



BUSINESSEUROPE VIEWS ON DIGITAL TRADE





June 2023

BusinessEurope Views on Digital Trade

KEY MESSAGES

- i. Free cross border data flow along with adequate protection of personal data, intellectual property rights and trade secrets (“data flow with trust”) is key for the competitiveness of all companies, regardless of their size and sector of activity. In the absence of a multilateral framework on digital trade, growing regulatory divergence is taking place and resulting in the fragmentation of international digital markets. The proliferation of regulations is eroding the competitiveness of companies, especially of small and medium-sized companies, which have more difficulties to adapt to different digital regulatory frameworks. Europe accounts for more than half of global exports of digitally delivered services.
- ii. The rules agreed in the digital trade chapter of the EU-UK Trade Cooperation Agreement (TCA) should represent the main reference in the negotiations of any trade agreement.
- iii. Free cross border data flows, the prohibition of forced data localization and the prohibition of mandatory disclosure or transfer of source code and algorithms, together with the appropriate protection of personal data, represent the backbone of any digital agreement or chapter. Exceptions to this rule (or principle) must be limited to the necessary to ensure that they do not set international precedents in this area.
- iv. Digital agreements or chapters should also include provisions related to the non-discrimination of services or goods provided by electronic means, the prohibition of forced transfer of technology, trade facilitation (electronic contracts, electronic signatures), consumer protection and open government data and appropriate instruments to ensure technical interoperability and common standards. They could also lay the ground for an open digital architecture and a trustworthy digital ecosystem.
- v. The conclusion of the negotiations on the WTO-World Trade Organisation Joint Initiative on e-commerce and the extension of the Moratorium on Customs Duties on Electronic Transmissions should be a priority in the negotiation agenda of the European Commission.
- vi. Bilateral trade agreements without relevant provisions on digital trade, should be reinforced with an appropriate digital trade agreement.
- vii. Impact assessments of any European piece of legislation on digitalization must analyse the consequences of such initiatives on trade and investments, as well as on the competitiveness of European businesses outside the EU.

- viii.** Regulatory convergence must be partnered with efforts to improve interoperability and pave the way to private investments in digital infrastructure to reduce the digital divide. The 'Global Gateway' must be used to help adopting adequate regulatory frameworks to incentivize the mobilization of private investments needed to expand safe and accessible internet coverage for all. Joint initiatives with other countries are encouraged to increase the impact of such projects.
- ix.** A timely and more extended stakeholder participation is key to develop ambitious and clear legislation in the digital trade sphere.



BusinessEurope's Views on Digital Trade

1. Introduction

The process of digitalization, meaning the continued integration of digital technologies and digitized data across the economy and society, is strongly influencing international trade in scale, scope, and speed. Within its main advantages, it allows companies the possibility to offer new products and services to a larger number of digitally connected customers; enables enterprises, especially SMEs, to use digital tools to overcome barriers to growth; and has altered the way we trade goods through digital platforms. Digital trade in particular influences the global economy and every company regardless of its activity and size. Digitalization not only fosters the global economy's growth potential, but also offers worldwide citizens the possibilities for improving the efficiency of their day-to-day activities and needs: digital tools are now available in a wide variety of formats, ranging from the purpose of looking after one's health and enabling prevention to the improvement of educational and training systems towards greater research and innovation.

Digital and green transitions are deeply interrelated. Digitalization and telecommunication networks play a critical role in Europe's green transition by enabling companies across all sectors to reach their sustainability targets. They help to optimize the use of energy and natural resources, as well as to reduce the greenhouse emissions in transport, industry, and cities.

Furthermore, digitalization strengthens the current trend of 'servicification,' whereby there is an increase in the use, production, and sale of services¹. Digitalization, and the internet in particular, have made it possible that services, such as legal, engineering, computer-related and financial services can now be provided totally or partially online.

The digital era has also enabled platforms in the business ecosystem that facilitate cooperation among customers, partners, and contractors in striving towards innovation and productivity. Data is also the backbone of new service models, such as cloud computing, the Internet of Things (IoT), Artificial Intelligence (AI) and additive manufacturing. The diverse ways in which digitalization interacts with trade adds complexity to find a clear definition, blurring the already grey distinctions between goods and services.

