Organisation for Economic Co-operation and Development

TAD/TC/WP(2020)14/FINAL

Unclassified **English - Or. English**

14 April 2021

TRADE AND AGRICULTURE DIRECTORATE
TRADE COMMITTEE

Cancels & replaces the same document of 13 April 2021

Working Party of the Trade Committee

Digital Trade Inventory

Pillar I: Rules, standards and principles

This paper was declassified by Delegations at the 16-17 March 2021 Working Party of the Trade Committee.

This work provides an overview of the rules, standards and principles that underpin the existing digital trade environment with a view to helping governments navigate the evolving policy landscape.

The work was prepared by Taku NEMOTO and Javier LOPEZ-GONZALEZ with research assistance from Alex WYCKOFF and Nasya DESIRIA. It also received useful comments and feedback from Andrea ANDRENELLI, Janos FERENCZ, Julia NIELSON, Irene OLIVAN-GARCIA, Silvia SORESCU and Susan STONE. The paper was also shared with STI.

The work is foreseen under Output Area 3.1.1.1.4 (Digital trade, emerging measures and new technologies) of the 2019-20 PWB. It is entirely funded by a voluntary contribution from the Government of Japan.

The work will be published as an OECD Trade Policy Paper

Contacts: Taku NEMOTO (Taku.NEMOTO@oecd.org) and Javier LOPEZ-GONZALEZ (Javier.LOPEZGONZALEZ@oecd.org)

JT03474738

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Table of contents

1. Why an Inventory? 5

2. What does the Inventory cover? 6

3. What does the Inventory tell us about specific issues? 8
- 3.1. Facilitating electronic transactions 8
- 3.2. Non-discrimination and liability 13
- 3.3. Consumer protection 14
- 3.4. Digital facilitation and logistics 15
- 3.5. Privacy: Protection of personal information/privacy 18
- 3.6. Flow of information 19
- 3.7. Cybersecurity 21
- 3.8. Telecoms: Updating the WTO Telecommunications Reference Paper 22
- 3.9. Customs duties: Customs duties on electronic transmissions 23
- 3.10. Access to internet and data 23
- 3.11. Business trust 25
- 3.12. Market Access 26

4. What does this mean for the evolving digital trade environment? 27
- 4.1. Development and spread of international rules 29
- 4.2. RTAs' contribution to development of rules 32

5. Conclusion 33

References 35

Annex A: Inventory of the rules, principles and standards relevant for digital trade 38
- 1. Facilitating electronic transactions 38
- 2. Non-discrimination and liability 51
- 3. Consumer protection 53
- 4. Digital trade facilitation and logistics 58
- 5. Privacy: Protection of personal information/privacy 68
- 6. Flow of Information 72
- 7. Cybersecurity 78
- 8. Telecoms: Updating the telecommunications reference paper 83
- 9. Customs duties; Customs duties on electronic transmissions 84
- 10. Access to internet and data 85
- 11. Business trust 89
- 12. Market Access 92

Annex B: Country breakdown 94

Annex C: Supporting Tables 95

Tables

Table 2.1. Issues covered in the Inventory 7
Table 3.1. Half of WTO Members have signed, ratified or been influenced by the UN Communication Convention or Model Law on Electronic Commerce 10
Table 3.2 Many jurisdictions are influenced by UNCITRAL instruments on e-authentication and e-signatures 12
Table 3.3. Privacy protection instruments have been widely developed in multiple international fora 19
Table 3.4. Spread of cybersecurity rules 22
Table 4.1. The Inventory covers a wide variety of rules developed in many different fora 27
Table 4.2. Many jurisdictions are now influenced by international instruments on electronic transaction frameworks and privacy protection 31
Table 4.3. Impacts of international instruments increase through being referenced by others 31

Figures

Figure 4.1. Adherence to international instruments varies widely 30
Figure 4.2. A wide variety of fora establish a different array of rules 32
Figure 4.3. RTAs have wide-ranging coverage 33

Boxes

Box 1. Examples of RTA provisions on electronic transaction framework 40
Box 2. Examples of RTA provisions on e-authentication and e-signatures 46
Box 3. Example of RTA provisions on electronic invoice 48
Box 4. Example of RTA provisions on e-payment 50
Box 5. Example of RTA provisions on non-discriminatory treatment of digital products 51
Box 6. Example of RTA provisions on interactive computer service 52
Box 7. Example of RTA provisions on consumer protection 55
Box 8. Example of RTA provisions on unsolicited commercial electronic messages 57
Box 9. Example of RTA provisions on paperless trading 61
Box 10. Example of RTA provisions on Electronic transferrable records 63
Box 11. Example of RTA provisions on customs procedures 66
Box 12. Example of RTA provisions on *de minimis* 67
Box 13. Example of RTA provisions on privacy 70
Box 14. Example of RTA provisions on cross-border transfer of information by electronic means 75
Box 15. Examples of RTA provisions on location of computing facilities 76
Box 16. Examples of RTA provisions on location of financial computing facilities 77
Box 17. Examples of RTA provisions on cybersecurity 82
Box 18. Examples of RTA provisions on customs duties on electronic transactions 85
Box 19. Examples of RTA provisions on open government data 86
Box 20. Example of RTA provisions on Access to the Internet 87
Box 21. Example of RTA provisions on Competition 88
Box 22. Examples of RTA provisions on Source code 89
Box 23. Example of RTA provisions on *ICT Products that Use Cryptography* 91

Key messages

This work provides an **overview of the rules, standards and principles that underpin the existing digital trade environment** with a view to helping governments navigate the evolving policy landscape. The scope of the Inventory reflects the issues under discussion at the WTO Joint Statement Initiative (JSI). For each of these issues, the Inventory documents relevant international instruments. The main findings from this exercise are:

- **The evolving regulatory landscape for digital trade is complex:** issues are discussed in various fora and touch upon many policy areas (from consumer protection, to the facilitation of electronic transactions, to cybersecurity and privacy). **The Inventory identifies 52 instruments that are directly relevant to digital trade in 24 different fora.** These instruments touch upon different issues according to the remit and membership of the institutions in which they are discussed. **Beyond the WTO, the OECD, ISO/IEC, UNECE/UNCEFACT and UNCITRAL each provide at least 4 relevant instruments**.
- Currently, **the strongest consensus exists in relation to trade facilitation, telecommunications, and goods market access for ICT products (reflecting progress at the WTO)**. There is also wide consensus on issues related to electronic transactions, where UNCITRAL instruments have had substantial influence across both JSI and non JSI participants.
- There is **a high degree of complementarity between different international instruments** which often cross-reference each other. For example, UN guidelines for Consumer Protection in E-commerce cite the OECD Recommendations on Consumer Protection. At the same time, trade agreements often reference tools including UNCITRAL, the APEC CBPR or the OECD Privacy Guidelines.
- **Regional Trade Agreements (RTAs) have played an important role in developing rules for digital trade**. Facilitating electronic transactions, which includes specific provisions on e-transaction frameworks, e-authentication and e-signatures, is the area that is most commonly covered. That said, in terms of specific provisions, protection of personal information, consumer protection, unsolicited electronic messages (spam) and customs duties on electronic transactions appear most frequently in RTAs, albeit with different levels of binding commitments.
- Overall, this Inventory reveals that **there is already substantial uptake of instruments on issues related to digital trade among JSI participants**. At the same time, **many non-JSI participants are also already in the process of undertaking reforms in some of these areas**. This Inventory shows that there is a solid basis of international instruments upon which the JSI discussions can build, and suggests that for non-JSI participants their existing and continuing efforts could facilitate eventual participation in the JSI.

It is hoped that the transparency exercise represented by this Inventory will provide a common basis of understanding so that countries can better leverage their resources towards enabling more informed discussions on digital trade whether at the WTO, or other international organisations, or in developing relevant domestic policies.

1. Why an Inventory?

1. Digitalisation provides a range of new opportunities for countries to benefit from trade (López González and Ferencz, 2018[1]) and even tackle some of the consequences of COVID-19 (OECD, 2020[2]). However, the benefits of digitalisation for trade, and of trade for digitalisation, are not automatic. They require a regulatory environment that enables cross-border digital transactions and allows governments to respond to the new challenges raised by digitalisation.

2. Existing multilateral rules and agreements under the World Trade Organisation (WTO) cover important aspects of the regulatory environment that underpins digital trade in goods and services. Indeed, the General Agreement on Trade in Services (GATS) and its annexes remain of primary importance for enabling trade in the services that underpin trade in the digital era. The General Agreement on Tariffs and Trade (GATT) and the Trade Facilitation Agreement (TFA) also cover many issues that support and facilitate trade in digitally ordered goods (López González and Jouanjean, 2017[3]).

3. However, there is an emerging view that international rules need to be updated to fully account for the issues arising for trade in the digital era. This is why a group of now 86 WTO Members have begun discussions on "trade-related aspects of electronic commerce" under the Joint Statement Initiative (JSI). These discussions touch on a diverse set of issues, including: cybersecurity, privacy, business trust, transparency, consumer protection and other matters deemed important for digital trade. Some of these issues are at the intersection of domestic policy-making and trade policy, with important implications for the consistency of different policy and rule-making efforts.

4. At the same time, regulation affecting digital trade is unfolding across a range of fora. Regional trade agreements (RTAs), such as the United States Mexico Canada Agreement (USMCA), the EU-Japan Economic Partnership Agreement (EU-Japan EPA) and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), increasingly include provisions related to trade in the digital era (See (Burri and Polanco, 2020[4]) (Monteiro and Teh, 2017[5]), and (Wu, 2017[6])). Moreover, rules, principles and standards related to digital trade, including on issues such as, electronic transactions, consumer protection, trade facilitation or telecommunications, are also the subject of deliberation in other international organisations such as the UN and UN agencies, the World Customs Organisation (WCO), the OECD and other regional institutions and international standard setting bodies.

5. The complexity of the issues and the diversity of the fora involved in these discussions underscores the need for greater transparency and visibility. Against this backdrop, the aim of this first pillar of the *Digital Trade Inventory Project* is to provide an account of existing rules, principles and standards that are of importance for digital trade. This pillar comprises three elements. The first is contained in the body of this paper, and provides an analysis of the issues covered by the Inventory. The second is the Inventory itself, which consists of a list of rules, principles and standards, with examples of language used and references to specific texts (Annex A). The third element is a matrix identifying which country adheres to which rule or principle (Annex B). It is hoped that this transparency exercise will provide a common basis of understanding so that countries can better leverage their resources towards enabling more informed discussions on digital trade whether at the WTO, or other international organisations, or in developing relevant domestic policies.

6. This report is divided into 5 parts. The next section discusses the criteria used to identify the issues and organisations that are the subject of the Inventory. Section 3 then provides an overview of the main findings of the Inventory, including a broad discussion of the issues at stake and the organisations where these are being discussed. Section 4 undertakes a meta-analysis, identifying the participation of countries in different discussions around the globe. Section 5 provides observations stemming from this exercise and discusses ways forward for this work. The Inventory listing the different rules, principles and standards identified is found in Annex A while the jurisdictions that have ratified, signed, committed to or adhered to the identified rules are listed in Annex B.

7. This work falls under Pillar I of the Digital Trade Inventory Project [TAD/TC/WP(2020)1].[1] The overall project seeks to provide greater transparency on the issues which are of importance to digital trade and to help countries leverage their resources for more informed discussions on digital trade. This report, provides an overview of the findings from work undertaken under Pillar I, which looks at different rules, principles and standards that are important for digital trade and where they are being discussed. It provides a simplified Inventory of a complex and evolving environment, drawing on publicly available information. The issues covered by the Inventory reflect the headings discussed at the WTO's Joint Statement Initiative. This is without prejudice to other issues also being considered as important in this space (e.g. intellectual property rights or digital services taxes). This exercise does not aim to evaluate progress at the WTO, nor does it seek to suggest priorities. It is simply a transparency exercise aimed at facilitating international discussions.

2. What does the Inventory cover?

8. The topics covered in this Inventory are based on the issues identified by WTO Members as important in their discussions on e-commerce at the Joint Statement Initiative, which 86 WTO Members (hereinafter called "JSI participants") have joined (Table 2.1.).[2] This means that the Inventory contains items that reflect a broad consensus on the areas that might be of importance for international discussions on rule-making for digital trade (without prejudice to other issues also being important).

9. The Inventory covers a range of rules, principles and standards (hereinafter collectively called "rules") focusing mainly on efforts underway outside the WTO to inform progress in the areas under discussion at the WTO and in other fora. For instance, on frameworks for electronic transactions, the Inventory provides an overview of what these entail and points to relevant texts in United Nations Commission on International Trade Law (UNCITRAL) and related rules developed in other fora. As such, it is meant to be a resource for governments to get a snapshot of the various initiatives underway under the broad heading of digital trade.

---

[1] The Digital Trade Inventory Project comprises 4 Pillars. This first pillar will be followed by work on a second pillar that provides a more detailed Inventory of existing debates on selected key issues relevant to digital trade. Pillar 3 will convene an event to discuss the emerging findings from the Project across a range of stakeholders and Pillar 4 will provide a deep-dive on cross-border data flows (see [TAD/TC/WP(2020)15]).

[2] As of 23 October 2020. They are: Albania; Argentina; Australia; Austria; Bahrain; Belgium; Benin; Brazil; Brunei Darussalam; Bulgaria; Burkina Faso; Cameroon; Canada; Chile; People's Republic of China (hereafter referred to as China); Colombia; Costa Rica; Côte d'Ivoire; Croatia; Cyprus; Czech Republic; Denmark; Ecuador, El Salvador; Estonia; Finland; France; Georgia; Germany; Greece; Guatemala; Honduras; Hong Kong (China); Hungary; Iceland; Indonesia; Ireland; Israel; Italy; Japan; Kazakhstan; Kenya; Korea; Kuwait; Lao People's Democratic Republic; Latvia; Liechtenstein; Lithuania; Luxembourg; Malaysia; Malta; Mexico; Republic of Moldova; Mongolia; Montenegro; Myanmar; Netherlands; New Zealand; Nicaragua; Nigeria; Republic of North Macedonia; Norway; Panama; Paraguay; Peru; Philippines; Poland; Portugal; Qatar; Romania; Russian Federation; Saudi Arabia; Singapore; Slovak Republic; Slovenia; Spain; Sweden; Switzerland; Chinese Taipei; Thailand; Turkey; Ukraine; United Arab Emirates; United Kingdom; United States; Uruguay.

Note by Turkey: The information in this document with reference to "Cyprus" relates to the southern part of the Island. There is no single authority representing both Turkish and Greek Cypriot people on the Island. Turkey recognises the Turkish Republic of Northern Cyprus (TRNC). Until a lasting and equitable solution is found within the context of the United Nations, Turkey shall preserve its position concerning the "Cyprus issue".

Note by all the European Union Member States of the OECD and the European Union: The Republic of Cyprus is recognised by all members of the United Nations with the exception of Turkey. The information in this document relates to the area under the effective control of the Government of the Republic of Cyprus.

10. The Inventory covers issues discussed across different international settings. They vary widely in terms of organisations (e.g., global or regional, intergovernmental or non-governmental) and issues (e.g., broad principles or more detailed standards, regulatory rules or technical rules, legally binding or non-binding).[3] The aim is to highlight progress being made across different fora and not to validate or justify where and how discussions should take place.

