

EU-Singapore Digital Partnership

Digital Trade Principles

Preamble

The European Union (EU) and Singapore:

recall their commitments on electronic commerce in the Chapter 8 of the EU-Singapore Free Trade Agreement.

support the ongoing negotiations under the framework of the Joint Statement Initiative on electronic commerce in the World Trade Organization as a key instrument to advance global rule-setting in digital trade, which should result in common rules for digital trade agreed and upheld at the World Trade Organization, benefiting developing and developed economies alike, and safeguarding each country's right to regulate for legitimate public policy objectives.

are united in their support for open digital and telecommunications markets which are competitive, transparent, fair, and free of unjustified barriers to international trade and investment.

recognise the role of digital trade as a key enabler of sustainable development and its contribution to the green and digital transformation of our economies and therefore consider that digital trade rules should be future-proofed and responsive to innovation and emerging technologies.

underline that digital trade should support entrepreneurship and empower a full range of businesses to participate in the global economy, notably women entrepreneurs and micro, small, and medium-sized enterprises, while promoting digital inclusion of groups and individuals that may disproportionately face barriers to digital trade.

emphasise that digital trade should be used to support jobs, raise living standards, and respond to the needs of workers, innovators, and consumers.

share the objectives of ensuring predictability and legal certainty for businesses engaged in cross-border digital trade, fostering a safe and secure online environment and contestable markets, and removing and preventing the emergence of unjustified barriers to digital trade, which have a detrimental impact on trade and investment flows.

share the understanding that in order to achieve these objectives, there is a need to cooperate and, where appropriate, coordinate their approaches on addressing measures that impose unjustified barriers to digital trade and growth of emerging technologies around the world.

confirm their common understanding of the following Digital Trade Principles as important means to achieve those objectives.

share the understanding that these Digital Trade Principles are not legally binding and are not intended to give rise to any rights or obligations under the respective domestic laws and regulations, or international law.

Digital Trade Facilitation

Paperless trading

To cut red tape and enable more businesses to trade, it is essential that governments and industry drive forward the digitisation of trade-related documents and processes, including through means of addressing legal, technical, and commercial barriers to the digitisation of paper processes.

In particular, the transition towards the use of forms and documents required for import, export, or transit of goods in data-based formats is important in order to create a paperless border environment for trade of goods.

The online publication of electronic forms issued or controlled by customs authorities and other government agencies for import, export, or transit of goods is an important element of this.

It is also important that customs authorities and other government agencies increasingly accept such forms and, as appropriate, supporting documents in electronic format, as the legal equivalent of the paper version of those documents.

The use of international standards and cooperation in international fora are important instruments to promote the use of electronic forms and documents required for import, export and transit, and thereby to facilitate trade in goods.

Where governments use digital systems for processing imports, exports, and goods in transit, it is important that such systems facilitate the flow of goods along the entirety of the supply chain.

Single windows

Single trade windows should be developed to streamline stakeholder interactions with border agencies. They should take into account common standards, with interoperability as a key goal, and in line with the best practice recommendations of the World Customs Organization.

Electronic Transactions Framework and Electronic Contracts

Maintaining a legal framework governing electronic transactions that is consistent with the principles of the UNCITRAL Model Law on Electronic Commerce (1996) is

indispensable to ensure legal certainty and predictability for businesses and consumers in the online environment.

The EU and Singapore should not put undue regulatory burden on electronic transactions and should facilitate input by interested persons in the development of the relevant legal framework for electronic transactions.

Electronic contracts are key enablers of any digital transaction. In order to provide businesses and consumers with legal certainty, and except in cases defined in domestic law, the legal effect, legal validity, or enforceability of an electronic contract, should not be denied solely on the basis that the contract has been made by electronic means.

Electronic authentication and electronic signatures

Electronic authentication and the use of electronic signatures facilitate digital transactions and make them more secure and efficient.

To enable digital transactions, it is key that electronic signatures are not denied legal effect, legal validity, or admissibility as evidence in legal proceedings solely on the basis that the signature is in electronic form.