¹ Miroudot, S., *The Servicification of Global Value Chains: Evidence and Policy Implications* (UNCTAD, 2017), p.1. <https://unctad.org/system/files/non-official-document/c1mem5_2017_124_S3_Miroudot_2.pdf>



Despite the challenge to find an all-accepted definition of **digital trade**, the definitional framework of the European Commission can be taken as a basis. It stipulates that digital trade refers to any commerce enabled by electronic means – by telecommunications and/or ICT services – that covers trade in both goods and services whether it is remunerated or not.

It is also relevant to distinguish between digital trade and e-commerce. On the one hand, **e-commerce** is circumscribed to the physical goods bought via digital platforms which are shipped overseas and passed through customs clearance into foreign markets. On the other hand, **digital trade** concerns the transfer of data, products, or services by electronic means. The connection between both terms resides in the fact that digital trade can play a role in e-commerce by facilitating the buying, selling, and servicing of physical goods and services.

For the time being, there is no methodology that can reflect and quantify the multifaceted nature of digital trade. The largest component of digitally deliverable services is the broad and varied category “other business services,” followed by “telecommunications, computer and information services.” However, the share of services that are delivered digitally is not distinguished yet.

This said, the most recent data of the WTO sheds light on the importance of digital trade². In this respect, global exports of digitally delivered services recorded an almost fourfold increase in value since 2005, rising 8.1% on average per year in the period 2005-2022, outpacing goods (5.6%) and other services exports (4.2%). While other services fell in this period, digitally delivered services exports continued to rise, reaching US\$ 3.82 trillion in 2022, and representing a 54% share in total global services exports. In 2022, business, professional, and technical services accounted for around 40% of digitally delivered services exports, followed by computer services (20%), financial services (16%), intellectual property related services (12%), insurance services (5%), telecommunications services (3%), audio-visual and other personal, cultural, and recreational services (3%), and information services (1%). Europe accounts for more than half of global exports of digitally delivered services. The five largest exporters in 2022 of digitally exported services were the US (632 billion), the United Kingdom (350 billion), Ireland (290 billion), Germany (227 billion) and India (227 billion).

² World Trade Organization – WTO, *Global Trade Outlook and Statistics, 2023*
<https://www.wto.org/english/res_e/publications_e/trade_outlook23_e.htm>



2. Barriers to digital trade

The reasons which lay behind the interest of governments to regulate digital trade are diverse. Governments may adopt measures to guarantee privacy and data protection; ensure data security within the boundaries of the country or region; secure access to information for regulatory control or audit purposes; allow security services to access and review data or protect sensitive information because of national security reasons; and encourage the digital domestic industry by polling national data. However, these regulations can have direct or indirect consequences that disrupt international digital trade. Amongst them, we can underline the following:

- **Data flow restrictions** take place whenever data flows are not allowed or are conditioned to ex- ante accountability, to safeguards or to ad hoc authorizations.
- **Mandatory data localization** can be achieved through mandatory legal or administrative requirements directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a specified jurisdiction.

There are different forms of data localization: a) data which must be stored but is not submitted to any flow restriction; b) data which must be stored, but the transfer or processing abroad is allowed under clearly defined conditions; c) data and processing which must be localized, and the transfer or processing is only accepted on an ad hoc basis. Forced localization can target personal data, non-personal data, or specific sectors.

For example, by 2021 there were, according to the OECD³, a total of ninety-two data localization measures in place across thirty-nine countries. Two-thirds of measures in place involved a storage requirement with a flow prohibition.

- **Requirements to disclose algorithms or other proprietary source code**, which involves organizations and companies transforming unintelligible data (encrypted data) to ensure its confidentiality to understandable data or to accede to the programming statements owned exclusively by companies that carefully guard knowledge about the technology or the product's inner workings. These measures can potentially cause infringement of the company's intellectual property rights.