11. The Inventory includes a broad range of rules in the areas detailed in Table 2.1,[4] and is up to date as of 1st of October 2020.[5]

Table 2.1. Issues covered in the Inventory

Broad Area	Specific area
Facilitating electronic transactions	Electronic transaction frameworks
	E-authentication and e-signatures
	Electronic contracts
	Electronic invoicing
	Facilitation of e-payments
Non-discrimination and liability	Non-discriminatory treatment of digital products
	Interactive computer services (limiting non-IP liability for suppliers and users and infringement of persons' rights)
Consumer protection	Online consumer protection
	Unsolicited commercial electronic messages/spam
Privacy	Protection of personal information/privacy
Digital trade facilitation and logistics	Paperless trading
	Electronic transferrable records
	Customs procedures
	De minimis
Flow of Information[6]	Cross-border transfer of information by electronic means
	Location of computing facilities
	Location of financial computing facilities
Cybersecurity	Cybersecurity
Telecoms	Updating the telecommunications reference paper
Customs duties	Customs duties on electronic transmissions
Access to internet and data	Open government data
	Access to the internet
	Access to online platforms/competition
Business trust	Source code
	ICT products that use cryptography
Market Access	Services market access
	Goods market access

Source: Authors' elaboration from agenda of discussions at the WTO Joint Statement Initiative in 2019.
Note: This table does not include all the issues discussed at the JSI. For instance, it does not cover transparency and cooperation. While these are issues of great importance in the WTO discussions, they are more general in nature and it is more difficult to draw parallels on these issues across different organisations.

[3] The characteristics and nature of the rules exemplified here are not exclusive to each other. For instance, a certain international instrument could include both regulatory principles and detailed regulatory standards. A particular organisation could also establish both regulatory principles and technical standards in different settings.

[4] While principles in General Agreement on Tariffs and Trade (GATT) and General Agreement on Trade in Services (GATS) would apply when goods or services related to each issue are traded or provided internationally (e.g., e-invoicing services or e-payment services), those fundamental agreements are not listed individually again in each section.

[5] The Inventory in this paper is up to date as of the 1st of October 2020 (unless otherwise specified) and relies on publicly available information. Continued updating thereafter will be contingent on Members' interest and subject to voluntary contributions.

[6] This includes flow of all types of information, including personal and non-personal.

12. Digital provisions in regional trade agreements are analysed using the Trade Agreements Provisions on Electronic-commerce and Data (TAPED) dataset (Burri and Polanco, 2020[4]) (without prejudice to the legal status of each agreement).[7] The Inventory also provides examples of specific provisions in particular areas across major trade agreements such as the USMCA, the EU-Japan EPA and the CPTPP, and recently developed digital trade agreements, such as The Digital Economy Partnership Agreement between Singapore, Chile and New Zealand (DEPA), ASEAN Agreement on Electronic Commerce (ASEAN E-commerce agreement) and Singapore-Australia Digital Economy Agreement (SADEA) – these are collectively referred to as "RTAs".

13. This Inventory exercise has been undertaken to provide greater transparency on i) the areas that see more development of rules and principles; ii) the rules that are more widely used; and iii) the forums that are most active across the different issues identified. Once approved by the Working Party, this Inventory could be entirely accessed through online tools.

3. What does the Inventory tell us about specific issues?

14. In this digital era, international trade transactions have become more numerous and complex and involve a combination of goods, services and data crossing different borders. This means that ensuring that benefits from these flows are reaped and mitigating associated challenges requires new ways of thinking about market openness (López González and Ferencz, 2018[1]) (Casalini, López González and Moïsé, 2019[7]). Trade today must not only be faster and more reliable, but must also meet a range of regulatory requirements that differ across markets, including issues such as privacy, consumer protection and cybersecurity.

15. Against this backdrop, the *Digital Trade Inventory* aims to provide some clarity and transparency as to developments on the more cross-cutting issues discussed under the WTO JSI. An overview of each broad area as listed in Table 2.1 is provided below, with a more comprehensive analysis detailed in the Annex A.

3.1. Facilitating electronic transactions

16. Electronic-authentication, e-signatures, e-contracts, e-invoices and e-payments have enabled a growing number of transactions to take place online. These have become especially important in the context of physical distancing during COVID-19, enabling speedier processes, including at the border, and decreasing the need for physical interaction (OECD, 2020[8]).

17. However, it is often the case that these technologies are not effectively supported by domestic law. Additionally, domestic laws and regulations governing e-transactions might not always be internationally harmonised or interoperable. In order to promote the adoption and use of the technologies that facilitate electronic transactions in the context of digital trade, discussions in a number of fora have focused on a range of regulatory principles with a view to achieving a common understanding of what the key issues for regulation might be.

[7]The Inventory exercise relies on the TAPED dataset and Codebook updated on the 8th of June 2020, which does not include most recent RTAs such as Regional Comprehensive Economic Partnership (RCEP) or the Japan-UK Comprehensive Economic Partnership Agreement (Japan-UK CEPA). The data was accessed on the 12th of October 2020 at the following link https://www.unilu.ch/en/faculties/faculty-of-law/professorships/managing-director-internationalisation/research/taped/.
It is worth noting that there are gaps between the TAPED dataset and the WTO RTA database. The analysis herein is without prejudice to the legal status of each agreement.

18. In this area, the United Nations Commission on International Trade Law (UNCITRAL) has played a foundational role in establishing regulatory rules and principles for e-transaction frameworks, e-authentication and e-signature and electronic contracts, while progress remains to be made on electronic invoices and electronic payments. At the same time, as the Inventory shows, ISO standards have also contributed to the development of technical standards for these technologies.

3.1.1. Electronic transaction frameworks

19. Electronic transaction frameworks refer to overarching legal frameworks providing key principles governing electronic transactions. On a global scale, UNCITRAL has played a leading role, establishing the legally-binding **United Nations Convention on the Use of Electronic Communications in International Contracts (UN Electronic Communications Convention)** and non-binding **UNCITRAL Model Law on Electronic Commerce (MLEC)**. These instruments promote harmonisation or unification of domestic laws and regulations on e-commerce transactions. The Convention and the Model law provide three fundamental principles for e-commerce legislation: non-discrimination, technological neutrality and functional equivalence between electronic communications and paper documents. The Inventory reveals that while 74 jurisdictions (including 31 JSI participants) have enacted domestic legislation based on or influenced by the MLEC, only 26 jurisdictions have signed or ratified the UN Electronic Communications Convention.

20. The principles included in the Convention as well as the Model Law, have been introduced into domestic legislation through **RTAs**. Overall, 15 jurisdictions (12 JSI participants) have signed RTAs explicitly referencing the Convention and 22 jurisdictions (19 JSI participants) have signed RTAs referencing the Model law. For instance, the **CPTPP** requires that a domestic legal framework governing electronic transactions be consistent with the principles of the Convention or the Model law. As a result, at least 91 jurisdictions (including 41 JSI participants) have ratified, signed or referenced either or both of those UN instruments (Table 3.1). Furthermore, some agreements, such as the **ASEAN E-commerce agreement**, require its members to maintain or adopt laws and regulations governing electronic transactions taking into account applicable international conventions or model laws relating to e-commerce, although without further specification. This implies that more jurisdictions than those that are currently recorded are likely to have been influenced by the Convention or the Model law.

21. RTAs not only reference the UN Electronic Communication Convention and MLEC but can also contain rules on technological neutrality and unnecessary barriers to e-commerce as a part of their electronic transaction framework. There are 50 jurisdictions (50 JSI participants) that have signed RTAs that include the principle of technological neutrality, one of the three fundamental principles of the Convention and the Model Law; and 72 (66 JSI participants) jurisdictions have signed RTAs that mention avoiding unnecessary barriers to e-commerce or minimising the regulatory burden on electronic commerce, usually under a Domestic Electronic Transaction Framework.

22. Provisions similar to those in the UN Electronic Communications Convention and MLEC are also included in the *Southern African Development Community (SADC)'s* **Model Law on Electronic Transactions and Electronic Commerce**.[8] UN regional bodies such as *the UN Economic and Social*

[8] SADC consists of Angola, Botswana, Comoros, Republic of the Congo, Kingdom of Eswatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, United Republic of Tanzania, Zambia and Zimbabwe (16 states). Although the number of states that have enacted domestic legislation based on or influenced by SADC Model Law on Electronic Transactions and Electronic Commerce was not publicly available (as of 15 October 2020), this report assumes that all states have done so for the sake of the analysis.

Commission for Western Asia (ESCWA) have also established the **ESCWA Cyber Legislation Directives**.[9]

Table 3.1. Half of WTO Members have signed, ratified or been influenced by the UN Communication Convention or Model Law on Electronic Commerce

	UN Electronic Communications Convention	UNCITRAL Model Law on Electronic Commerce	RTA referencing the UN Communication Convention	RTA referencing the Model law on Electronic Commerce	Jurisdictions ratified or influenced by either of the UN Convention or the UN Model law (including through RTA referencing them)
Number of jurisdictions ratified/signed/referenced each convention/model law/RTAs	26 jurisdictions (14 JSI participants) (signature or ratification)	74 jurisdictions (31 JSI participants) (have enacted domestic legislation based on or influenced by)	15 jurisdictions (12 JSI participants)	22 jurisdictions (19 JSI participants)	91 jurisdictions (83 WTO Members and 41 JSI participants)

Source: Authors' calculations based on UNCITRAL websites on UN Electronic Communication Convention and Model Law on Electronic Commerce, the TAPED dataset and (Burri and Polanco Lazo, 2019[9]). See Annex B.

3.1.2. E-authentication and e-signatures

23. Although countries tend to have domestic rules authorising the legal validity of paper-based documents used for transactions, including requirements for handwritten signatures, it is not always the case that transactions based on electronic communications, which often include e-signatures, enjoy the same level of legal certainty. This issue becomes more challenging when considering the legal validity of documents for transactions that cross borders and involve more than one jurisdiction. Paper-based documents can take more time to produce and to clear, and can also be lost or misplaced. Standards for legislative frameworks providing functional equivalence between electronic communications and paper documents, as well as between electronic signatures and handwritten signatures, have the potential to greatly facilitate trade.

24. The establishment of harmonised legislative frameworks has been mainly promoted by *UNCITRAL*. In addition to the abovementioned **UN Electronic Communications Convention** and the **UNCITRAL Model Law on Electronic Commerce**, both of which include provisions on e-authentication and e-signature, UNCITRAL has also developed **the Model Law on Electronic Signatures**. This lays out criteria related to technical reliability for the equivalence between electronic and hand-written signatures. Legislation based on, or influenced by, this Model Law has been adopted in 33 jurisdictions (13 JSI participants).

[9] ESCWA comprises 20 Arab States: Algeria, Bahrain, Egypt, Iraq, Jordan, Kuwait, Lebanon, Libya, Morocco, Mauritania, Oman, Palestinian Authority, Qatar, Saudi Arabia, Somalia, Sudan, Syrian Arab Republic, Tunisia, United Arab Emirates and Yemen. Although the number of states that have enacted domestic legislation based on or influenced by ESCWA Cyber Legislation Directives was not publicly available (as of 15 October 2020), this report assumes that all states have done so for the sake of the analysis.

25. Rules on e-authentication and e-signatures that are included in the UN Electronic Communication Convention and the Model Law on Electronic Commerce again impact domestic legislation through RTAs that reference either or both of these instruments (Table 3.2). However, although the Model Law on Electronic Signatures does not appear to be referenced in *RTAs*, 87 jurisdictions (66 JSI participants) have signed *RTAs* that include at least one provision on e-authentication and/or e-signatures. These provisions stipulate that the legal validity of a signature shall not be denied solely on the basis that the signature is in electronic form,[10] similar principles to which are also included in the UN Electronic Convention and the Model Law on Electronic Commerce.[11]

26. Part of the provisions of the UNCITRAL Model Law on Electronic Signatures are reflected in other regional instruments, such as **SADC Model Law on Electronic Transactions and Electronic Commerce**. **ESCWA Cyber Legislation Directives** and **Supplementary Act A/SA.2/01/10 on electronic transactions within ECOWAS**[12] also contain provisions on e-signatures.

27. In the context of trade facilitation, *the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT, see also 3.4.1)* has developed a **recommendation** for governments to review requirements for paper-based signatures in international trade documents in favour of these being undertaken electronically (Recommendation 14).

28. At the same time, technical standards on e-signatures have been established in the *International Organization for Standardization (ISO)*, an independent, non-governmental, international organization developing voluntary and consensus-based international standards with a membership of 165 national standard bodies**.**[13] Its **ISO 14533** provides technical standards to ensure long-term authenticity and interoperability of e-signatures.[14]

[10] CPTPP, Art. 14.6., USMCA, Art. 19.6., EU-Japan EPA, Art. 8.77, ASEAN e-commerce agreement Art. 7, SADEA, Art. 9.

[11] The UN Electronic Communication Convention, Art. 8, the Model Law on Electronic Commerce, Art. 5.

[12] The Economic Community of West African States (ECOWAS) and Ibero-American Data Protection Network.

[13] https://www.iso.org/about-us.html (accessed on 12 October 2020).

[14] Although these technical standards might be widely accepted by businesses and governments, numbers on the extent of adoption are not usually publicly available. The same holds true with other ISO standards identified in the Inventory.

Table 3.2 Many jurisdictions are influenced by UNCITRAL instruments on e-authentication and e-signatures

	UN Electronic Communications Convention (including rules on e-signature and e-authentication)	UNCITRAL Model Law on Electronic Commerce (including rules on e-signature and e-authentication)	UNCITRAL Model Law on Electronic Signatures	RTA referencing the UN Communication Convention	RTA referencing the Model law on Electronic Commerce	Ratified or influenced by either of the UN Convention or the UN Model law (including through RTA referencing them)	RTAs including a provision on e-signature and e-authentication
Number of jurisdictions ratified/signed/influenced by each convention/model law/RTAs	26 jurisdictions (14 JSI participants) (signature or ratification)	74 jurisdictions (31 JSI participants) (have enacted domestic legislation based on or influenced by)	33 jurisdictions (13 JSI participants) (have enacted domestic legislation based on or influenced by)	15 jurisdictions (12 JSI participants)	22 jurisdictions (19 JSI participants)	91 jurisdictions (83 WTO Members and 41 JSI participants)	87 jurisdictions (66 JSI participants)

Source: Authors' calculations based on UNCITRAL websites on UN Electronic Communication Convention, Model Law on Electronic Commerce Model Law on Electronic Signature and the TAPED dataset (Burri and Polanco Lazo, 2019[9]). See Annex B.

3.1.3. Electronic contracts

29. Contracts are a key element of international trade transactions, and although contracts could potentially be concluded electronically, the legal validity and enforceability of electronic contracts remains unclear, especially if they are not anticipated in domestic legislation.[15]

30. The **UN Electronic Communications Convention** and **UNCITRAL Model Law on Electronic Commerce** include provisions stating that the validity or enforceability of a communication or a contract shall not be denied solely on the grounds that it is in electronic form. Other regional fora have also developed rules on electronic contracts, including **SADC's Model Law on Electronic Transactions and Electronic Commerce** and **Supplementary Act A/SA.2/01/10 on electronic transactions within ECOWAS.** Furthermore, as mentioned above, *RTAs* explicitly referencing the Convention have been signed by 15 jurisdictions while RTAs referencing the Model law have been signed by 22 jurisdictions.

