 30% consdier them relatively high (7 and above out of 10). A majority of respondents think that the costs that their businesses have to incur due to Korean regulations on digital trade and digital economy are relatively high (7 and above out of 10).

The biggest barriers identified by EU companies in Korea are as follows.

- Local digital channels (Naver, Coupang, Kakao, etc.).
- Although electronic payments have become easier with the rise of tools such as Paymentwall, Korea's unique banking system will face some hurdles, including its strong reliance on mobile phone numbers.

- Authentication certificates.
- Banking services.
- Data privacy punishments are too strict.
- Digital payments, data storage and cybersecurity.
- The lack of regulatory oversight to ensure fair, open, digital platforms.

To improve the digital business environment, respondents suggested the following.

- The fact that immigrants/expats are subjected to different rules and laws with banking (traditional and digital, such as Kakao Bank) is unfair and limits the market.
- Mutual acceptance of authentication certificates.
- Personal data protection needs to be more succinct and feasible.
- Remove data storage laws that specify long- or short-term duration for non-security-related applications. Make it easier for foreigners without access to local online banks to make payments.
- If digital platforms are mandated to provide fair access for third-party companies as in the EU DMA, it could help create more services via platforms.

All of the respondents think that regulatory alignment with other countries (the EU, US, UK, etc.) would help their business operations in Korea.

Section 10. General conclusions

European businesses perceive Korea's market as offering opportunities for digital trade and the digital economy in general. This is due to its well-developed infrastructure, position as a leading manufacturer of ICT technologies, the growing e-commerce market and well-connected consumers. At the same time, there has been a trend towards more data-related regulation in Korea in recent years that resulted in additional operational costs and unfair competitive practices due to regulatory fragmentation at international level.

Korea has always been a proponent of an open and rule-based multilateral trading system. It remains a supporter of the ongoing negotiation on digital rules in the WTO known as Joint Statement Initiative on E-Commerce. All of Korea's FTAs that contain e-commerce chapters and DTAs include provisions for adhering to WTO agreements. The country would benefit from internationally applied regulatory principles for digital trade as regulatory alignment and consistency in rules is beneficial for business in general. Growing Digitalisation of trade increases demand for ICT infrastructure, which is one of the key export items for Korean companies.

The Korean government is taking a proactive position towards the digital trade policy pursuing ambitious commitments in relation to data flows, e-authentication and protection against forced tech transfer. Korea increasingly seeks agreements with the like-minded countries to insure interoperability of standards essential for the development of digital trade. At the same time, geopolitical complexities necessitate Korea to adhere to practices for sensitive data to pursue legitimate public policy objectives. Network segregation for financial institutions is one of the examples of such practices.

Different standards for authentication and encryption may also become an issue, especially for small and microbusinesses as they have limited financial means to overcome such challenges compared to big businesses. It should be noted however, that due to demands from institutions within the country the Korean government is undertaking serious efforts to make the regulation clearer and less burdensome for businesses to comply with.

A future DTA between the EU and Korea may not be a solution for overcoming all challenges that European companies face in the local market, but it would offer a range of advantages. First, it would create a predictable regulatory environment for businesses, increasing the stability of rules. Interoperability of standards would also help companies to optimise costs.

A future agreement would also help to unlock more business opportunities for SMEs and women, as well as encouraging smoother customs clearance and better detention of counterfeited goods. Data management and data security are crucial for the resilience of supply chains, and having these aligned between the EU and Korea would help supply chains to operate more effectively and efficiently. These are only a few potential outcomes of a future DTA between the EU and Korea.

While much remains unknown about such an agreement, it is important to remember that data penetrates all sectors of the economy, as well as international trade. Having rules around data flows aligned between the EU and Korea would help to deepen bilateral trade relations, while minimising potential disruptions and security risks.