The mutual recognition of electronic identities, including digital identity wallets, and digital signatures has a direct trade facilitating effect for businesses engaged in cross-border transactions and increases the connectivity of the economies.

Interoperability involves both the legal and regulatory frameworks supporting digital identities and the technical and architectural specifications and standards needed for implementing them.

These principles are equally important for electronic seals, electronic time stamps and electronic registered delivery services, should they exist in domestic law.

Electronic invoicing

The use of electronic invoices has a major trade facilitating effect in business-to-business, business-to-consumer and business-to-government transactions.

In order to facilitate cross-border digital trade, domestic measures related to electronic invoices should support cross-border interoperability and, where appropriate, build on existing international frameworks such as Peppol.

Cooperation in sharing best practices and promoting interoperable electronic invoicing frameworks in international fora has an important role to play in this context.

Electronic transferable records and freight transport information

Paper-based transactions, which still dominate international trade and transport, are a source of cost, delay, inefficiency, fraud, error and environmental impact. Replacing paper documents with electronic records and information exchanges will therefore generate efficiencies and economic savings.

To that end, it is important to develop appropriate legal frameworks to enable the use of electronic transferable records across borders, as well as the use of digital communication by businesses with authorities to facilitate freight transport, through the digitalisation of administrative procedures, including by supporting technical interoperability.

These legal frameworks should be consistent with the UNCITRAL Model Law on Electronic Transferable Records.

Dialogue on the design and implementation of the legal frameworks, sharing of best practices and solutions for the exchange of freight transport information and documents using electronic platforms, and cooperation to support ongoing work in relevant international fora on interoperability and the development of international standards for the use of new technologies in trade processes, will play an important role in this context.

Customs duties

The EU and Singapore emphasise the importance and high economic value of their commitment in the EU-Singapore Free Trade Agreement that prohibits the imposition of customs duties on electronic transmissions and support a permanent ban on customs duties on electronic transmissions in the World Trade Organization.

Standards, Technical Regulations and Conformity Assessment Procedures

The continued evolution of emerging technologies such as Artificial intelligence and blockchain and their applications in the digital economy calls for updates to cooperation mechanisms for standards, technical regulations and conformity assessment procedures (STRACAP). Furthermore, STRACAP are applicable to several mechanisms that underpin digital trade, such as paperless trading, electronic invoicing and electronic payments. Greater clarity on these STRACAP are important and contribute to the reduction of barriers to digital trade by increasing compatibility, interoperability, and reliability.

International standards for digital trade should be developed in a way that complies with the six principles of the WTO Technical Barriers to Trade Committee, namely transparency, openness, impartiality and consensus, effectiveness and relevance, coherence, and the development dimension. Such standards must continue to play an important role in supporting an open, free, and fair environment in the digital age.

Where available, international standards should also be used as the basis for technical regulations and conformity assessment procedures related to digital trade. Mechanisms which facilitate the cross-border recognition of conformity assessment results can support the digital economy and should be explored where viable. Information on technical regulations related to digital trade should be shared openly where appropriate.

Data Governance

Data free flow with trust

The EU and Singapore share the view that to support the trade of goods and services and for individuals and businesses to harness the opportunities of the digital economy, data should be able to flow freely across borders with trust, based on instruments for cross border data flows ensuring a high level of data protection and security.

It is indispensable that personal data is protected by high enforceable standards, including when it is transferred across borders. Cooperation on data protection should be strengthened, including enforcement cooperation between supervisory authorities.

At the same time, data localisation requirements are a serious cause for concern and should not be imposed unless they are justified by legitimate public policy objectives. It is therefore essential to address unjustified obstacles to cross border data flows, while preserving our policy and regulatory autonomy.

It is important to enhance cooperation on data governance, privacy and data protection. The EU and Singapore will work towards identifying commonalities, complementarities and elements of convergence between their regulatory approaches with a view to explore future interoperability to facilitate data to flow with trust.

Non-personal data should benefit from protection applicable under domestic law, such as intellectual property or the protection of trade secrets, including when it is transferred across borders.