3.1.4. Electronic invoicing

31. Issuing invoices electronically can also lead to important efficiency gains, enabling greater accuracy and reliability of international commercial transactions. This is an area that is not currently covered by UNCITRAL instruments. That said, **Supplementary Act A/SA.2/01/10 on electronic transactions within ECOWAS** includes a provision that requires an electronic document to be accepted for invoicing in the same manner as a hard copy. **DEPA** requires that measures related to e-invoicing be based on international standards, guidelines or recommendations so as to ensure cross-border interoperability. At the same time, technical standards on electronic invoicing have been developed at *UN/CEFACT* (**the Cross Industry Invoice (CII)**) and *ISO* (**ISO 20022**).

[15] See (Nunn, 2007[33]), (Spencer, 2005[34]) and (Antras, 2003[35])for a review of different issues raised by contracts for international trade.

3.1.5. E-payment

32. International trade could be further facilitated if efficient, safe and secure cross-border electronic payment services become more widely available. For this to happen, interoperability and the interlinking of electronic payment services and infrastructure are an important precondition. This is especially important in the context of COVID-19, where the wider use of e-payments can help maintain economic activities by reducing the need for personal contact when undertaking trade transactions (OECD, 2020[8]).

33. The international regulatory framework for online payments builds on sectoral regulations on financial services, including the GATS Annex on Financial Services and various chapters on financial services in RTAs. However, specific regulatory rules on e-payments remain limited and are not covered by UNCITRAL instruments. Nevertheless the **Trade Facilitation Agreement** and the **OECD Recommendation of the Council on Consumer Protection in E-commerce** contain language covering specific contexts where e-payments are used, i.e., at Customs or when consumer protection is required.

34. General principles focusing on e-payment tend to be found in digital-trade-specific agreements, such as **DEPA**. This provides for principles such as transparency of e-payment regulations and consideration of internationally accepted payment standards promoting the use of Application Programming Interface (API). The **ASEAN E-commerce agreement** also requires members to encourage the use of safe and secure, efficient, and interoperable e-payment systems.

35. *ISO* established **ISO 20022**, which is a widely recognized technical standard on payments.[16] As of September 2019, according to asianbankingandfinance.net, this standard has been used by market infrastructures in more than 70 countries for payments and securities business.[17]

3.2. Non-discrimination and liability

3.2.1. Non-discriminatory treatment of digital products

36. While the GATT and the GATS prohibit discriminatory treatment of goods and services, it is not necessarily clear whether "digital products" are accorded the same protection as their non-digital counterparts under the WTO agreements.[18] As more products are delivered digitally, questions related to non-discriminatory treatment of "digital products" are increasing being raised.

37. The principle of non-discrimination has primarily been developed through *RTAs*: 35 jurisdictions (29 JSI participants) have signed RTAs including a provision on national treatment for "digital products" while 33 jurisdictions (28 JSI participants) have signed RTAs including a provision on most-favoured-nation treatment for "digital products".[19]

3.2.2. Interactive computer services (limiting non-IP liability for suppliers and users and infringement of persons' rights)

38. Online trade is made possible through services that enable access to the Internet, including broadband Internet access service providers or search engines (so called "interactive computer services"). Given the importance of these services for digital trade, it has been proposed that the scope of non-IP

[16] Various other ISO standards such as ISO/IEC 7816 for electronic identification cards with contacts (e.g., smart cards) and ISO/IEC 14443 for contactless integrated circuit cards might also be relevant in this space.

[17] https://asianbankingandfinance.net/co-written-partner/sponsored-articles/iso-20022-common-standard-transform-global-payments (accessed on 12 October 2020).

[18] The term "digital products" is used here in the context of the issues being discussed at the JSI without prejudice as to what the term is considered to encompass.

[19] The term "digital products" is often, although not always, defined in the relevant RTAs.

liability for harm related to information stored, distributed or made available over the Internet be defined. Development of rules on these issues is sensitive and still in a nascent stage. Few *RTAs,* involving 4 jurisdictions, have included references to principles in this area (including **USMCA and US-Japan**).

3.3. Consumer protection

3.3.1. Online consumer protection

39. Promoting trust between consumers and suppliers may be more important online than offline considering that contact, the means by which consumers usually test the reliability of retailers and the quality of products, can be limited. Consumers are also often required to disclose sensitive information when undertaking online purchases, such as providing credit card details and personal data (World Economic Forum, 2019[10]).

40. A first international instrument for consumer protection dealing with risks arising from e-commerce is the non-binding **OECD Recommendation of the Council on Consumer Protection in E-commerce**, which was developed in 2016.[20] The recommendation, which is adhered to by 39 jurisdictions (39 JSI participants), provides detailed guidance to address core characteristics of consumer protection for e-commerce. It includes principles on transparent and effective consumer protection, fair business practices, online disclosures, payment, dispute resolution and redress, privacy and security.

41. *UNCTAD* has also developed the non-binding **UN Guidelines for Consumer Protection**, which includes a provision encouraging UN Member States to enhance consumer confidence in e-commerce.[21] These Guidelines also request UN Member States to study the relevant international guidance and standards on e-commerce, in particular the **OECD Recommendation of the Council on Consumer Protection in E-commerce**. **The SADC Model Law on Electronic Transactions and Electronic Commerce** also includes provisions on consumer protection. Additionally, technical standards on consumer protection are under development, for instance, at *ISO*.

42. There are 98 jurisdictions (76 JSI participants) that have signed *RTAs* including a provision on consumer protection. Major trade agreements, such as the **CPTPP**, the **USMCA** and the **EU-Japan EPA** include provisions asking parties to recognise the importance of adopting and maintaining transparent and effective consumer protection measures in the context of digital trade transactions and highlighting the importance of cooperation among national consumer protection agencies.[22]

3.3.2. Unsolicited commercial electronic messages/spam

43. One of the protections that consumers may be provided is the right to choose whether or not they wish to receive unsolicited commercial electronic messages. In this area, the **OECD Recommendation of the Council on Consumer Protection in E-commerce** requests businesses to develop and implement effective and easy-to-use procedures to provide consumers with this protection. **The SADC Model Law on Electronic Transactions and Electronic Commerce** also include provisions on unsolicited commercial communications.

44. There are 91 jurisdictions (73 JSI participants) that have signed an RTA including a provision on unsolicited commercial electronic messages. For instance, the **CPTPP**, the **USMCA** and the **EU-Japan EPA** require parties to adopt or maintain measures that require suppliers of unsolicited commercial

[20] https://legalinstruments.oecd.org/en/instruments/183#adherents

[21] The authors were unable to locate data on states adhering to these guidelines.

[22] CPTPP Art. 14.7, USMCA, Art. 19.7, EU-Japan EPA, Art. 8.78.

electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages; and require the prior consent of recipients to receive commercial electronic messages.[23]

3.4. Digital facilitation and logistics

45. The speed and costs of border measures is an important aspect of the e-commerce landscape since they can affect the speed and delivery of imported and exported goods ordered online. This is especially the case for SMEs, which tend to find it disproportionately more difficult to bear the costs of engaging in international trade. Indeed, recent evidence shows that streamlining procedures and automation of border processes, both of which can be accomplished through the use of digital technologies, are particularly important in enabling SMEs to become exporters (López González and Sorescu, 2019[11]).

46. This area already has comparatively more rules, starting with the **WTO's Trade Facilitation Agreement (TFA)**, which covers a broad range of trade facilitation and Customs compliance issues. UN agencies, such as the United Nations Economic Commission for Europe (UNECE), and the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT), UN Economic and Social Commission for Asia and the Pacific (ESCAP), and UNCITRAL, have also provided recommendations, framework agreements and model laws. Other global inter-governmental organisations, such as the World Customs Organisations (WCO) and the Universal Postal Union (UPU), have also developed standards and binding rules.

3.4.1. Paperless trading

47. Transformation from a traditional paper-based documentation system into an electronic format system can reduce the Customs clearance time and the cost of doing cross-border business, especially for SMEs and e-traders (World Economic Forum, 2017[12]).

48. Globally, *WTO* Members concluded negotiations on the **TFA** in 2013, which entered into force in 2017 and has been ratified by 153 Members (all 86 JSI participants). It aims to further expedite the movement, release and clearance of goods, enhancing assistance and support for capacity building and promoting effective cooperation among Members on trade facilitation and Customs compliance issues.[24] The Agreement includes provisions that can promote paperless trade, including on pre-arrival processing of documents in electronic format, acceptance of electronic copies of required documents and single windows.

49. Other UN fora promoting paperless trading are *the United Nations Economic Commission for Europe (UNECE)*, and its subsidiary, *the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT)*. UNECE has developed and maintained a series of non-obligatory **recommendations for international trade** reflecting best practices in trade procedures and data and documentary requirements (World Economic Forum, 2017[12]). These include, for instance, a recommendation that governments use the UN/EDIFACT standard (see below) for international applications of electronic data interchange (EDI) among different parties (Recommendation 25). *The UN/CEFACT* has also established **standards for data exchange**. For instance, **the United Nations rules for Electronic Data Interchange for Administration, Commerce and Transport (UN/EDIFACT)** is a set of internationally agreed standards, directories, and guidelines for the electronic interchange of structured data, between independent computerized information systems.

50. Regional instruments for paperless trade include **the Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific,** developed by *UN Economic and Social*

[23] CPTPP Art. 14.14, USMCA, Art. 19.13, EU-Japan EPA, Art. 8.79.

[24] Preamble of the TFA.

*Commission for Asia and the Pacific (UN ESCAP)***.** The Framework Agreement, which provides general principles and key provisions for facilitation of paperless trade, is complementary to the WTO TFA.[25] It is open to ESCAP member states and, to date, 7 jurisdictions (3 JSI participants) have signed or ratified the Framework Agreement.[26]

51. With regards to *RTAs*, 78 jurisdictions (70 JSI participants) have signed agreements including a provision on paperless trading. For instance, the **CPTPP** stipulates that each party shall endeavour to make trade administration documents available to the public in electronic form; and accept trade administration documents submitted electronically as the legal equivalent of the paper version of those documents.[27] **DEPA** and the **SADEA** include more details on paperless trade, such as measures to facilitate the exchange of data relating to trade administration documents.[28]

3.4.2. Electronic transferable records

52. The availability of transferable documents and instruments in electronic form benefits cross-border e-commerce, allowing for faster and more secure transmission while reducing risks associated with unauthorized duplication. Given that a fully paperless trade environment cannot be established without electronic transferable records, progress in this area can make a significant contribution to trade facilitation.[29]

53. **UNCITRAL** has developed **the Model Law on Electronic Transferable Records (MLETR)**, which was adopted by the UN General Assembly in July 2017. Building on the principles of non-discrimination for the use of electronic means, functional equivalence and technology neutrality that underpin all UNCITRAL texts on electronic commerce,[30] the MLETR aims to enable the legal use of electronic transferable records both domestically and across borders.[31] While legislation based on or influenced by the MLETR has only been enacted by 3 states,[32] some RTAs, such as **DEPA** and **SADEA,** require parties to endeavour to adopt or take into account the MLETR.[33]

3.4.3. Customs procedures

54. Issues such as the time-sensitive flow of goods, growing volumes of cross-border trade in parcels, participation of new, unknown players in trade, and return/refund processes, have brought new challenges

[25] https://www.unescap.org/sites/default/files/FAQ%20on%20the%20Framework%20Agreement_Nov%202016.pdf

[26] https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=X-20&chapter=10&clang=_en (as of 26 October 2020).

[27] CPTPP, Art. 14.9.

[28] DEPA, Art. 2.2 and SADEA Art. 12.

[29] United Nations Commission on International Trade Law, *UNCITRAL Model Law on Electronic Transferable Records* (Explanatory Note to the UNCITRAL Model Law on Electronic Transferable Records) (2018).

[30] Namely, the Electronic Communication Convention, the UNCITRAL Model Law on Electronic Commerce and the UNCITRAL Model Law on Electronic Signatures.

[31] https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records

[32] These are Bahrain, Singapore and the United Arab Emirates. See UNCITRAL Model Law on Electronic Transferable Records (2017) - Status | United Nations Commission On International Trade Law accessed 12 April 2021.

[33] DEPA, Art. 2.3, SADEA Art. 8.

for Customs administrations with regard to a range of issues, including trade facilitation and security, and the fair and efficient collection of duties and taxes.[34]

55. In this area, the **TFA** includes broad rules and principles to expedite the movement, release and clearance of goods. For instance, Art.10 stipulates rules on Customs procedures regarding formalities and documentation requirements, acceptance of copies (including electronic copies), use of international standards, single window and pre-shipment inspection.

56. Another global rule-making forum on Customs procedures is *The World Customs Organization (WCO)*, which has engaged with relevant stakeholders to define approaches to deal with challenges arising from digital trade. The WCO has developed various tools that support e-commerce, for instance, the **Cross-Border E-commerce Framework of Standards**, which provides global baseline standards for the effective management of cross-border e-commerce, from both facilitation and control perspectives, to assist Customs and other relevant government agencies in developing e-commerce strategic and operational frameworks (World Customs Organization, 2018[13]). The WCO also developed the **SAFE Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework)**, which establishes standards that serve to secure revenue collections, act as a deterrent to international terrorism and promote trade facilitation. The SAFE Framework is referenced by some *RTAs*, such as **EU-Japan EPA**, which requires that Customs procedures of parties be consistent with international standards and recommended practices, including the SAFE Framework.[35]

57. *The Universal Postal Union (UPU)*, the primary forum for cooperation between postal sector players, sets the rules for international mail exchange and makes recommendations to stimulate growth in mail, parcel and financial services and to improve quality of service for customers.[36] With regards to digital trade, the UPU established the **Universal Postal Convention and its Regulations**, which provide binding rules applicable throughout the international postal service, and provisions concerning the letter-post and postal parcels services. For instance, these provisions urge designated operators (DOs) to make efforts to develop mechanisms for sending electronic advanced data (EAD) on international postal shipments, to be used for both Customs and aviation security purposes.

58. Regionally, *ASEAN* developed the **ASEAN Agreement on Customs** in 2012 to simplify and harmonise Customs valuation, tariff nomenclature and Customs procedures. While digitalisation elements are not explicitly included in the text, many of the provisions can have implications for digital trade. *RTAs*, on the other hand, tend to include some of the issues relevant to digital trade in their provisions on trade facilitation or Customs procedures.

3.4.4. De minimis

59. *De minimis* is a valuation ceiling for goods below which no duty or tax is charged and clearance procedures, including data requirements, are minimal. Consumers and businesses may benefit from *de minimis* as it can reduce costs associated with digitally ordered goods crossing borders (given that these may no longer need to pay duties, taxes and brokerage fees, and may benefit from expedited clearance procedures (Latipov, McDaniel and Schropp, 2017[14])). At the same time, it is argued by some that high de minimis thresholds may provide an unfair tax advantage to foreign retailers over domestic retailers. In the context of COVID, higher *de minimis* thresholds could help Customs and other border agencies expedite clearance and deal with growing workloads and lower availability of personnel (OECD, 2020[8]).

---

[34] See *Cross-Border e-Commerce*, WCO, http://www.wcoomd.org/en/topics/facilitation/activities-and-programmes/ecommerce.aspx (accessed on 12 October 2020).