³ Source: OECD, A Preliminary Mapping of Data Localisation Measures, 13 June 2022
<<https://www.oecd.org/digital/a-preliminary-mapping-of-data-localisation-measures-c5ca3fed-en.htm>>



- **Customs duties and related reporting on e-commerce and data flows.** For instance, despite the WTO e-commerce moratorium, Indonesia has imposed burdensome customs reporting requirements for intangible goods delivered via electronic transmission.
- **Barriers to Internet Services** entail inappropriate application of old regulatory regimes to new business models.
- **Other barriers**, which can potentially refer to divergent local regulation in respect to electronic authentication and signatures, internet domain names, digital products, electronic payment platforms, discriminatory testing requirements for hardware and software imports, and other discriminatory practices.

Market fragmentation emerges as a result of barriers to digital trade, where companies operating in multiple jurisdictions must align to different data flow legislations and/or are forced to localize the storage and even the processing of data in different countries. In addition, it leads to less interoperability, undermines the efficiency of global value chains, and finally erodes business competitiveness. This new reality is not only challenging for big companies across all sectors, but also small and medium-sized companies (SMEs) which also rely on international data flows for the supply of raw materials and components, the manufacturing of goods, logistics as well as the marketing of their products and services.

Another important barrier to digital trade is the lack of interoperability and of safe and accessible digital infrastructures. These barriers hinder millions of people and businesses, mostly from the informal sector, benefiting from digital trade. The OECD highlighted that in Africa 70% of young people live in rural areas, yet only 26% of those people have internet access. In Asia and Latin America, access in rural areas for the same demographic sits at 35% and 40%, respectively. Regulatory convergence must be partnered by better interoperability and the expansion of digital infrastructures to expand the opportunities offered by digital trade.

3. International regulatory landscape

In absence of rules to discipline digital trade, governments attempt to address trade restrictive measures at plurilateral and bilateral levels with different degrees of success.

a) Multilateral framework



Although the regulatory framework of the WTO has not adapted to the far-reaching consequences and opportunities of digitalization on international trade, the General Agreement on Trade in Services (GATS) remains an important piece of legislation for digitally enabled services. It provides general principles of most-favored-nation treatment (MFN), national treatment and transparency. Trade agreements also refer to article XIV of GATS dedicated to the justifications for trade restricting rules or article XX of GATT dedicated to exceptions.

Worth mentioning is also the Moratorium on Customs Duties on Electronic Transmissions, a statement agreed in 1998 and prolonged ever since on a temporary basis. The WTO members decided in the 12th Ministerial Conference (MC12) to uphold the moratorium until the celebration of the next Ministerial Conference MC13 in 2024. Nevertheless, certain countries including India, Indonesia and South Africa have indicated a desire to end the moratorium and to begin unilaterally imposing tariffs on cross-border data flows.

b) Joint Statement Initiative on e-commerce

Still under negotiation, the eighty-eight countries involved in the negotiations aim to reach a level playing field by agreeing a set of common rules across a range of electronic issues including enabling electronic commerce; promoting openness and trust in e-commerce; cross-cutting issues; telecommunications and market access for e-commerce firms.

At the end of 2022, convergence was achieved in paperless trading, electronic contracts, electronic authentication and electronic signatures, unsolicited commercial electronic messages, online consumer protection, open government data, open internet access, transparency, cybersecurity, and electronic transactions frameworks.

Other aspects remain open, such as privacy, cross-border data flows, data localization, source code, ban on customs duties on electronic transmissions and ICT products that use cryptography. Under the leadership of Australia, Japan and Singapore, WTO members agreed in January 2023 to target substantial conclusion of negotiations by the end of 2023.

c) Regional trade agreements

The example of the United States, Mexico, Canada Agreement (USCMA):
This agreement includes a chapter on digital trade (Chapter 19), which is



applicable to investments (Chapter 14), cross-border trade in services (Chapter 15) and financial services (Chapter 17).

Among the most relevant provisions mentioned in the digital trade chapter we should underpin the following ones: ban on custom duties, fees or other charges on the importation or exportation on electronic transmissions; the commitment to neither prohibit nor restrict the cross-border transfer of information, including personal information; the ban on forced location on computing facilities and the prohibition to require access to a source code for data transfer.