ANNEXES

A1.1 Digital trade policy issues discussed under the WTO JSA on e-commerce, stabilised text

A. Scope and General Provisions	A1-3	The agreement applies to measures affecting trade by electronic means, echoing language from the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) No Definition of E-commerce: Interestingly, the text does not define "electronic commerce," which was previously included in earlier drafts
B. Enabling E-Commerce	A.4 Electronic transaction framework	Provisions to facilitate electronic transactions, including electronic signatures, invoicing, and payment services.
	A.5 Electronic authentication and electronic signatures	
	A.6 Electronic contract	
	A.7 Electronic invoicing	
	A.8 Paperless trading	
	A.9 Single windows data exchange and system interoperability	Notably absent are provisions related to cross-border data flows and data localisation, which were contentious issues during negotiations. The U.S.'s withdrawal from supporting robust data flow norms significantly impacted this aspect of the agreement
	A.10 Electronic payments	
C. Openness and E-Commerce	A.11. Customs duties on electronic transmissions	Commitment to maintaining a moratorium on customs duties for electronic transmissions, although this is subject to periodic review.
	A.12. Open government data	

	A.13 Access to and use of Internet for electronic commerce	Ensures open access to the internet and government data, promoting transparency
D. Trust and E-Commerce	A.14 Online consumer protection	Measures for online consumer protection, including regulations against unsolicited commercial messages (spam) and personal data protection.
	A.15 Unsolicited commercial electronic messages	
	A.16 Personal data protection	
	A.17 Cybersecurity	Provisions aimed at enhancing cybersecurity measures within digital trade frameworks.
E. Transparency, Cooperation and Development	A.18 Transparency	
	A.19 Cooperation	
	A.20 Development	Specific clauses aimed at bridging the digital divide, offering technical assistance and capacity building for developing nations 16. However, these commitments are often framed in "best effort" language, raising concerns about their enforceability.
F. Telecommunications	A.21 Telecommunications	Based on existing GATS frameworks, covering competitive safeguards and licensing processes
G. Exceptions	A.22 General Exceptions	
	A.23 Security Exceptions	
	A.24 Prudential Measures	
	A.25 Personal Data Protection Exceptions	
	A.26 Indigenous People	
	A.27 Dispute Settlement	

H. Institutional Arrangements and Final Provisions	A.28 Committee on Trade-Related Aspect of Electronic Commerce	
	A.29 Acceptance and Entry into Force	
	A.30 Implementation	
	A.31 Reservations	
	A.32 Amendments	
	A.33 Withdrawal	
	A.34 Non-application of This Agreement between Particular Parties	
	A.35 Review	
	A.36 Secretariat	
	A.37 Deposit	
	A.38 Registration	
ANNEX		

Source: WTO ELECTRONIC COMMERCE NEGOTIATIONS STABILIZED TEXT – July 26, 2024.https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/87.pdf&Open=True

The text includes many "endeavour" commitments (32 instances) and "encourage" references (11 instances), which may lead to ambiguity regarding the obligations of member states.[175]

[175] WTO electronic commerce negotiations stabilized text July 2024

A1.2 Digital trade agenda issues covered in Korea's FTAs e-commerce chapters

Policy issues /agreement	Kor-Peru	Kor-US	Kor-Aus	Kor-Can	Kor-China	Kor-Viet	Kor-Col	Kor-CA	RCEP	Kor-Isr	Kor-Sing
E-commerce chapter	+	+	+	+	+	+	+	+			
WTO rules applicability	+	+	+	+	+	+	+	+		+	+
Domestic Regulatory Frameworks UNCITRAL Model Law on Electronic Commerce 1996			+			+	+		+	+	+
Customs Duties	+	+	+	+	+				+		+
Electronic Authentication and Electronic Signatures	+/-	+	+		+	+			+	+	+
Online Consumer Protection	+	+	+	+		+		+		+	+
Paperless Trading	+	+	+	+	+/-	+	+	+	+	+	+
Access To and Use of The Internet for Electronic Commerce		+									+
Cross-Border Information Flows		+							+		+
Unsolicited Commercial Electronic Messages			+						+		+
Cooperation	+			+	+	+	+	+	+	+	+
Electronic supply of services								+		+	
Digital Products								+			
Transparency									+		
Cyber Security									+		+
Location of Computing Facilities									+		
Settlement of Disputes									+		
Non-Discriminatory Treatment of Digital Products										+	
Online PERSONAL DATA PROTECTION	+		+	+		+	+	+	+		
Electronic Invoicing											+
Location of Computing Facilities for Financial Services											+
Electronic Payments											+
Information and Communication Technology Products that Use Cryptography											+
Source Code											+