[35] EU-Japan EPA Art. 4.4.

[36] https://www.upu.int/en/Universal-Postal-Union (accessed on 12 October 2020).

60. The **TFA** requires each Member to provide "to the extent possible" a *de minimis* shipment value."[37] Furthermore, the **USMCA** provides the minimum fixed amount that the parties are obliged to set as *de minimis.*[38]

3.5. Privacy: Protection of personal information/privacy

61. Trade in the digital era is increasingly underpinned by the movement of data across borders (Casalini and López González, 2019[15]). Owing to the nature of emerging trade transactions, much of this data can arguably be considered personal or personally identifiable in nature. The growing cross-border exchange of this type of data has raised concerns related, among others, to privacy protection (Mattoo and Meltzer, 2019[16]) (Casalini and López González, 2019[15]) (OECD, 2020[17]) (Casalini, Lopez-Gonzalez and Nemoto, 2021[18]).

62. Rules to secure privacy and personal data protection have been developed in a number of international fora (Table 3.3). The first internationally agreed upon set of privacy principles on the protection of personal data was the *OECD*'s **1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data** (revised in 2013). Although they are not legally binding, at least all OECD members, 37 governments, have agreed to these. The OECD Privacy Guidelines have also influenced the development of other international privacy frameworks, including the **APEC Privacy Framework**, which is consistent with the core elements of the OECD Privacy Guidelines. APEC further developed the **Cross Border Privacy Rules (CBPR)** system, a government-backed data privacy certification framework, allowing companies to transfer data between CBPR participating economies with greater trust.[39]

63. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)** of *the Council of Europe*, which 55 jurisdictions, including non-European jurisdictions, have ratified, is a binding treaty with enforcement mechanisms.[40] Other Regional organizations, such as *ASEAN*, the *African Union, the Economic Community of West African States (ECOWAS) and Ibero-American Data Protection Network* have also established their own privacy protection arrangements (**ASEAN PDP Framework**, **African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), Supplementary Act A/SA. 1/01/10 on Personal Data Protection within ECOWAS,** and **Data Protection Standards of the Ibero-American States**).[41]

64. With regards to *RTAs*, 103 jurisdictions (79 JSI participants) have signed agreements including a provision on data protection, including protection of personal data or data privacy. For instance, some require adopting or maintaining a legal framework for the protection of personal information of the users of e-commerce. Among them, 78 jurisdictions (60 JSI participants) have also signed RTAs that recognise international standards in the area of data protection. For example, the **USMCA** and the **SADEA** reference the APEC Privacy Framework/APEC CBPR System and the OECD Privacy Guidelines as principles and

[37] TFA, Art. 7.8.2(d).

[38] USMCA, Art. 7.8.1 (f).

[39] The CBPR System is not mandatory for APEC economies, and even when an economy adheres to it, companies can choose whether to seek certification under the System. However, once a company acquires the CBPR certification, it assumes liability under the CBPR framework vis-á-vis participating economies.

[40] The Convention 108 is followed by The 2001 Additional Protocol, which 50 states that have signed or ratified, and the 2018 Amending Protocol (creating what is commonly known as Convention 108+), which 42 states have signed or ratified. The 2018 Amending Protocol, when it enters into force, will update the provisions on the flow of personal data between signatories.

[41] Furthermore, at the 31st *International Conference of Data Protection and Privacy Commissioners*, protection authorities of 50 countries adopted the "**Madrid Resolution**", a non-binding resolution that includes principles for privacy protection legal systems.

guidelines that parties are requested to take into account in the development of legal frameworks for personal information protection.[42]

65. Given that different countries can take different legal approaches to protecting personal information, some agreements encourage the development of mechanisms to promote compatibility or interoperability between different regimes.[43] In particular, the **USMCA** stipulates that parties recognize that the APEC Cross Border Privacy Rules system is a valid mechanism to facilitate cross-border information transfers while protecting personal information.

66. Technical standards on privacy protection have also been developed in *ISO* and the *International Electrotechnical Commission (IEC)*. **ISO/IEC 27701** lays out requirements and guidance for privacy management within the context of the adopting organisation.

Table 3.3. Privacy protection instruments have been widely developed in multiple international fora

	The OECD Privacy Guidelines	APEC Privacy Framework	APEC CBPR system	Convention 108 (ratified)	ASEAN PDP Framework	AU Malabo Convention[44]	ECOWAS Supplementary Act A/SA. 1/01/10 on Personal Data Protection	Data Protection Standards of the Ibero-American States	RTAs including privacy principles	RTAs including provisions on data protection recognising certain international standards
Number of jurisdictions ratifying/adhering to each arrangement (number of JSI participants))	37 (37)	21 (19)	9 (9)	55 (43)	10 (8)	19 (1)	15 (4)	10 (9)	103 (79)	78 (60)

Source: Authors' calculations based on websites of the OECD Privacy Guidelines, APEC CBPR system, Convention 108, ASEAN PDP Framework, AU Malabo Convention, ECOWAS and Ibero-American Data Protection Network and the TAPED dataset. See Annex B.

3.6. Flow of information

3.6.1. Cross-border transfer of information by electronic means

67. Whether large or small, businesses across all industries are increasingly reliant on data transfers in support of their activities, including in global value chains (OECD, 2020[17]). However, as noted previously, the movement of data across borders can generate challenges with respect to privacy and data protection, but also in areas such as intellectual property rights, cybersecurity, regulatory reach, competition and industrial policy. Due to these regulatory challenges, a growing number of countries are now placing conditions on the transfer of data across borders (Casalini and López González, 2019[15]).

68. In order to promote cross-border data flows while securing "trust", international instruments on cross-border data flows have been developed in a range of international fora, many of which focus on

[42] USMCA, Art. 19.8.2., SADEA, Art. 17.2.

[43] See, for instance, CPTPP, Art. 14.8.5, USMCA, Art. 19.8.6, DEPA, 4.2.6 and SADEA, Art. 17.7.

[44] As of latest available data published 18/06/2020.

cross-border flow of personal data. In fact, many instruments listed in the section above (section 3.5), relating to plurilateral arrangements, include mechanisms to foster cross-border flows of personal data between participating economies while ensuring privacy protection.

69. RTAs are another tool to secure cross-border information flows. There are 72 jurisdictions (55 JSI participants) that have signed *RTAs* including provisions on cross-border data flows, which cover all types of data, including personal as well as non-personal data. The depth and density of rules varies across agreements. Among different approaches, some agreements include provisions that enshrine unrestricted cross-border movement of data between signatories, while providing for exceptions where legitimate public policy objectives are concerned, and provided that measures are non-discriminatory and not unnecessarily trade restrictive (See (Casalini, Lopez-Gonzalez and Nemoto, 2021[18])for further details).[45]

3.6.2. Location of computing facilities

70. Another type of data-related regulation are requirements to store or process data in local computer facilities (Casalini and López González, 2019[15]). Local storage requirements can affect cross border data flows to the extent that companies switch from a foreign supplier to a domestic supplier to store and process data that is collected in a certain country (OECD, 2020[17]). Switching to a domestic server might add to the costs for the companies to doing business worldwide.

71. Rules that seek to curtail requirements to locate computing facilities domestically are emerging, with 19 jurisdictions (17 JSI participants) having signed **RTAs** including such provisions. Among different approaches, some stipulate that using or locating computing facilities in a party's territory shall not be required, while, at the same time, allowing parties to maintain measures to achieve legitimate public policy objectives (provided these measures are non-discriminatory and not unnecessarily trade restrictive).[46] Furthermore, the **USMCA** and the **ASEAN e-commerce agreement** stipulate that parties shall not, or agree not, to impose local computer facility requirements.[47] However, rules stipulating that countries cannot impose local storage requirements do not appear to have been developed in other inter-governmental fora.

3.6.3. Location of financial computing facilities

72. While storing and processing data is crucial for financial sector businesses, securing access to financial data can be critical to financial regulatory and supervision authorities. The importance of access to financial data can give rise to special requirements on location of financial computing facilities.

73. Although no rules or principles related to the location of financial computing facilities have been as yet developed across international fora, a few RTAs, such as the **USMCA** and the **SADEA**,[48] stipulate that using local computing facilities shall not be required provided that the financial regulatory authorities have immediate, direct, complete, and ongoing access to information processed or stored on computing facilities located abroad.[49]

[45] See, for instance, CPTPP, Art. 14.11, USMCA, Art. 19.11, DEPA, Art. 4.3, SADEA, Art. 23 and US-Japan digital trade agreement, Art. 11.

[46] For instance, see CPTPP, Art. 14.8, DEPA, Art. 4.4 and SADEA, Art. 24.

[47] USMCA, Art. 19.12, ASEAN e-commerce agreement 7.6.

[48] The TAPED dataset does not provide data for location of financial computing facilities.

[49] USMCA, Art. 17.18, SADEA, Art. 25.

3.7. Cybersecurity

74. With the growing reliance of business and governments on digital networks for trade, the associated growth in cyber risk, including increasing cyberattack vectors and data breaches, have deepened cybersecurity concerns more generally (Huang, Madnick and Johnson, 2018[19]). According to (Meltzer and Cameron, 2019[20]) "trade and cybersecurity are increasingly intertwined [..] new trade rules that can both support risk based effective cybersecurity regulation, build bridges between the cybersecurity policy in different countries to maximise synergies, and minimise barriers to trade are needed".

75. Cybersecurity rules and principles have been established in multiple international governmental and non-governmental fora, in line with their respective mandates. Globally, the **UN Charter** and existing **international law,** which address national and international security, could apply to state use of ICT.[50] Security aspects are also covered by **the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies,** which includes software and technologies that are designed or could be used for the conduct of military offensive cyber operations.

76. *The OECD* focuses on economic and social aspects of cybersecurity. The organisation adopted the **OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity** and its companion Document in 2015, which provides guidance on national strategies for the management of digital security risks aimed at optimise the economic and social benefits expected from digital openness. The OECD also adopted the **Recommendation on Digital Security of Critical Activities** in 2019. The former has 39 adherents (39 JSI participants), while the latter has 38 adherents (38 JSI participants).

77. *The Council of Europe* established **the Convention on Cybercrime (the Budapest Convention)**, which is a legally-binding international instrument to pursue a common criminal policy aimed at the protection of society against cybercrime. It is ratified or signed by 68 jurisdictions (52 JSI participants) including jurisdictions outside Europe.[51] In 2011, the *ECOWAS* also developed the **Directive C/DIR/1/08/11 on Fighting Cyber Crime within ECOWAS** to adapt the substantive criminal law and procedures of the Member States to address cybercrime.

78. There are 66 jurisdictions (61 JSI participants) that have signed *RTAs* including a provision on cybersecurity. The **CPTPP** and the **ASEAN e-commerce agreement**, for instance, stipulate that the parties recognise the importance of: building the capacity of their national entities responsible for computer security incident response; and using existing collaboration mechanisms to cooperate on matters related to cyber security (without specifying what these mechanisms might be).[52] The **USMCA** further requires each party to endeavour to employ risk-based approaches that rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events.[53]

79. Other regional arrangements, such as **AU's Malabo Convention** and **ESCWA Cyber Legislation Directives,** also include provisions on cyber security or cybercrime**.**

80. *ISO and IEC* established the **ISO/IEC 27000 family**, which provide information security standards, helping to protect IT systems. **IEC 62443** is designed to keep operational technology systems

[50] The consensus report of the United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (adopted by UN General Assembly on 22 July 2015 (A/70/174)).

[51] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=qSvWi9lH (accessed on 27 October 2020).

[52] CPTPP, Art. 14.16, ASEAN e-commerce agreement, Art. 8.

[53] USMCA, Art. 19.15.2.

running in the physical world. *The IEEE*, the world's largest technical professional society, has also established standards on cybersecurity, such as **Standard for Intelligent Electronic Devices Cyber Security Capabilities** and **Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities**.

Table 3.4. Spread of cybersecurity rules

	OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity (adherents)	OECD Recommendation on Digital Security of Critical Activities (adherents)	The Budapest Convention of the Council of Europe (ratification)	RTAs including provisions on cybersecurity
Number of jurisdictions ratifying/adhering to each arrangement	39	38	65	65

Source: Authors' calculations based on websites of the OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity, the OECD Recommendation on Digital Security of Critical Activities, the Convention on Cybercrime of the Council of Europe and the TAPED dataset. See Annex B.

3.8. Telecoms: Updating the WTO Telecommunications Reference Paper

81. The quality and cost of access to digital networks are conditioned by the available physical infrastructure and the cost of an internet connection, which are ultimately affected by the regulations and degree of competition in the telecommunications service market (López González and Ferencz, 2018[1]).

82. In order to ensure that dominant market positions of suppliers are not used to the detriment of new entrants in telecommunications markets (Bronckers and Larouche, 2012[21]), key regulatory principles of telecommunications are provided by **the WTO Telecommunications Reference Paper**, in addition to those included in GATS Annex on Telecommunications. The Reference Paper, to which 96 WTO Members have committed and 7 WTO Members have partly committed, has not been updated since its establishment. Meanwhile, rules have been developed in *RTAs*, many of which include a chapter or a section dedicated to telecommunications.[54] For instance, the **EU-Japan EPA** includes rules related to telecommunications beyond those contained in the WTO Telecommunications Reference Paper. This includes issues such as number portability, resale, authorisation to provide telecommunications networks and services, allocation and use of scarce resources and resolution of telecommunications disputes.[55]

83. Technical standards have also been established in multiple inter-governmental and non-governmental standard-setting fora. The *International Telecommunication Union (ITU)*, a specialized UN agency focusing on technical issues (e.g., frequency allocation and standardization), has developed international standards known as **ITU-T Recommendations,** which act as defining elements in the global infrastructure of ICTs. *ISO* and *IEC* also deal with technical issues of telecommunication. Its subcommittee, SC6, which works on standardization in the field of telecommunications, has published 289 **ISO/IEC standards**.

84. Industry associations or international communities, such as *Telecommunication Industry Association (TIA)*, *The European Telecommunications Standards Institute (ETSI)* and *The Internet Engineering Task Force (IETF)* have also developed telecommunication or internet standards.

[54] The TAPED dataset does not provide how many states have signed RTAs including telecom provisions.

[55] EU-Japan EPA, Chapter 8, Section E, Sub-section 4.

3.9. Customs duties: Customs duties on electronic transmissions

85. An important aspect of the evolving digital transformation is the ability to transmit electronic content via digital networks – often referred to as electronic transmissions.[56] Since 1998, WTO Members have regularly extended a Moratorium on imposing customs duties on electronic transmissions. Most recently, at the General Council meeting in December 2019, Members agreed to maintain that practice until the 12th WTO Ministerial Conference (MC12).[57] However as more trade becomes digitally deliverable, some WTO Members are voicing concerns about possible foregone government revenue due to the Moratorium (Andrenelli and López González, 2019[22]).

86. Rules on customs duties on electronic transmissions have also been included in **RTAs,** with 90 jurisdictions (70 JSI participants) signing RTAs that include a provision stating the permanency of the moratorium on duty free treatment of electronic transmission for signatories to the agreement.

3.10. Access to internet and data

3.10.1. Open government data

87. Governments produce, collect and store a wide range of data in their day-to-day activities. Facilitating public access to and use of that data is expected to generate significant social and economic benefits. For instance, open government data policies can help domestic and foreign businesses, including SMEs, identify new business opportunities (OECD/ADB, 2019[23]).