As far as the protection of personal data is concerned, the development of national legislations should take inspiration of principles and guidelines, such as the APEC Privacy and the OECD Recommendation concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal data (2013).

Another interesting aspect is the compromise that digital platforms are not liable for content posted by third parties and that they must remain free to delete postings by third parties. The preference to a risk-based approach is another element to be considered.

Other provisions refer to the non-discriminatory use of digital products; the consistency of the domestic frameworks to the principles of the UNCITRAL Model law on Electronic Commerce 1996; the electronic authentication and electronic signatures, the online consumer protection, the unsolicited commercial electronic communications; the government open data and the paperless administration. The digital chapter of USMCA is the most ambitious of all digital chapters negotiated by the US in its free trade agreements.

d) Bilateral agreements with the focus on the European Union

The **Trade and Cooperation Agreement with the UK** includes the most ambitious digital trade chapter of all agreements the EU has so far in vigor. Apart from imposing a ban on custom duties, the digital trade chapter includes exhaustive articles on ensuring cross-border data flows, and on the protection of personal data and privacy, the non-requirement of prior authorization of the provision of certain services by electronic means, the conclusion of contracts by electronic means; the electronic authentication and electronic trust services; the ban of not requiring the transfer of, or access to, the source code of software; the maintenance of measures to ensure the effective protection of consumers engaging in electronic commerce transactions; the protection of users against unsolicited direct marketing communications; the recognition that facilitating



public access to, and use of, government data contributes to stimulating economic and social development, competitiveness, productivity and innovation; the cooperation on regulatory issues with regard to digital trade; and the understanding on computer services.

Other **last generation EU free trade agreements with Singapore, Vietnam, Japan, or South Korea** do not include specific chapters on digital trade or e-commerce. They reaffirm the WTO principles, such as MFN and national treatment in cross border-services and include provisions on the supply of cross border services (Mode 1), which also comprises computer delivered services.

Complementing some of the FTAs already in place, the EU has signed **Digital Partnerships with Singapore, South Korea and Japan**. They can be extensive in scope, considering that they also include cooperation in cutting-edge technologies, cooperation in international organizations or joint projects.

Digital Partnerships might also be useful for regulatory purposes considering that both parties commit to digital trade principles. Although these principles are non-binding, they show a mutual understanding on key issues relevant to digital trade and a joint commitment to an open digital economy, free of unjustified barriers to international trade and they provide a common space for regulatory cooperation.

e) Unilateral mechanisms

The absence of a multilateral agreement and the non-existence of mutually agreed definitions and principles, as well as the growing divergence of national legislations, have led countries to adopt unilateral mechanisms that enable the transfer of certain types of data to countries outside the domestic territory under certain conditions.

Usually, unilateral mechanisms can serve to safeguard cross-border transfers of data, and these mechanisms can be grouped around two branches: open safeguards or pre-authorized safeguards.

The difference between these two mechanisms is that pre-authorized safeguards require some form of public sector approval before transfer, while open safeguards leave more discretion to the private sector as to how to safeguard the data being transferred.

The EU, which has become a frontrunner in the regulation of data privacy, has adopted the pre-authorized safeguards to ensure GDPR compliance in third countries.



This is achieved either by adopting an adequacy decision in respect to a third country's regulation or the use by the private user of standard contractual clauses (SCCs), which are pre-approved legal provisions for transferring personal data from the EU to the rest of the world in compliance with the EU's General Data Protection Regulation.

The European Commission has recognized equivalencies to a number of countries, including some with which it has free trade agreements, such as Canada, Japan, the Republic of Korea and the United Kingdom.

However, pre-authorized mechanisms, like standard contractual clauses (SCCs) can be challenged in the Court of Justice of the European Union (CJEU) as we can see in the case Schrems I, when the EU-US Data Protection Shield was invalidated because individuals were not offered guarantees in the US substantially equivalent to those required by EU law, or the Schrems II case, where the Privacy Shield Decision was invalidated on account of invasive US surveillance programs.