The EU and Singapore share the understanding that it is essential to exchange information and seek to advance cooperation in areas including enhancing the trusted flow of data, privacy enhancing technologies, and identifying areas for industry and research collaboration.

The EU and Singapore share the view that the promotion of common principles for trusted government access to personal data held by the private sector helps to provide transparency and legal certainty and supports the transfer of data between jurisdictions by commercial entities, resulting in positive economic and social impacts.

Open government data

Open government data can play an important role in digital trade and in fostering economic and social development, competitiveness, and innovation. Therefore, there is value in expanding the coverage of open government data, such as through engagement and consultation with interested stakeholders. There are clear benefits to making data, the disclosure of which is not restricted under domestic law, which is held by any level of the government, digitally available for public access and use.

Where appropriate, government data should be made publicly available in an anonymized, open, interoperable and machine-readable format. The reproduction, redistribution, republishing, regrouping or the use of the data for commercial and non-commercial purposes should be facilitated.

Exchanging information and experiences on practices and policies has an important role to play in encouraging the development of digital trade and creating business opportunities, especially for small and medium-sized enterprises.

Consumer trust

Online consumer protection

Effective measures are needed to ensure a high level of consumer protection when purchasing goods and services online.

In order to enhance consumer confidence and trust in digital trade, it is necessary to ensure that domestic law proscribes misleading, fraudulent and deceptive commercial activities that cause harm, or potential harm, to consumers engaged in digital transactions.

To protect consumers in the online environment, it is important that suppliers of goods and services deal fairly and honestly with consumers, that they provide complete, accurate, and transparent information on goods and services, including any terms and conditions of purchase; and that they ensure the safety of goods and, where applicable, services, during normal or reasonably foreseeable use. Consumers should be provided with meaningful access to fair, transparent and effective mechanisms to resolve disputes with suppliers of goods and services related to digital transactions and obtain redress, as appropriate.

Overall, the level of protection of consumers who are engaged in digital transactions should not be less than that is afforded to consumers who are engaged in other forms of commerce.

In the case of cross-border transactions, cooperation between national authorities, consumer protection agencies and other relevant entities, including through the exchange of information and experience, is important to protect consumers in the online environment and to combat illegal, non-compliant or counterfeit products.

Unsolicited commercial electronic messages

Transparent and effective measures that limit unsolicited commercial electronic messages have an important role to play in promoting confidence and trust in electronic commerce.

Accordingly, it is necessary to ensure that senders of commercial electronic messages either obtain the consent of recipients to receive commercial electronic messages; or facilitate the ability of recipients to prevent ongoing reception of those messages, as specified in domestic laws and regulations.

In order to protect the recipients, commercial electronic messages should be clearly identifiable as such, clearly disclose on whose behalf they are sent, and contain the necessary information to enable recipients to request cessation free of charge and at any time.

The recipients should have the right to redress against suppliers of unsolicited commercial electronic messages.

It is important to develop a global and coordinated approach to address unsolicited commercial electronic messaging. The EU and Singapore share the understanding that it is essential to cooperate in appropriate cases of mutual concern regarding the regulation of unsolicited commercial electronic messages.

Safety online

A safe and secure online environment supports the digital economy by protecting users from illegal or harmful content and creating a sphere where businesses, innovation and creativity can thrive.

Multilateral cooperation among governments (including in international fora) as well as working with technology service providers and users are key to address online harms.

Business trust

Open internet access

As the bedrock of a thriving and innovative digital economy, the internet must be open, free, and secure.

End-users greatly benefit from the ability to access and use services and applications of their choice available on the internet subject to reasonable network management which does not block or slow down traffic for competitive advantage¹, and to connect the devices of their choice to the Internet, provided that such devices do not harm the network, and to access transparent and clear information on the network management practices of their internet access service supplier.

Cybersecurity

¹ The EU and Singapore recognise that an Internet access service supplier that offers its subscribers certain content on an exclusive basis would not be acting in contrary to this principle.

Businesses need a secure digital trading environment, with the highest standards of cybersecurity and resilience against illicit or malicious activity.