88. Principles on "open government data" were set out in the **G8 Open Data Charter** signed in 2013. The charter includes principles of Open Data by Default, Quality and Quantity, Usable by All, Releasing Data for Improved Governance, Releasing Data for Innovation. The charter also identifies 14 high-value areas, from education to transport and from health to crime and justice, from which G8 members will release data.

89. **The OECD's Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information (The OECD Recommendation on Public Sector Information)**, which was adopted in 2008, is also relevant to the issue of open government data. The Recommendation provides policy guidelines that are designed to improve access and increase use of public sector information through greater transparency, enhanced competition and more competitive pricing.[58] There are 38 jurisdictions (38 JSI participants) that have adhered to the Recommendation.[59]

90. In terms of RTAs, only 3 agreements (7 signatory jurisdictions), including the **USMCA** and **DEPA**, contain provisions on it to encourage access to and use of government information.[60]

---

[56] See (Andrenelli and López González, 2019[22]) for a summary of the issues that electronic transmissions raise in the context of trade.

[57] https://www.wto.org/english/news_e/news19_e/gc_10dec19_e.htm

[58] The OECD website of OECD Recommendation on Public Sector Information (https://www.oecd.org/sti/oecdrecommendationonpublicsectorinformationpsi.htm#:~:text=The%20OECD%20Recommendation%20on%20public,Council%20on%2030%20April%202008.)

[59] As government data also enjoys protection provided by the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) where it falls under patent, copyright, or trade secrets protection, decisions about how and whether to make it "open" may implicate WTO TRIPS.

[60] USMCA, Art. 19.15, DEPA, Art. 9.4.

3.10.2. Access to the Internet

91. The benefits of digitalization cannot be fully reaped unless access to the Internet and services provided online are assured. While regulatory rules and principles on access to the Internet have not been established in global fora and other inter-governmental fora, 46 jurisdictions (44 JSI participants) have signed **RTAs** including such provisions. For instance, the **CPTPP** stipulates that its parties recognise the benefits of consumers in their territories having the ability to: access and use services and applications of their choice available on the Internet; connect the end-user devices of a consumer's choice to the Internet; and access information on the network management practices of a consumer's Internet access service supplier.[61]

92. On technical front, Internet standards, technical specifications that underpin the infrastructure of the Internet, have been developed by non-governmental technical standard-setting bodies, such as *Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA), the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB), the World Wide Web Consortium (W3C),* and the *Internet Society*.[62]

3.10.3. Access to online platforms/competition

93. Competition in major digital markets may be different to competition arising in more traditional markets. This is because digital markets may include more platform-based, multisided markets, or business models, with strong network effects and economies of scale, rendering competition issues more complex.[63] While access to online platforms, which support many personal and business activities including digital trade (e.g., online shopping platform), generates social and economic benefits, their significant and growing market presence may also raise new concerns. These might include unfair competition practices, such as abuses of market dominance, as well as winner-takes-most dynamics amplified by the wider adoption of digital platforms and technologies.

94. Discussions on cooperation among competition authorities have been promoted through the *International Competition Network (ICN)*, an informal, project-oriented network of antitrust agencies from 129 jurisdictions. The ICN has developed recommendations, or "best practices" on competition policies based on consensus of its members which then decide whether and how to implement these. To date, ICN has developed 7 **Recommended Practices** and 8 **Recommendations** on competition policies and competition law enforcement, although these have a wider focus than platforms and digital markets.

95. Inter-governmental cooperation arrangements on competition investigations and competition law enforcement have also emerged. For instance, the *OECD* adopted **Recommendation concerning International Co-operation on Competition Investigations and Proceedings**, which calls for governments to promote further international co-operation among competition authorities. So far, 40 jurisdictions (40 JSI participants) have adhered to these recommendations. **Co-operation agreements on competition** have also been concluded between two or more jurisdictions/competition authorities for effective action against anti-competitive practices with a cross-border connotation.[64]

96. Convergence of competition policy and cooperation among competent authorities have also progressed through *RTAs* that include chapters dedicated to competition or competition provisions. While

[61] CPTPP, Art. 14.10.

[62] For more details see https://www.internetsociety.org/policybriefs/openstandards/

[63] https://www.oecd.org/competition/digital-economy-innovation-and-competition.htm (Accessed on 14 October 2020).

[64] An inventory of international co-operation agreements on competition, focusing on 15 bilateral agreements is available on the OECD website (http://www.oecd.org/competition/inventory-competition-agreements.htm) (Accessed on 9 November 2020).

digital elements are not specially referred to in many competition chapters, **DEPA** requires its parties to consider undertaking mutually agreed technical cooperation activities in developing and implementing competition policies to address the challenges that arise from the digital economy.[65]

3.11. Business trust

3.11.1. Source code

97. . Recently, some governments have enacted or are considering requirements that firms disclose source code (the programming instructions or 'recipe' of software) for review as a condition of doing business. The main reasons cited have to do with fears of potential backdoors embedded into technology products that may compromise national security or citizens' privacy. However, there are concerns that such requirements also facilitate unauthorised technology transfer and IPR theft (Wu, 2017[6]).

98. Source code enjoys protection provided by the **WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement)** where it falls under patent, copy right or trade secrets protection.[66] Furthermore, under the **WTO agreement on technical barriers to trade (TBT Agreement)**, WTO Members are allowed to set technical specifications for products embedded with software, provided such specifications are not "more trade-restrictive than necessary to fulfil a legitimate objective". WTO Members also have the right to assure that imported products embedded with software conform to such technical specifications based on the rules in the agreement.

99. Specific rules on source code have mainly been developed through **RTAs**. There are 42 jurisdictions (41 JSI participants) that have signed agreements including provisions on source code. The **EU-Japan EPA**, for instance, stipulates that the transfer of, or access to, source code of software shall not be required by a government, but it also provides for exceptions.[67] Furthermore, some trade agreements, such as the **USMCA** and the **Japan-UK EPA**, also include an algorithm expressed in the source code of software within the scope of protection.

3.11.2. ICT products that use cryptography

100. Cryptographic technology increasingly underpins cross-border trade, securing many online transactions. Cryptography can enable speedy international payments to take place, offer a means of preventing cybercrime and provide secure environments for outsourcing specific operations on sensitive data, including to the cloud abroad (The Royal Society, 2019[24]). In the context of trade in goods, cryptographic technology can be embedded in exported and imported ICT products.

101. While WTO Agreements do not include specific provisions on cryptography, **the TBT Agreement** and **the TRIPS Agreement** could apply to ICT products using cryptography.

102. Rules on cryptography have also been developed at the *OECD*. Recognising that cryptography can be effective to secure information and communication networks and systems, while its misuse can adversely affect the operation of e-commerce, protection of privacy, etc., the OECD established the **Guidelines for Cryptography Policy** in 1997, to which 37 jurisdictions (37 JSI participants) adhere. The Guidelines lay out principles on cryptography policy, including a principle on lawful access which admits that national cryptography policies may allow lawful access to plaintext, or cryptographic keys, of

[65] DEPA, Art. 8.4.

[66] TRIPS Agreement, Article 10(1) stipulates "[c]omputer programs, whether in source or object code, shall be protected as literary works under the Berne Convention (1971)."

[67] EU-Japan EPA, Art. 8.73.

encrypted data, while requiring that these policies respect the other principles contained in the guidelines.[68]

103. Specific rules on ICT products using cryptography are also included in two **RTAs** (5 signatory jurisdictions). For instance, under the **USMCA**, parties shall not require manufacturers or suppliers of ICT goods using cryptography to transfer or provide access to their proprietary information relating to cryptographic technology. The recent **Japan-UK EPA** applies the same principle to "commercial information and communication technology products", which also includes software.[69]

104. With regards to technical standards, ISO/IEC has developed **ISO/IEC 18033**, which covers encryption systems (ciphers) for the purpose of data confidentiality.

3.12. Market Access

3.12.1. Service market access

105. Digital trade is subject to rules governing, and closely entwined with, traditional trade in goods and services. Therefore existing regulatory barriers and market access considerations affect digital trade. In case of services, commitments related to market access accorded by governments to digitally enabled services will be of key importance (López González and Ferencz, 2018[1]).

106. Access to domestic services markets is based on specific commitments that WTO Members schedule under the **GATS**. Service sectors under the GATS schedule of specific commitments relevant to digital trade include computer services, telecommunication distribution services and other services that could be digitally provided (for instance, financial services, professional services or audio-visual services, to name a few).

107. Preferential market access commitments are also generally included in **RTAs**.

3.12.2. Goods market access

108. As digitalization progresses, the volume of goods that are digitally ordered, or that might fall under digital trade, is increasing. Agreed tariffs and other rules under the **GATT** apply to all trade in digitally ordered goods. Other WTO agreements, such as **TBT Agreement**, also deal with non-tariff measures on these goods.

109. Tariff elimination on IT products has progressed among the WTO Members. In 1996, the **Information Technology Agreement (ITA)** was concluded, eliminating, on a most-favoured nation basis, tariffs on a large number of IT products covered, such as computers and telecommunication equipment. The number of participants has grown to 81[70] (68 JSI participants). In 2015, 53 participants[71] (52 JSI participants) concluded the **expansion of the Agreement**, which covers an additional 201 IT products such as new generation semi-conductors and advanced medical equipment. Members agreed to remove tariffs on selected products by 2024.

[68] The issue of government access to personal data is currently under discussion at the OECD Committee on Digital Economy Policy.

[69] Japan-UK EPA, Art. 8.86

[70] Counting each Member State of the European Union as one participant. https://www.wto.org/english/tratop_e/inftec_e/itscheds_e.htm (accessed on 27 October 2020)

[71] Counting each Member State of the European Union as one participant. https://www.wto.org/english/tratop_e/inftec_e/itaintro_e.htm (accessed on 27 October 2020).

4. What does this mean for the evolving digital trade environment?

110. The analysis in the previous section has shown the complex regulatory environment that underpins digital trade, highlighting the diverse fora in which rules are discussed, and identifying the number of jurisdictions that have ratified, signed, committed to, adhered to or have transcribed these regulations. Table 4.1 provides an overview of the rules covered and the different institutions that have contributed to these (referencing the section in which issues were discussed). The remainder of this section discusses the main lessons learned from the Inventory exercise and what this means for the evolving environment.

Table 4.1. The Inventory covers a wide variety of rules developed in many different fora

Broad Area	Specific area	Rules (number of jurisdictions[72]/number of JSI participants)	Number of jurisdictions signing RTAs including provisions on each issue (number of jurisdictions/number of JSI participants)
3.1. Facilitating electronic transactions	3.1.1. Electronic transaction frameworks	UN Electronic Communications Convention (26/14) UNCITRAL Model Law on Electronic Commerce (74/31) SADC Model Law on Electronic Transactions and Electronic Commerce (20/5) ESCWA Cyber Legislation Directives (16/0)	referencing the UN Electronic Communications Convention (15/12) referencing the UNCITRAL Model Law on Electronic Commerce (22/19) mentioning avoiding unnecessary barriers to ecommerce, or to minimise the regulatory burden on electronic commerce (72/66) including a principle of technological neutrality (50/50)
	3.1.2. E-authentication and e-signatures	UN Electronic Communications Convention (26/14) UNCITRAL Model Law on Electronic Commerce (74/31) UNCITRAL Model Law on Electronic Signatures (33/13) SADC Model Law on Electronic Transactions and Electronic Commerce (20/5) ESCWA Cyber Legislation Directives (16/0) ECOWAS Supplementary Act A/SA.2/01/10 on electronic transactions (15/4) UN/CEFACT recommandation (N/A) ISO 14553 (N/A)	referencing the UN Electronic Communications Convention (15/12) referencing the UNCITRAL Model Law on Electronic Commerce (22/19) including a provision on e-authentication and e-signature (87/66)
	3.1.3. Electronic contracts	UN Electronic Communications Convention (26/14) UNCITRAL Model Law on Electronic Commerce (74/31) SADC Model Law on Electronic Transactions and Electronic Commerce (20/5) ESCWA Cyber Legislation Directives (16/0) ECOWAS Supplementary Act A/SA.2/01/10 on electronic transactions (15/4)	referencing the UN Electronic Communications Convention (15/12) referencing the UNCITRAL Model Law on Electronic Commerce (22/19) including a provision on e-authentication and e-signature (87/66)
	3.1.4. Electronic invoicing	ECOWAS Supplementary Act A/SA.2/01/10 on electronic transactions (15/4) UN/CEFACT Cross Industry Invoice (N/A) ISO 20022 (N/A)	(The number is not available on the TAPED dataset)
	3.1.5. Facilitation of e-payments	WTO Trade Facilitation Agreement (153/86) OECD Recommendation of the Council on Consumer Protection in E-commerce (39/39) ISO 20022 (N/A)	(The number is not available on the TAPED dataset)
3.2. Non-discrimination and liability	3.2.1. Non-discriminatory treatment of digital products	N/A	including a provision on national treatment or MFN treatment in e-commerce (35/29)
	3.2.2. Interactive computer services	N/A	including a provision on interactive computer service (4/4)
3.3. Consumer protection	3.3.1. Online consumer protection	OECD Recommendation of the Council on Consumer Protection in E-commerce (39/39) UN Guidelines for Consumer Protection (N/A)	including a provision on consumer protection (98/76)

[72] The jurisdictions that signed, ratified, adhere to, committed to, or are influenced by rules are counted.