A new EU-US Data Privacy Framework on data flows was announced in March 2023. The European Commission launched the process to adopt an adequacy decision, which will foster trans-Atlantic data flows and address the concerns raised by the Court of Justice of the European Union in its Schrems II decision of July 2020. The proposal for a draft adequacy decision follows the signature of an Executive Order which introduces new binding safeguards in the US. It imposes limitations and safeguards on access to data by US intelligence agencies and establishes an independent and impartial redress mechanism to resolve complaints from Europeans concerning the collection of their data for national security purposes. It remains to be seen if the new Framework satisfies all the requirements in case of an appeal to the Court.

4. Recommendations

i. Digital Trade Principles

Trade agreements negotiated by the European Union, must:

1. Ban the imposition of customs **duties on electronic transmissions**.
2. Ensure **cross-border data flow** to facilitate trade in the digital economy. This implies that the signatory parties cannot require the use of computing facilities, nor force the localization in their respective territories; neither ban storage or



processing of data in the territory of the other Party making the cross-border transfer of data contingent upon the use of computing facilities or network elements in its territory and the signatory parties should not enforce similar onerous requirements which may aggravate cross-border data transfers within the signatory parties as per their local laws.

3. Clearly define the **general** and **security exception** applied to the **free flow of cross-border data**. For instance, we can refer to Article XX of GATT, which includes exceptions related to the protection of public morals or of human, animal or plant life or health to take a few examples. However, exceptions to protect public security or public morals or to maintain public order may be invoked only where a serious threat is posed to one of the fundamental interests of society.
4. Guarantee that the individuals have the right to the protection of **personal data and privacy**. High standards in this area contribute to trust in the digital economy and to the development of trade. Parties should be able to adopt or maintain measures for the protection of personal data and privacy, while at the same time providing instruments that ensure the adequate transfer of data.
5. **Prohibit in general the transfer or access to source code and algorithms** owned by a natural or legal person of the other Party.
6. Clearly define the cases where regulatory authorities, law enforcement, judicial or conformity assessment bodies can **access the source code, or an algorithm expressed in that source code**. Such exceptions should be limited to the necessary to ensure that the European Union does not set international precedents, which other countries could copy.
7. Ensure a **trustworthy digital ecosystem** and guarantee that business can operate based on a clear legal framework across borders. Governments and legislators should ensure that the policy and regulatory environments for data protection and data access are up-to-date and reflect the best practices in respect of privacy and security. The lack interoperability across jurisdictions can create administrative burdens and compliance inconsistencies, which limit the potential of the global digital economy.
8. Prohibit **forced technology transfer** by prohibiting Parties from requiring companies to transfer technology, Intellectual Property, trade secrets, production processes, or the preparatory information as a condition for accessing the market.



9. Promote the use of international standards and **adherence to WTO/TBT-Technical Barriers to Trade principles for international standards development.**
10. Encourage the widespread use of **high-performing, secure and energy efficient architectures to drive innovation in key technologies**, including semiconductors, cloud computing, AI and 5G/6G telecommunications and ensure, through technology neutral regulation that companies can choose their suppliers of choice, irrespective of where they are headquartered. The use of any architectures should not prevent interoperability, competition or limit the ability of companies and state-owned enterprises to use the most-effective, secure, and innovative technologies through regulatory technology specific mandates. At the same time, regulation should not make it more difficult for smaller and non-incumbent firms to be globally competitive.
11. **Provide non-discriminatory treatment to services**, service suppliers, and digital products of the other Party. New digital products and services should be protected against future discrimination, unless a specific, negotiated exception applies.
12. Build **confidence in data economy** by protecting innovation and encryption products that enhance security and privacy while allowing law enforcement access to communications consistent with applicable law.
13. Not prohibit or prevent the use of **electronic signatures** and facilitate **contracts by electronic means**. Only specific services should be excluded from electronic contracts based on a negative list. Authorities should not prevent or limit the **electronic authentication** and **electronic trust services**. Specific rules should also be introduced regarding electronic records to facilitate cross-border electronic transactions and to determine their probative force before courts and authorities of the signatory parties.
14. Adopt national measures to ensure transparent and effective **protection of consumers online** and limit **unsolicited direct marketing communications**.
15. Recognize **open government data by** facilitating public access to government data, which can stimulate economic and social development, competitiveness, productivity, and innovation.