Cybersecurity incidents and threats undermine confidence in digital trade and have a detrimental effect on trust in the online environment.

In order to prevent or mitigate those incidents and threats and thereby facilitate digital trade, it is important to build domestic capabilities for cybersecurity incident response and to promote information exchange and cooperation. This should be done both at bilateral level and in international fora in line with the Digital Partnership, in order to identify and mitigate malicious activities, including intrusions or dissemination of malicious code that affect electronic networks.

As risk-based approaches are generally more effective in addressing these threats and minimising trade barriers, businesses should be encouraged to use such approaches that rely on open, transparent and consensus-based standards as well as risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity incidents.

Source code

To ensure that consumers and businesses can benefit from digital innovation, effective and balanced intellectual property frameworks should be maintained, with protections for trade secrets.

Businesses should not be required or coerced to transfer technology, in particular to transfer or provide access to source code as a condition for the import, distribution, sale, or use of that software, or of products containing that software.

At the same time, public authorities should retain sufficient flexibility to obtain the transfer of or access to source code, when pursuing legitimate public policy objectives, subject to safeguards against unauthorised disclosure.

ICT products that use cryptography

Encryption technologies have an important role in supporting digital trade by protecting confidentiality and security of data. With encryption utilised in most commonly used and globally traded Information and Communication Technology (ICT) products, discriminatory and restrictive policies could put digital trade and the large trade in ICT products at risk.

Therefore, as a condition of the manufacture, sale, distribution, import or use of an ICT product, businesses should not be required or coerced to transfer or provide access to encryption keys or any proprietary information relating to cryptography; partner or create joint ventures with local businesses; or use or integrate a particular cryptographic algorithm or cipher.

At the same time, public authorities should retain sufficient flexibility to request the manufacturer or supplier of an ICT product to transfer or provide access to any information that is necessary to pursue in a proportionate way legitimate public policy objectives including health and safety, subject to safeguards against unauthorised disclosure.

Artificial Intelligence

The use and adoption of Artificial Intelligence (AI) technologies offers significant social and economy benefits to people and businesses. To fully realise the benefits of AI, it is important to develop ethical governance frameworks for the trusted, safe and responsible use of AI technologies.

These frameworks should take into consideration internationally-recognised principles (such as those developed by the OECD) or guidelines, so that the AI technologies may be adopted, used and incorporated in a consistent manner.

Cooperation on digital trade

The EU and Singapore recognise the benefit of greater cooperation and sharing on regulatory matters affecting digital trade, given the fast-paced and evolving nature of the digital economy. The EU and Singapore support the establishment of an enabling environment that facilitates digital trade, including regulatory framework, norms and standards to foster the development of a human-centric digital economy and society.

Businesses and people will benefit from participating in the digital economy, and can make significant contributions to its development. As some individuals and groups such as women and low socio-economic groups disproportionately face barriers to participating in the digital economy, it is essential for governments to identify and address these barriers, improve digital skills and access to online business tools, and promote inclusive and sustainable economic growth.

Micro, Small and Medium Enterprises (MSMEs) play a particularly fundamental role in maintaining dynamism and enhancing competitiveness in the digital economy. The EU and Singapore support a digital trade framework conducive to MSMEs' continued adaptation to the digital economy, by leveraging digital tools to improve their capabilities and market reach, access capital and credit, participate in government procurement opportunities, and access platforms that link them with international suppliers, buyers, and other potential business partners.

The EU and Singapore share the assessment that digital and telecommunications markets should be open, competitive, transparent, fair, and free of unjustified barriers to international trade and investment.

The EU and Singapore therefore support the development of a coordinated approach towards such barriers. To facilitate this coordination, they share the understanding for the

need to establish a relevant point of contact in the Directorate General for Trade of the European Commission and the Ministry of Trade and Industry Singapore.

The EU and Singapore recognize the fast evolving nature of digital technologies and digital trade may require that these Digital Trade Principles are adapted in the future and affirm their commitment to cooperation on matters relating to digital trade and, building on these Principles, to explore the deepening of their bilateral relations with respect to digital trade, including on digital trade rules.