		SADC Model Law on Electronic Transactions and Electronic Commerce (20/5)	
	3.3.2. Unsolicited commercial electronic messages/spam	OECD Recommendation of the Council on Consumer Protection in E-commerce (39/39) SADC Model Law on Electronic Transactions and Electronic Commerce (20/5)	including a provision on unsolicited commercial electronic messages (91/73)
3.4. Digital trade facilitation and logistics	3.4.1. Paperless trading	WTO Trade Facilitation Agreement(153/86) UNECE recommendations for international trade (N/A) UN/CEFACT standards for data exchange (N/A) UN ESCAP Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific (7/3)	including a provision on paperless trading (78/70)
	3.4.2. Electronic transferrable records	UNCITRAL Model Law on Electronic Transferable Records (3/3)	(The number is not available on the TAPED dataset)
	3.4.3. Customs procedures	WTO Trade Facilitation Agreement (153/86) WCO Cross-Border E-commerce Framework of Standards (N/A) WCO SAFE Framework (N/A) UPU Universal Postal Convention and its Regulations (N/A) ASEAN Agreement on Customs (7/6)	(The number is not available on the TAPED dataset)
	3.4.4. De minimis	WTO Trade Facilitation Agreement (153/86)	(The number is not available on the TAPED dataset)
3.5. Privacy	3.5. Protection of personal information/privacy	OECD Privacy Guidelines (37/37) APEC Privacy Framework (21/19) APEC CBPR systems (9/9) Council of Europe Convention 108 (55/43) ASEAN PDP Framework (10/8) AU Malabo Convention (19/1) ECOWAS Supplementary Act A/SA. 1/01/10 on Personal Data Protection (15/4) Data Protection Standards of the Ibero-American States (10/9) ISO/IEC 27701 (N/A)	including a provision on data protection (103/79) including provisions on data protection recognizing certain international standards (78/60)
3.6. Flow of Information	3.6.1. Cross-border transfer of information by electronic means	OECD Privacy Guidelines (37/37) APEC Privacy Framework (21/19) APEC CBPR systems (9/9) Council of Europe Convention 108 (55/43) ASEAN PDP Framework (10/8) AU Malabo Convention (19/1) ECOWAS Supplementary Act A/SA. 1/01/10 on Personal Data Protection (15/4) Data Protection Standards of the Ibero-American States (10/9)	including a provision on cross-border data flow (73/56)
	3.6.2. Location of computing facilities	N/A	including a provision on location of computing facilities (19/17)
	3.6.3. Location of financial computing facilities	N/A	(The number is not available on the TAPED dataset)
3.7. Cybersecurity	3.7. Cybersecurity	UN Charter and international law (N/A) The Wassenaar Arrangement (42/40) OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity (39/39) OECD Recommendation on Digital Security of Critical Activities (38/38) The Council of Europe Budapest Convention (68/52) AU Malabo Convention (19/1) ESCWA Cyber Legislation Directives (16/0) ECOWAS Directive C/DIR/1/08/11 on Fighting Cyber Crime (15/4) ISO/IEC 27000 family, IEC 62443 (N/A) IEEF standards on cybersecurity (N/A)	including provisions on cyber security (66/61)

3.8. Telecoms	3.8. Updating the telecommunications reference paper	WTO Telecommunications Reference Paper (103/69)[73] ITU-T Recommendations (N/A) ISO/IEC standards on telecommunications (N/A) Standards by TIA, ETSI, IETF (N/A)	(The number is not available on the TAPED dataset)
3.9. Customs duties	3.9. Customs duties on electronic transmissions	N/A	including provisions on the non-imposition of custom duties (90/70)
3.10. Access to internet and data	3.10.1. Open government data	G8 Open Data Charter (8/8) OECD Recommendation on Public Sector Information (38/38)	including provisions on open government data (7/7)
	3.10.2. Access to the internet	Internet standards by IEEE-SA, IETF, IAB, W3C, Internet Society (N/A)	including provisions on access to the Internet (46/44)
	3.10.3. Access to online platforms/competition	ICN Recommended Practices and Recommendations (N/A) OECD Recommendation concerning International Co-operation on Competition Investigations and Proceedings (40/40) Bilateral or Plurilateral Co-operation agreements on competition (N/A)	(The number is not available on the TAPED dataset)
3.11 Business trust	3.11.1 Source code	WTO TBT agreement WTO TRIPS Agreement	including provisions on source code (42/41)
	3.11. 2. ICT products that use cryptography	WTO TBT agreement WTO TRIPS Agreement OECD Guidelines for Cryptography Policy (37/37) ISO/IEC 18033	including provisions on cryptography (5/5)
3.12. Market Access	3.12.1. Services market access	WTO GATS	(Many RTAs include rules on services market access)
	3.12.2. Goods market access	WTO GATT Information Technology Agreement (81/68) Expanded Information Technology Agreement (53/52)	(RTAs usually include rules on goods market access)

Source: Author's compilation, See Annex A and B.

4.1. Development and spread of international rules

111. In terms of international rules that have been ratified, signed, committed to or adhered to this analysis suggests that the most widely accepted are in the areas of trade facilitation, telecommunications and goods market access for ICT products, with progress made mainly under WTO processes. The TFA has been ratified by all 86 JSI participants (153 WTO Members overall) while the Telecommunications Reference Paper has been committed by 66 JSI participants (103 WTO Members). There is also a high degree of convergence around some elements of goods market access for ICT products, with 68 JSI participants having ratified the ITA and more than half of the JSI participants having ratified the expanded ITA (See Figure 4.1 and Annex Table C1).

112. Other areas where JSI participants share the adoption of common policy principles are cybersecurity, privacy, online consumer protection and cryptography. Here, the OECD has made strong contributions through its non-binding Guidelines or Recommendations. Although these have been agreed to by about half of the JSI participants, there are no indications of whether non-JSI participants agree to these.[74] The Council of Europe has also played an important role in the areas of cybersecurity and privacy through binding conventions. Its Convention on Cybercrime (Budapest Convention) has been signed by

[73] The numbers include states partly committing to the telecom reference paper.

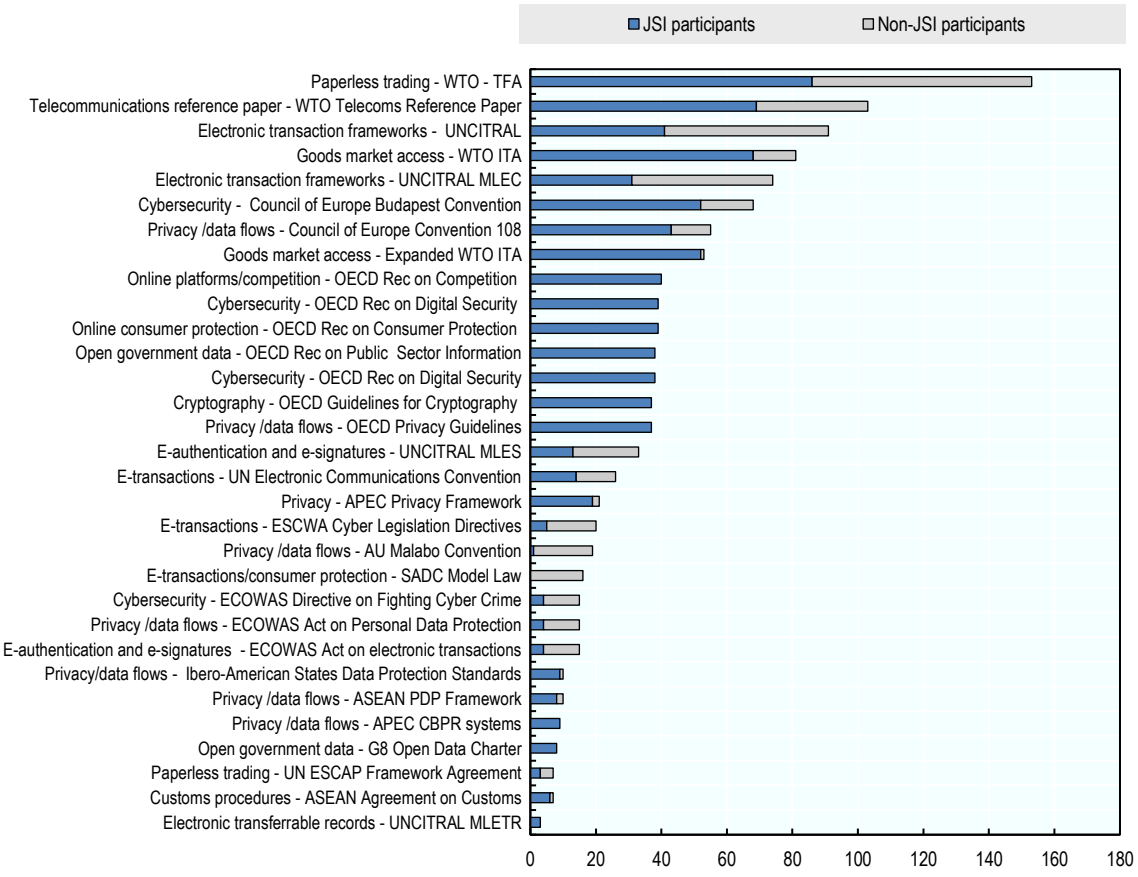
[74] The OECD Recommendation concerning International Co-operation on Competition Investigations and Proceedings is mainly designed to facilitate co-operation among government rather than to provide regulatory principles.

52 JSI participants (68 jurisdictions overall) while the Convention 108 has been signed by 43 JSI participants (55 jurisdictions overall).

113. In the area of electronic transactions, the UN (UNCITRAL) instruments such as the UN Electronic Communication Convention and the UNCITRAL Model Law on Electronic Commerce have exercised substantial influence on domestic legislation, including in the context of RTAs. About half of JSI participants and 50 non-JSI participants have been influenced by these instruments.

Figure 4.1. Adherence to international instruments varies widely

Number of jurisdictions that adhere or agree to international instruments



Note: WTO agreements applying to all WTO members, such as GATT, GATS and the TBT agreement, are excluded from the table.
Source: Author's analysis based on information in Annex B (see also Annex Table C1).

114. Rules developed in regional fora such as APEC, ASEAN, AU, SADC, ECOWAS and ESCWA have mainly focused on electronic transaction frameworks and cross-border information transfer/protection of personal information. As a result, these areas have the most rules established globally across regions (Table 4.3). In total, 109 jurisdictions (41 JSI participants) have adopted one or more international instruments on electronic transaction frameworks, including UNCITRAL Model Law on Electronic Commerce and the UN Electronic Communication Convention. At the same time, 103 jurisdictions (69 JSI participants) have adopted elements of protection on personal information, including Council of Europe Convention 108 and OECD Privacy Guidelines (Table 4.2).

Table 4.2. Many jurisdictions are now influenced by international instruments on electronic transaction frameworks and privacy protection

	jurisdictions	JSI participants
Total number of jurisdictions influenced by international instruments on electronic transaction frameworks	109	41
Total number of jurisdictions influenced by international instruments on protection on personal information	103	69

Source: Author's calculation based on the analysis based on information in Annex B.

115. There is also overlap across international instruments that have been cross-referenced in different fora (Table 4.3). For example, in terms of consumer protection, the UN Guidelines for Consumer Protection references the OECD Recommendation of the Council on Consumer Protection in E-commerce and RTAs also reference other tools such as the APEC CBPR or the OECD Privacy Guidelines.

Table 4.3. Impacts of international instruments increase through being referenced by others

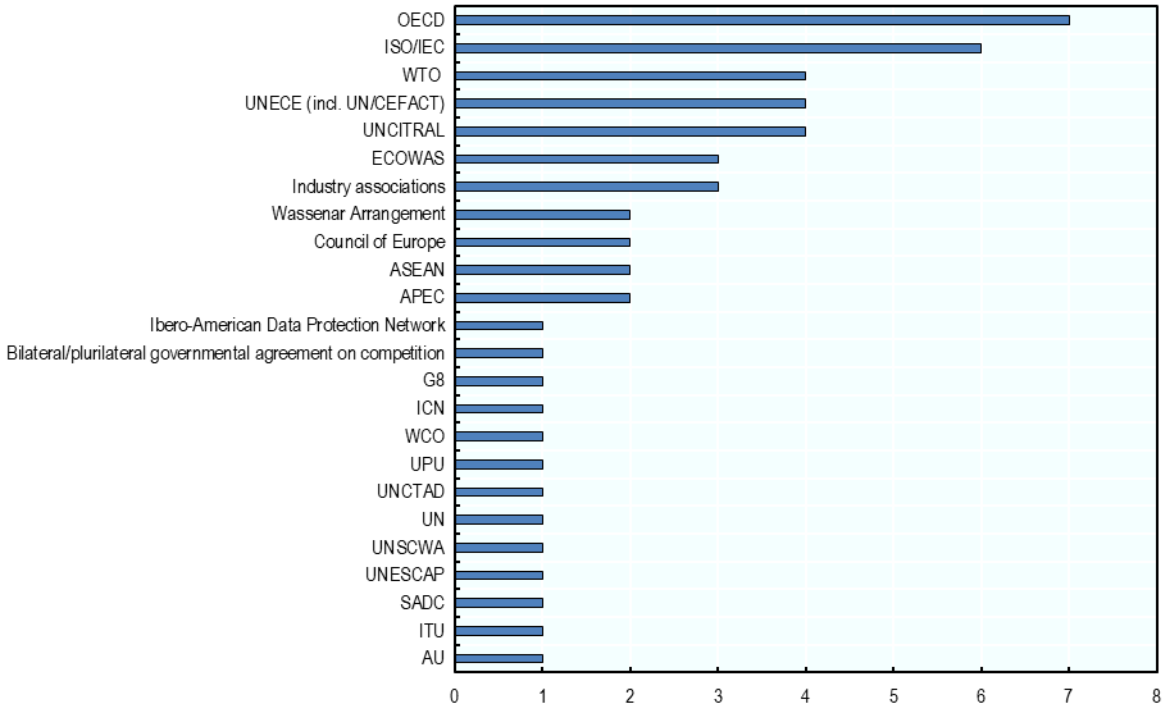
Broad areas	Specific areas	Examples of references
Facilitating electronic transactions	Electronic transaction frameworks	RTAs such as the CPTPP and DEPA references the UN Electronic Communication Convention or the UNCITRAL Model Law on Electronic Commerce
Consumer protection	Online consumer protection	UN Guidelines for Consumer Protection references OECD Recommendation of the Council on Consumer Protection in E-commerce.
Digital facilitation and logistics	Electronic transferrable records	SADEA and DEPA reference UNCITRAL Model Law on Electronic Transferable Records
	Customs procedures	EU-Japan EPA references the WCO SAFE Framework
Privacy	Privacy: Protection of personal information/privacy	RTAs such as the USMCA and the SADEA references the APEC Privacy Framework/APEC CBPR System and the OECD Privacy Guidelines
Facilitating electronic transactions	Electronic invoicing	DEPA requires that measures related to e-invoicing are based on international standards
Facilitating electronic transactions	Facilitation of e-payments	Parties of DEPA agree to take into account internationally accepted payment standards

Source: Based on author's analysis based on information in Annex A.

116. In terms of the fora that have contributed to the rules and principles that underpin digital trade, different organisations have contributed to different areas in global discussions. These have involved a range of UN agencies, such as UNCITRAL, UNECE (including UN/CEFACT), UN ESCWA and UN ESCAP, especially in the areas of electronic transactions and trade facilitations and the ITU, the UPU and UNCTAD. But other organisations such as the WCO, the OECD, the Council of Europe, APEC, SADC, ASEAN, and the African Union have also established rules relevant to digital trade across a range of areas. ISO and the IEC are also playing a role in setting standards (Figure 4.2). Each organisation has a different membership and mandate and therefore touches on different issues with different jurisdictions (See Annex Table C2).