**ii. Process**

1. The EU should engage **in the definition and interpretations of digital trade principles** with the United States of America within the Trade and Technological Council (TTC) and the rest of the like-minded members in the G7 and the OECD.

TTC, the G7 and the OECD should lay the ground for reaching a common understanding in the definition and interpretation of principles and exceptions to avoid further regulatory fragmentation and overcome the main stumbling blocks in the negotiations of free trade or digital agreements.

Although we are still waiting for the final adequacy decision by the European Commission to implement a new European Union-US data Privacy Framework between the EU and the US, the Executive Order signed by President Biden on October 7, 2022 ‘Enhancing Safeguard for United States Signals Intelligence Activities’, by which personal data and privacy protections are enhanced, could be used for reaching a common understanding on free data flows, personal data and privacy.

2. **In international statements and plurilateral digital agreements**, it is an absolute priority to reach a permanent **Moratorium on Electronic Transmissions** and to conclude the **Joint Agreement on E-commerce** where differences remain to overcome in respect to cross-border data flows, data localisation, and source code.
3. The EU should continue using **in bilateral free trade agreements** the strong wording it has started using since the EU-UK Trade and Cooperation Agreement. It must pursue an ambitious digital trade agreement with Japan and negotiate ambitious digital chapters, like the ones negotiated with the UK, Chile, and New Zealand, in the forthcoming bilateral trade agreements. The EU should consider reinforcing existing free trade agreements, custom unions, and economic partnership agreements with similar digital chapters.
4. **Regarding the Digital Partnerships** with e.g Japan and South Korea the EU should aim to complement the free trade agreements by opening the possibility to deepen collaboration in semiconductors, generation mobile networks, quantum and high-performance computing, artificial intelligence, beyond 5G/6G technologies, secure 5G, cybersecurity and skills. But they can also, like in the Digital Partnership with Singapore, open a dialogue on data flows and data innovation, digital trust, standards, and digital trade facilitation.



5. As regards **EU's domestic legislation**, the impact assessment that should precede any European legislative initiative in the digital field, should analyse the impact on trade and investment and the EU's international competitiveness.
6. Regulatory convergence must go in tandem with enhanced interoperability to pave the way to private investments in digital infrastructures and reduce the digital divide. The **Global Gateway** can enable the deployment of high capacity and robust Fixed, Mobile and Satellite Broadband Connectivity to reduce the digital divide and to allow businesses and communities to grow their competitiveness, quality of life, education, and economic prosperity. This should also include the promotion of policy measures to overcome barriers of entry and unlock the private investment needed to expand network coverage.
7. A timely and more extended **stakeholder participation** is key to develop ambitious and clear legislation in the digital trade sphere.

BUSINESSEUROPE



BusinessEurope is the leading advocate for growth and competitiveness at the European level, standing up for companies across the continent and campaigning on the issues that most influence their performance. A recognised social partner, we speak for all sized enterprises in 35 European countries whose national business federations are our direct members.



Austria



Belgium



Bulgaria



Croatia



Cyprus



Czech Republic



Denmark



Denmark



Estonia



Finland



France



Germany



Germany



Greece



Hungary



Iceland



Iceland



Ireland



Italy



Latvia



Lithuania



Luxembourg



Malta



Montenegro



Norway



Poland



Portugal



Rep. of San Marino



Romania



Serbia



Slovak Republic



Slovenia



Spain



Sweden



Switzerland



Switzerland



The Netherlands



Turkey



Turkey



United Kingdom



Avenue de Cortenbergh 168
B - 1000 Brussels, Belgium
Tel: +32(0)22376511 / Fax: +32(0)22311445
E-mail: main@businesseurope.eu

WWW.BUSINESSEUROPE.EU

EU Transparency Register 3978240953-79