Policy issues /agreement	Kor-Peru	Kor-US	Kor-Aus	Kor-Can	Kor-China	Kor-Viet	Kor-Col	Kor-CA	RCEP	Kor-Isr	Kor-Sing
Cybersecurity Cooperation; Online Safety and Security, Principles on Access to and Use of the Internet for Electronic Commerce											+
Data Innovation											+
Open Government Data											+
Competition											+
Artificial Intelligence											+
FinTech Cooperation											+
Digital Identities											+
Standards, Technical Regulations and Conformity Assessment Procedures for Digital Economy											+
SMEs and Startups											+
Stakeholder Engagement											+

Annex 2

A2.1 Korean legislator bills that shaped current Act on AI

1	Evaluation by council	2123709	인공지능 책임 및 규제법안(안철수의원 등 10 인)	Artificial Intelligence Responsibility and Regulation Bill (Rep. Ahn Chul-su and 10 others)	Member	8 Aug 23
2	Evaluation by council	2120353	인공지능책임법안(황희의원 등 14 인)	Artificial Intelligence Responsibility Bill (Rep. Hwang Hee and 14 others)	Member	28 Feb 23
3	Submitted to council	2118726	인공지능산업 육성 및 신뢰 확보에 관한 법률안(윤두현의원 등 12 인)	A bill to foster the artificial intelligence industry and secure trust (Rep. Yoon Doo-hyun and 12 others)	Member	7 Dec 22
4	Evaluation by council	2116986	인공지능교육진흥법안(조해진의원 등 12 인)	Artificial Intelligence Education Promotion Bill(Rep. Cho Hae-jin and 12 others)	Member	24 Aug 22
5	Evaluation by council	2115314	한국인공지능·반도체 공과대학교법안(안민석의원 등 13 인)	Korean Artificial Intelligence and Semiconductor Technology University Bill(Rep. Ahn Min-seok and 13 others)	Member	18 Apr 22
6	Evaluation by council	2113509	알고리즘 및 인공지능에 관한 법률안(윤영찬의원 등 12 인)	A bill for a law on algorithms and artificial intelligence (Rep. Yoon Young-chan and 12 others)	Member	24 Nov 21
7	Evaluation by council	2111573	인공지능에 관한 법률안(이용빈의원등 31 인)	Bill on Artificial Intelligence (Rep. Lee Yong-bin and 31 others)	Member	19 Jul 21
8	Evaluation by council	2111261	인공지능 육성 및 신뢰 기반 조성 등에 관한 법률안(정필모의원 등 23 인)	A bill for a law on fostering artificial intelligence and creating a trust foundation (Rep. Chung Pil-mo and 23 others)	Member	1 Jul 21

9	Evaluation by council	2110148	인공지능교육진흥법안 (안민석의원 등 10 인)	Artificial Intelligence Education Promotion Bill (Rep. Ahn Min-seok and 10 others)	Member	17 May 21
10	Evaluation by council	2104772	인공지능 기술 기본법안(민형배의원 등 10 인)	Artificial Intelligence Technology Basic Bill (10 lawmakers, including Min Hyung-bae)	Member	29 Oct 20
11	Evaluation by council	2104564	인공지능 집적단지의 육성에 관한 특별법안(송갑석의원 등 11 인)	A special bill for the fostering of artificial intelligence integrated complexes (11 lawmakers, including Song Gap-seok)	Member	19 Oct 20
12	Evaluation by council	2103515	인공지능산업 육성에 관한 법률안(양향자의원 등 23 인)	A bill to foster the artificial intelligence industry (23 Representatives, including Yang Hyang-ja)	Member	3 Sep 20
13	Evaluation by council	2101823	인공지능 연구개발 및 산업 진흥, 윤리적 책임 등에 관한 법률안(이상민의원 등 11 인)	A Bill for the Promotion of Artificial Intelligence Research and Development, Industry Promotion, and Ethical Responsibility (Rep. Lee Sang-min and 11 others)	Member	13 Jul 20