Figure 4.2. A wide variety of fora establish a different array of rules

Number of instruments covered by the Inventory by forum



Note: WTO agreements applying to all WTO Members, such as GATT, GATS and the TBT Agreement, are excluded from the table.
Source: Author's analysis based on information in Annex B (see also Annex Table C2)

4.2. RTAs' contribution to development of rules

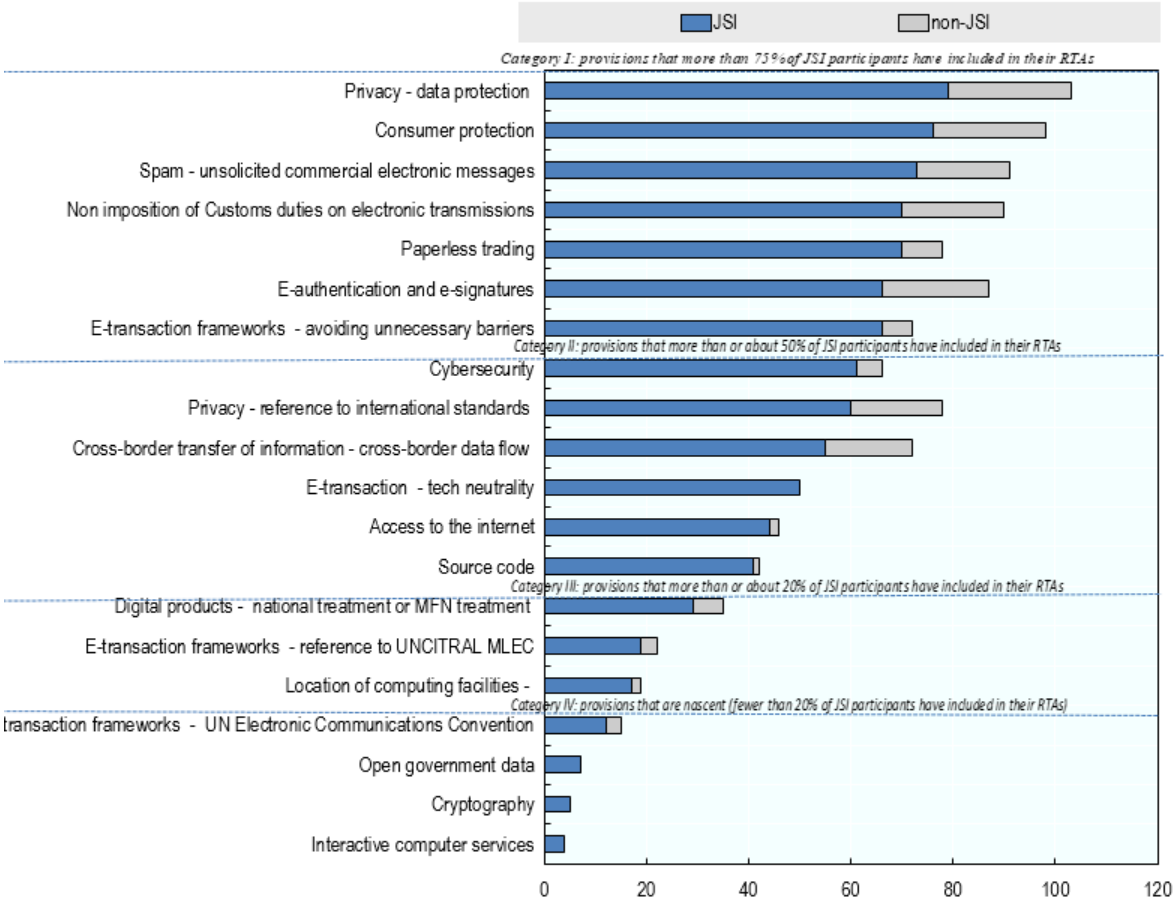
117. RTAs have played an important role in developing rules across a range of areas that are of importance to digital trade, although the depth and density of these varies (Figure 4.3 and Annex Table C3). RTA provisions can be sub-divided into different categories indicating the broad coverage of different provisions. The first category includes widely accepted provisions where more than 75% of JSI participants have signed RTAs provisions. This category includes issues such as: data protection (including provisions on data protection recognition of certain international standards), consumer protection, unsolicited commercial electronic messages, non-imposition of custom duties, e-authentication and e-signature, paperless trading and electronic transaction framework. Many of these provisions are included in the RTAs that more than, or about half, of WTO Members have signed.

118. The second category includes provisions in RTAs that more than, or about half, of the JSI participants have signed. This category includes: access to the Internet, cross-border data flows, and source code. The third category covers provisions that are not as widely accepted. More than or about 20% of the JSI participants have signed RTAs with provisions on national treatment or MFN treatment in e-commerce, reference to UNCITRAL Model Law on Electronic Commerce and location of computing facilities.

119. The last category includes provisions that are still in a nascent stage. Provisions on reference to the UN Electronic Communication Convention, open government data, ICT products that use cryptography and interactive computer service fall into this category.

Figure 4.3. RTAs have wide-ranging coverage

Number of jurisdictions and coverage of issues in RTAs



Note: Descending order of JSI participants. Data on RTA provisions related to Electronic invoicing, Facilitation of e-payment, Electronic transferrable records, Customs procedures, de minimis, location of financial computing facilities, telecommunications, online platform/competition are not provided in the TAPED dataset.
Source: Author's calculation based on the TAPED dataset.

5. Conclusion

120. This Inventory provides an overview of different rules, developed across different fora that underpin digital trade. The analysis has shown the diversity of issues covered and the range of organisations involved. Indeed, the evolving digital trade regulatory landscape is complex. The Inventory identified 52 instruments directly relevant to digital trade discussions discussed across 24 fora. Currently, the areas where there is most consensus relate to trade facilitation, telecommunication and IT goods market access (owing to progress at the WTO). However, there is also strong consensus on issues related to electronic transactions, where UNCITRAL instruments have exercised substantial influence across both JSI and non JSI participants. International instruments often cross-reference each other, ensuring a high degree of complementarity, including in the context of RTAs.

121. Overall, the Inventory shows that there appears to be a relatively high degree of uptake of rules across both JSI and non-JSI participants. This implies that many countries that are currently not in the JSI discussions have already shown some interest in dealing with issues that are being discussed at the JSI. The analysis also shows that many of the rules developed across the different organisations are being picked up in trade instruments such as RTAs.

122. This Inventory shows that there is a solid basis of international instruments upon which the JSI discussions can build, and suggests that for non-JSI participants their existing and continuing efforts could facilitate eventual participation in the JSI. It is hoped that the transparency exercise represented by this Inventory will provide a common basis of understanding so that countries can better leverage their resources towards enabling more informed discussions on digital trade whether at the WTO, or other international organisations, or in developing relevant domestic policies.

References

Andrenelli, A. and J. López González (2019), "Electronic transmissions and international trade - shedding new light on the moratorium debate", *OECD Trade Policy Papers*, No. 233, OECD Publishing, Paris, https://dx.doi.org/10.1787/57b50a4b-en. [22]

Antras, P. (2003), "Firms, Contracts, and Trade Structure", *The Quarterly Journal of Economics*, Vol. 118/4, pp. 1375-1418, http://dx.doi.org/10.1162/003355303322552829. [35]

Bronckers, M. and P. Larouche (2012), "A review of the wto regime for telecommunications services", in *The World Trade Organization and Trade in Services*, Brill, http://dx.doi.org/10.1163/ej.9789004162440.1-1024.43. [21]

Burri, M. and R. Polanco Lazo (2019), "Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset", *SSRN Electronic Journal*, http://dx.doi.org/10.2139/ssrn.3482470. [9]

Burri, M. and R. Polanco (2020), "Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset", *Journal of International Economic Law*, Vol. 23/1, pp. 187-220, http://dx.doi.org/10.1093/jiel/jgz044. [4]

Cadot, O., J. Gourdon and F. van Tongeren (2018), "Estimating Ad Valorem Equivalents of Non-Tariff Measures: Combining Price-Based and Quantity-Based Approaches", *OECD Trade Policy Papers, No.25*, Vol. OECD Publishing, Paris, http://dx.doi.org/10.1787/f3cd5bdc-en. [31]

Casalini, F. and J. López González (2019), "Trade and Cross-Border Data Flows", *OECD Trade Policy Papers*, No. 220, OECD Publishing, Paris, https://dx.doi.org/10.1787/b2023a47-en. [15]

Casalini, F., J. López González and E. Moïsé (2019), "Approaches to market openness in the digital age", *OECD Trade Policy Papers*, No. 219, OECD Publishing, Paris, https://dx.doi.org/10.1787/818a7498-en. [7]

Casalini, F., J. Lopez-Gonzalez and T. Nemoto (2021), "Mapping commonalities in regulatory approaches to cross-border data transfers", *OECD Trade Policy Papers*. [18]

ECOWAS Commission (2017), *ECOWAS Directive and related texts on Cyber legislation*, https://rm.coe.int/-3148-3-2-3-nigeria-ecowas-o-3-auc-moctar-yedaly-pdf/1680748652 (accessed on 11 January 2021). [25]

Greenleaf, G. and B. Cottier (2020), "Comparing African Data Privacy Laws: International, African and Regional Commitments", *SSRN Electronic Journal*, http://dx.doi.org/10.2139/ssrn.3582478. [27]

Huang, K., S. Madnick and S. Johnson (2018), *Interactions Between Cybersecurity and International Trade: A Systematic Framework*, http://www.spiegel.de/netzwelt/netzpolitik/bnd-skandal-netbotz-baut-offenbar-hintertueren-in-seine-kameras-a-1114252.html. [19]

International Conference of Data Protection and Privacy Commissioners (2009), *The Madrid Resolution International Standards on the Protection of Personal Data and Privacy*, http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf (accessed on 7 January 2021). [28]

Latipov, O., C. McDaniel and S. Schropp (2017), "The de minimis threshold in international trade: The costs of being too low", *The World Economy*, Vol. 41/1, pp. 337-356, http://dx.doi.org/10.1111/twec.12577. [14]

López González, J. and J. Ferencz (2018), "Digital Trade and Market Openness", *OECD Trade Policy Papers*, No. 217, OECD Publishing, Paris, https://dx.doi.org/10.1787/1bd89c9a-en. [1]

López González, J. and M. Jouanjean (2017), "Digital Trade: Developing a Framework for Analysis", *OECD Trade Policy Papers*, No. 205, OECD Publishing, Paris, https://dx.doi.org/10.1787/524c8c83-en. [3]

López González, J. and S. Sorescu (2019), "Helping SMEs internationalise through trade facilitation", *OECD Trade Policy Papers*, No. 229, OECD Publishing, Paris, https://dx.doi.org/10.1787/2050e6b0-en. [11]

Lopez-Gonzalez, J. and M. Jouanjean (2017), *Digital Trade: Developing a Framework for Analysis*, OECD Publishing, Paris,, https://doi.org/10.1787/524c8c83-en. [32]

Mattoo, A. and J. Meltzer (2019), "International data flows and privacy: The conflict and its resolution", *Journal of International Economic Law*, Vol. 21/4, pp. 769-789, http://dx.doi.org/10.1093/jiel/jgy044. [16]

Meltzer, J. and K. Cameron (2019), "Cybersecurity and digital trade: getting it right", *Brookings*, https://www.brookings.edu/research/cybersecurity-and-digital-trade-getting-it-right/. [20]

Monteiro, J. and R. Teh (2017), "Provisions on Electronic Commerce in Regional Trade Agreements", *WTO Working Papers*, No. 2017/11, World Trade Organization, Geneva, https://dx.doi.org/10.30875/82592628-en. [5]

Nations Economic, U. and S. Commission for Western Asia (2007), *UN-ESCWA United Nation Economic and Social Commission for Western Asia, The ESCWA Cyber Legislation Digest Development Account Project Regional Harmonization of Cyber Legislation to Promote Knowledge Society in the Arab Region*. [26]

Nunn, N. (2007), *Relationship-Specificity, Incomplete Contracts, and the Pattern of Trade*, https://academic.oup.com/qje/article/122/2/569/1942086. [33]

OECD (2020), *"Connecting Businesses and Consumers During COVID-19: Trade in Parcels" OECD Policy Responses to Coronavirus (COVID-19)*, https://www.oecd.org/coronavirus/policy-responses/connecting-businesses-and-consumers-during-covid-19-trade-in-parcels-d18de131/. [8]

OECD (2020), *"Leveraging digital trade to fight the consequences of COVID-19", OECD Policy Responses to Coronavirus (COVID-19)*, https://www.oecd.org/coronavirus/policy-responses/leveraging-digital-trade-to-fight-the-consequences-of-covid-19-f712f404/. [2]

OECD (2020), *MAPPING APPROACHES TO DATA AND DATA FLOWS*, http://www.oecd.org/termsandconditions. [17]

OECD (2020), *Recommendation of the Council on Digital Security of Critical Activities*, http://legalinstruments.oecd.org. [30]

OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264245471-en. [29]

OECD/ADB (2019), "Open government data", in *Government at a Glance Southeast Asia 2019*, OECD Publishing, Paris, https://dx.doi.org/10.1787/672bd105-en. [23]

Spencer, B. (2005), *International Outsourcing and Incomplete Contracts*, http://www.nber.org/papers/w11418. [34]

The Royal Society (2019), *Protecting privacy in practice: The current use, development and limits of Privacy Enhancing Technologies in data analysis*, https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf. [24]

World Customs Organization (2018), *Cross-Border E-Commerce Framework of Standards*, http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/activities-and-programmes/ecommerce/wco-framework-of-standards-on-crossborder-ecommerce_en.pdf?db=web (accessed on 12 October 2020). [13]

World Economic Forum (2020), *Connecting Digital Economies: Policy Recommendations for Cross-Border Payments*, http://www.weforum.org. [37]

World Economic Forum (2020), *Connecting Digital Economies: Policy Recommendations for Cross-Border Payments*, http://www.weforum.org. [39]

World Economic Forum (2019), *The Global Governance of Online Consumer Protection and E-commerce Building Trust*, http://www.weforum.org. [10]

World Economic Forum (2018), *Addressing E-Payment Challenges in Global E-Commerce*. [38]

World Economic Forum (2017), *Making Deals in Cyberspace: What's the Problem?*, http://www3.weforum.org/docs/WEF_White_Paper_Making_Deals_in_Cyberspace.pdf. [36]

World Economic Forum (2017), *Paperless Trading: How Does It Impact the Trade System?*. [12]

Wu, M. (2017), "Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System Acknowledgements Acknowledgements". [6]

Annex A: Inventory of the rules, principles and standards relevant for digital trade

1. Facilitating electronic transactions

1.1. Electronic transaction frameworks

UNCITRAL

The United Nations Commission on International Trade Law (UNCITRAL), which was established in 1966, is a subsidiary body of the General Assembly of the UN. Its general mandate is to further the progressive harmonisation and unification of the law of international trade. UNCITRAL has since prepared a wide range of conventions, model laws and other instruments dealing with the substantive law that governs trade transactions or other aspects of business law which have an impact on international trade. While the WTO deals with "state- to state" trade policy issues, UNCITRAL deals with the laws applicable to private parties in international transactions. [75] More information is available at the UNCTRAL website.

UN Electronic Communications Convention

United Nations Convention on the Use of Electronic Communications in International Contracts (**UN Electronic Communications Convention)**, which was adopted on 23 November 2005 during the 53rd plenary meeting of the General Assembly by resolution A/60/21, provides "*a common solution to remove legal obstacles to the use of electronic communications in a manner acceptable to States with different legal, social and economic systems*" (Preamble). It aims at facilitating the use of electronic communications in international trade by assuring that contracts concluded and other communications exchanged electronically are as valid and enforceable as their traditional paper-based equivalents. To that end, the Convention incorporate three fundamental principles of e-commerce legislation, namely non-discrimination, technological neutrality and functional equivalence, which had already been established by the UNCITRAL Model Law on Electronic Commerce and the UNCITRAL Model Law on Electronic Signatures. The Convention also establishes the general principle that communications are not to be denied legal validity solely on the grounds that they were made in electronic form. More information is available at UNCITRAL website on UN Electronic Communications Convention.

UNCITRAL Model Law on Electronic Commerce (1996)

UNCITRAL Model Law on Electronic Commerce (MLEC) was adopted by UNICITRAL in 1996. This model law aims "*to enable and facilitate commerce conducted using electronic means by providing national legislators with a set of internationally acceptable rules aimed at removing legal obstacles and increasing legal predictability for electronic commerce*." [76] The MLEC was the first legislative text to incorporate the three key principles of non-discrimination, technological neutrality and functional equivalence, which are fundamental elements of e-commerce law. Although this model law is not legally-binding, all States are recommended to give favourable

[75] https://uncitral.un.org/en/about/faq/mandate_composition/history

[76] https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce

consideration to the MLEC when they enact or revise their laws on relevant topics. More information is available at the website of UNCITRAL on MLEC.