Annex 3

A3.1 Standards comparison between Korea and EU

Area	Korea	EU
A standard cryptographic technique	ARIA KS X 1213:2004	Advanced Encryption Standard (AES) algorithm to ISO/IEC 29167-10:2015
Cloud services	Personal Information and Information Security Management System (ISMS-P) based on international ISOIEC 27001 with stricter controls K-ISMS CSAP (Cloud Security Assurance Program) CSAP IaaS CSAP SaaS CSAP DaaS	ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27017[176]
Cybersecurity		Based on ISO/IEC 17788; ISO/IEC 17000; ISO/IEC 9000; ISO/IEC 27000 ISO/IEC 29147 and ISO/IEC 30111 ISO/IEC27005
Electronic identification		the eIDAS (electronic Identification, Authentication, and trust Services)
Data sharing	PIPA (Personal Information Protection Act)	ISO/IEC 23751
Electronic health records	EMR System Certification[177]	ISO 13606
Healthcare Management System	EMR System Certification based on international and domestic practices	ISO 7101
Evaluation criteria for IT security	ISMS-P (Information Security. Management System)	ISO 15408
AI ethical standards	ISO 42001	ISO 42001: 2023
Protection of payment related data	PCI DSS[178]	

[176] EU Cloud Certification Scheme

[177] EMR System Certification

[178] PCI DSS

Annex 4

A4.1 Key international technical standards for ICT Security

ISO/IEC 27701	ISO – ISO/IEC 27701:2019 – Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
ISO/IEC 27559:2022	Information Security, Cybersecurity and Privacy Protection – Privacy Enhancing Data De-Identification Framework for identifying and mitigating re-identification risks and risks associated with the lifecycle of de-identified data.
ISO/IEC 29134:2023	Security techniques — Guidelines for Privacy Impact Assessment: a process on privacy impact assessments, and a structure and content of a PIA report.
ISO/IEC 29167	The Advanced Encryption Standard (AES) algorithm.
ISO/IEC 31700	ISO – ISO 31700-1:2023 – Consumer protection — Privacy by design for consumer goods and services — Part 1: High-level requirements
ISO 13606:2019	ISO 13606 standard defines a rigorous and stable information architecture for communicating part of or all the electronic health record (EHR) of a patient between EHR systems.

Annex 5

A5.1 Interview questionnaire

Question	Reply
1. What best describes the size of your business?	a. SME b. big company c. individual entrepreneur d. other _____
2. What best describes the nature of a sector your company operates in?	a. F&B b. Insurance & Finance c. Consulting e. Manufacturing f. E-commerce g. Retail and wholesale trade h. Education i. Arts, entertainment and recreation j. Other _____
3. How would you describe the reliance of your business on digital means of operations in Korea?	a. Highly dependent b. Somewhat dependent c. Digital does not play any significant role in my business d. Unsure e. Other _____
4. Do you have to use digital intermediation platforms (DIPs), online marketplaces, apps, etc., in Korea to facilitate transactions for your business? If yes, which ones _____	a) YES b) NO
5. How would you evaluate on a scale 1 to 5 barriers in the digital value chain when using DIPs in Korea? 1-low barrier - high barrier	a. Order placement. ____ b. Payment ____ c. Delivery ____ d. Security ____ e. Cloud computing ____ f. Authentication ____ g. Other _____
6. How would you characterise the cost of using digital services in Korea compared to your country?	a. More expensive b. Less expensive c. Similar d. Not sure
7. Which Korean government policies regarding digital trade affect your business the most?	

Question	EU - KR Digital FTA impact
1. Would you agree that EU and Korea need digital trade agreement to facilitate transactions in digital economy and trade?	a. Highly agree b. Somewhat agree c. Neutral d. Somewhat disagree e. Disagree

Question	EU - KR Digital FTA impact
2. On a scale of 1 to 5 (low to high) which *thematic areas* are a priority for your business to be addressed in the EU - Korea Digital Free Trade Agreement? • Collaborative Research • Semiconductors • HPC and Quantum Technologies • Cybersecurity and Trust • Beyond 5G/6G • Skills-Mobility Digital Inclusion • Artificial Intelligence • Online & Digital Platform Cooperation • Data related Platform Cooperation • Digital Identity and Trust Services • Digital Trade (including cross border data transfers)	Coherence
3. When would you like to see the *implementation* of the areas you gave a 4 or 5 rating to? a. In the next one to two years b. In the next two to three years c. In the next three to four years	Effectiveness
4. On a scale of 1 to 5 in your view, what are the main *inhibitors or barriers* to your ability to engage today in digitally enabled trade in Korea? a. Technology and Infrastructure b. Human resource, institutional aspect c. Laws and regulations d. Business model (investment, operation, etc.) e. Other	Coherence
5. What do you think will need to be done to *improve the areas* you gave a 4 or 5 rating to?	Impact, Sustainability
6. How would or should an EU- Korea Digital FTA *improve your business* between the EU and Korea or v/v?	Coherence, Impact
7. Korea is engaging with other countries in digital agreements for trade, such as Korea – Singapore Digital Partnership, and has joined the Digital Economy Partnership Agreement (DEPA). What do you foresee on the impact of these agreements on your business from such agreements? a. Positive impact on my business b. No impact on my business c. Negative impact on my business d. Unsure	Risk, Impact
8. (**For Private sector stakeholder only**) How much savings (for example, as a percentage of the value of your trade revenue) could be generated from the increased use of digital technologies in your business?	Effectiveness, Efficiency
9. (**For public sector stakeholder only**) Do you foresee any risks or concerns related to a Korea – EU Digital FTA? If yes, how might these risks be mitigated?	Risks and Mitigation
10. Do you have any other comments or views related to digital trade, cross border data flows, or anything else	Coherence, Impact

Question	EU - KR Digital FTA impact
that should be addressed in an EU- Korea Digital FTA to improve your business?	

A5.2 Survey questionnaire

	Questions	Responses
1	Which of the following best describes size your business?	Big business Medium business Small business Micro-business Other
2	Do you see opportunities to expand your business in Korea in the next 2-3 years?	Yes, my business will expand Business will remain same or better Business will remain same or worse Other
3	What advantages does Korea have to offer for your business?	
4	Do you think your company is involved in digital trade?	Yes No Other
5	If yes, please, choose parts of the digital value chain that apply to your business.	digital ordering but physical delivery digital ordering and digital delivery digital payments e-invoicing e-signatures digital customs data storage data transfer encryption network segregation privacy cybersecurity other
6	Which of the above face the biggest regulatory scrutiny in Korea?	
7	How do you perceive overall digital barriers in Korea on a scale from 1 to 10 with 10 being impossible to overcome?	1 – low 10 – high
8	Which of the digital related barriers in Korea has the biggest impact on your business?	
9	On a scale from 1 (low) to 10 (high) how do you perceive costs that your business has to incur due to Korean regulation related to digital trade and digital economy?	1 – low 10 – high
10	What aspects of Korean digital regulation do you think could be improved to make it business friendly?	
11	Do you think that regulatory alignment with other countries (EU, US, UK, etc.) can help your business?	Yes No Other
12	How much are you aware of the digital trade agreements and their role in promoting digital trade?	Unaware Somewhat aware Well aware


twitter.com/ICF


linkedin.com/company/icf-international


facebook.com/ThisIsICF

icf.com


#thisisicf

About ICF

ICF (NASDAQ:ICFI) is a global consulting and digital services company with over 7,000 full- and part-time employees, but we are not your typical consultants. At ICF, business analysts and policy specialists work together with digital strategists, data scientists and creatives. We combine unmatched industry expertise with cutting-edge engagement capabilities to help organizations solve their most complex challenges. Since 1969, public and private sector clients have worked with ICF to navigate change and shape the future. Learn more at icf.com.