The MLEC includes the following provision:

> *Article 5. Legal recognition of data messages*
>
> *Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.*
>
> *Article 5 bis. Incorporation by reference*
>
> *(as adopted by the Commission at its thirty-first session, in June 1998)*
>
> *Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is not contained in the data message purporting to give rise to such legal effect, but is merely referred to in that data message.*

ESCWA

The *UN Economic and Social Commission for Western Asia (ESCWA)* is a regional commission created by the United Nations in 1973 in order to stimulate economic activity in member countries, strengthen cooperation between them promote development.[77]

Having taken a lead to promote digital trade in Arab region, the ESCWA published the **ESCWA Cyber Legislation Directives**, which aims at supporting Arab countries in the formulation and enactment of national cyber laws, promoting regional integration and facilitating electronic transactions among countries of the region.[78] The ESCWA Cyber Legislation Directives covers six areas: electronic communications and freedom of expression, processing personal data, cybercrime, electronic transactions and signatures, e-commerce and consumer protection, intellectual property in the fields of Information Technology and Cyberspace.

SADC

The *Southern African Development Community (SADC)* was formed in 1992 and comprises 16 Member States.[79]

Under its Harmonization of ICT Policies in the Sub-Sahara Africa (HIPSSA) project, which was executed by the International Telecommunication Union (ITU) and co-chaired by the AU, the **SADC Model Law on Electronic Transactions and Electronic Commerce** were adopted by the SADC Ministers in charge of ICT and telecommunications in 2012.[80]

---

[77] https://www.unescwa.org/about-escwa

"The five regional commissions were created by the United Nations in order to fulfil the economic and social goals set out in the Charter by promoting cooperation and integration between countries in each region of the world. Those commissions are: the Economic Commission for Europe (ECE, established in 1947); the Economic and Social Commission for Asia and the Pacific (ESCAP, 1947); the Economic Commission for Latin America and the Caribbean (ECLAC, 1948); the Economic Commission for Africa (ECA, 1958); and the Economic and Social Commission for Western Asia (ESCWA, 1973)."

[78] https://www.unescwa.org/news/escwa-launches-cyber-legislation-directives

[79] Angola, Botswana, Comoros, Democratic Republic of the Congo, Kingdom of Eswatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, United Republic of Tanzania, Zambia and Zimbabwe https://ccdcoe.org/organisations/sadc/

[80] https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_e-transactions.pdf

The SADC Model Law "seeks to enhance regional integration and has adopted the best practices and collective efforts of Member States to address the legal aspects of e-transactions and e-commerce" (Preamble). As it is a model law, it is non-binding and there is no ratification process.

The SADC Model Law includes the following provisions:

> *Section 4: Legal recognition of electronic communications*
>
> *A data message shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic communication.*
>
> *Section 5: Recognition by parties of electronic communications*
>
> *Between the originator and the addressee of an electronic communication, a declaration of will, other statement or action shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of an electronic communication.*

Box 1. Examples of RTA provisions on electronic transaction framework

CPTPP

Article 14.5: Domestic Electronic Transactions Framework

1. Each Party shall maintain a legal framework governing electronic transactions consistent with the principles of the UNCITRAL Model Law on Electronic Commerce 1996 or the United Nations Convention on the Use of Electronic Communications in International Contracts, done at New York, November 23, 2005.

2. Each Party shall endeavour to: (a) avoid any unnecessary regulatory burden on electronic transactions; and (b) facilitate input by interested persons in the development of its legal framework for electronic transactions.

The ASEAN Agreement on Electronic Commerce

Article 5 Principles

1. In the development and promotion of e-commerce, the role of each Member State shall be geared towards providing an enabling legal and regulatory environment, providing a conducive and competitive business environment, and protecting the public interest.

2. Each Member State shall maintain, or adopt as soon as practicable, laws and regulations governing electronic transactions taking into account applicable international conventions or model laws relating to e-commerce.

3. Each Member State shall encourage the use of alternative dispute resolution to facilitate the resolution of claims e-commerce transactions.

4. Member States shall endeavour to recognise the importance of the principle of technology neutrality and recognise the need for alignment in policy and regulatory approaches among Member States to facilitate cross border e-commerce.

RCEP

Article 12.10: Domestic Regulatory Framework

1. Each Party shall adopt or maintain a legal framework governing electronic transactions, taking into account the UNCITRAL Model Law on Electronic Commerce 1996, the United Nations Convention on the Use of

Electronic Communications in International Contracts done at New York on 23 November 2005, or other applicable international conventions and model laws relating to electronic commerce.[81]

2. Each Party shall endeavour to avoid any unnecessary regulatory burden on electronic transactions.

1.2. E-authentication and e-signatures

UNCITRAL

UN Electronic Communications Convention

The UN Electronic Communications Convention (see section 1.1 in this annex) sets out the following criteria for establishing the functional equivalence between electronic communications and paper documents, as well as between electronic authentication methods and handwritten signatures:

Article 9. Form requirements

1. Nothing in this Convention requires a communication or a contract to be made or evidenced in any particular form.

2. Where the law requires that a communication or a contract should be in writing, or provides consequences for the absence of a writing, that requirement is met by an electronic communication if the information contained therein is accessible so as to be usable for subsequent reference.

3. Where the law requires that a communication or a contract should be signed by a party, or provides consequences for the absence of a signature, that requirement is met in relation to an electronic communication if:

(a) A method is used to identify the party and to indicate that party's intention in respect of the information contained in the electronic communication; and

(b) The method used is either:

(i) As reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or

(ii) Proven in fact to have fulfilled the functions described in subparagraph (a) above, by itself or together with further evidence.[82,83]

[81] Footnote 10: *Cambodia shall not be obliged to apply this paragraph for a period of five years after the date of entry into force of this Agreement.*

[82] The purpose of various techniques currently available on the market or still under development is to offer the technical means by which some or all of the functions identified as characteristic of handwritten signatures can be performed in an electronic environment. Such techniques may be referred to broadly as "electronic signatures" (Explanatory note by the UNCITRAL secretariat on the United Nations Convention on the Use of Electronic Communications in International Contracts)

[83] The Convention does not attempt to identify specific technological equivalents to particular functions of handwritten signatures. Instead, it establishes the general conditions under which electronic communications would be regarded as authenticated with sufficient credibility and would be enforceable in the face of signature requirements. Focusing on the two basic functions of a signature, paragraph 3 (a) of article 9 establishes the principle that, in an electronic environment, the basic legal functions of a signature are performed by way of a method that identifies the originator of an electronic communication and indicates the originator's intention in respect of the information contained in the electronic communication. " (Explanatory note by the UNCITRAL secretariat on the United Nations Convention on the Use of Electronic Communications in International Contracts)

4. Where the law requires that a communication or a contract should be made available or retained in its original form, or provides consequences for the absence of an original, that requirement is met in relation to an electronic communication if:

(a) There exists a reliable assurance as to the integrity of the information it contains from the time when it was first generated in its final form, as an electronic communication or otherwise; and

(b) Where it is required that the information it contains be made available, that information is capable of being displayed to the person to whom it is to be made available.

5. For the purposes of paragraph 4 (a):

(a) The criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage and display; and

(b) The standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

UNCITRAL Model Law on Electronic Commerce (1996)

The UNCITRAL Model Law on Electronic Commerce (see section 1.1 in this annex) also includes model provisions for data message and electronic signature to establish the functional equivalence between electronic communications and paper documents, as well as between electronic authentication methods and handwritten signatures:[84]

Article 6. Writing

(1) Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.

(3) The provisions of this article do not apply to the following: [...].

Article 7. Signature

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) The provisions of this article do not apply to the following: [...].

UNCITRAL Model Law on Electronic Signatures (2001)

UNCITRAL Model Law on Electronic Signatures was adopted by UNCITRAL in 2001. It aims to enhance legal certainty in electronic commerce by "*the harmonization of certain rules on the legal recognition of electronic signatures on a technologically neutral basis and by the establishment of a method to assess in a technologically neutral manner the practical reliability and the commercial adequacy of electronic signature techniques*" (Preamble).

[84] https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-04970_ebook.pdf

Although it is not legally binding, General Assembly resolution 56/80[85] recommends that all states give favourable consideration to the Model Law on Electronic Signatures, together with the Model Law on Electronic Commerce, when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based forms of communication, storage and authentication of information. More information is available at UNCITRAL website on the model law.

Building on the fundamental principles underlying article 7 of the UNCITRAL Model Law on Electronic Commerce, the Model Law on Electronic Signatures stipulates, among others: Equal treatment of signature technologies; Compliance with a requirement for a signature; Conduct of the signatory; Conduct of the certification service provider; and Recognition of foreign certificates and electronic signatures.

UNECE and UN/CEFACT

T*he United Nations Economic Commission for Europe (UNECE)*, which was set up in 1947, is one of five regional commissions of the United Nations.[86] *The United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT)* is a subsidiary, intergovernmental body of the UNECE, which serves as a focal point within the United Nations Economic and Social Council for trade facilitation recommendations and electronic business standards. It has global membership and its members are experts from intergovernmental organizations, individual countries' authorities and also from the business community.[87]

As described below *Paperless trading* (see section 4.1 in this annex), the UNECE has developed a series of recommendations and standards for international trade in the context of trade facilitation. Its Recommendation 14 "*seeks to encourage the use of electronic data transfer in international trade by recommending that Governments review national and international requirements for signatures on international trade documents, in order to eliminate the requirement for paper documents by meeting the requirement for signatures through authentication methods or guarantees, which can be electronically transmitted.*"

SADC

The **SADC Model Law on Electronic Transactions and Electronic Commerce** (see section 1.1 in this annex) includes the following model provisions for an electronic communication and electronic signature to establish the functional equivalence between electronic communications and paper documents, as well as between electronic authentication methods and handwritten signatures:

> *Section 6: Writing*
>
> *(1) Where a law requires information to be in writing, that requirement is met by an electronic communication if the information contained therein is accessible so as to be usable for subsequent reference.*
>
> *(2) Subsection 1 applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.*
>
> *(…)*
>
> *Section 7: Signature*
>
> *(1) If a law requires the signature of a person, an electronic signature will be deemed to be valid, provided the electronic signature complies with the requirements as prescribed by Regulation.*
>
> *(2) The requirements for an electronic signature referred to in subsection 1 above will be met if:*

[85] https://undocs.org/en/A/RES/56/80

[86] https://www.unece.org/mission.html

[87] https://www.unece.org/cefact.html

a. the method is used to identify the person and to indicate the person's intention in regard to the information communicated; and

b. at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated in light of all the relevant circumstances.

(3) Where two persons or parties agree to make use of electronic signatures they may agree to use any method of signing as they deem appropriate.

(4) Subsection (1) applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(5) The provisions of this section do not apply to the requirement for a signature for the following acts: (…)

Section 8: Creation and recognition of secure electronic signature

(1) Member States may by Regulation provide that accredited authentication products or services are recognised as a secure electronic signature and may prescribe certain standards and licensing procedures for such products or services including the recognition of foreign, secure electronic signatures.

(2) Any recognition granted in terms of this sub-section 1 should be consistent with generally recognized international technical standards.

(3) Where a secure electronic signature has been used, the signature is regarded as being a valid electronic signature and having been applied properly, unless the contrary is proved.

(4) Electronic signatures that are not secure electronic signatures are not subject to the presumptions set out in subsection 3 above and section 18 below.

Section 9: Incorporation by reference

Information shall not be denied legal effect, validity or enforceability solely on the ground that it is not contained in the electronic communication purporting to give rise to such legal effect, validity or enforceability, but is merely referred to in that electronic communication.

ECOWAS

In order to establish a harmonized legal framework to regulate electronic transactions, *the ECOWAS* has developed the **Supplementary Act A/SA.2/01/10 on electronic transactions within ECOWAS** in 2010. As of June 2017, 9 countries had enacted laws on electronic transaction (ECOWAS Commission, 2017[25]).[88] The Supplementary Act includes the following rules on electronic signatures:

Article 34: Electronic Signature

1) Electronic signature consists of the use of a reliable identification process guaranteeing its link with the document to which it is attached. It shall be accepted in electronic transactions.

2) The process shall be presumed reliable when the electronic signature is created, until the evidence is shown to the contrary.

Article 35: Conditions of acceptance of electronic signature

An electronic signature created by a secure arrangement that the signatory can maintain under his exclusive control, which is based on a digital certificate, shall be accepted as a signature in like manner as a handwritten signature.

[88] Benin, Burkina Faso, Cabo Verde, Cote dÍvoire, Gambia, Ghana, Guinea, Niger, Senegal (note that this does not assess the consistency of these laws with the Supplementary Act).

ESCWA

The ESCWA Cyber Legislation Directives (see section 1.1 in this annex) includes chapters on:

- Electronic Records and Signatures
- the duties and responsibilities of the certification service provider or the owner of the certification and the relying party
- Legal recognition of countries outside the Arab region of electronic certification.
- Banking and Financial Transactions[89]

ISO

International Organization for Standardization (ISO) is an independent, non-governmental international organization with a membership of 165 national standards bodies. It develops voluntary, consensus-based, market relevant international standards that support innovation and provide solutions to global challenges.[90] ISO has more than 300 ISO technical committees (TC) developing standards covering a myriad of sectors.[91]

ISO 14533, which was developed by ISO/TC 154, *Processes, data elements and documents in commerce, industry and administration*, will help business and governments guarantee the long-term authenticity of electronic signatures. Following the requirements of ISO 14533 will also ensure the interoperability of electronic signatures when the documents they authenticate are transferred and processed through different information technology systems. Users who will benefit from the standards include organizations and governments who wish to preserve, or are mandated to preserve, electronic documents for a long period of time. These include organizations who wish to store electronic messages (such as EDI and XML based), agreements, contracts, or other documents.[92]

This standard consists of three parts:

- ISO 14533-1:2012, *Processes, data elements and documents in commerce, industry and administration – Long term signature profiles* – Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)
- ISO 14533-2:2012, *Processes, data elements and documents in commerce, industry and administration – Long term signature profiles* – Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)[93]
- ISO 14533-3:2017, *Processes, data elements and documents in commerce, industry and administration – Long term signature profiles* – Part 3: Long term signature profiles for PDF Advanced Electronic Signatures (PAdES)[94]

[89] (Nations Economic and Commission for Western Asia, 2007[26])

[90] https://www.iso.org/about-us.html

[91] https://www.iso.org/technical-committees.html

[92] https://www.iso.org/news/2013/02/Ref1706.html

[93] https://www.iso.org/news/2013/02/Ref1706.html

[94] https://www.iso.org/standard/67937.html

Box 2. Examples of RTA provisions on e-authentication and e-signatures

EU-Japan EPA

Article 8.77 Electronic authentication and electronic signature

1. Unless otherwise provided for in its laws and regulations, a Party shall not deny the legal validity of a signature solely on the grounds that the signature is in electronic form.

2. A Party shall not adopt or maintain measures regulating electronic authentication and electronic signature that would:

(a) prohibit parties to an electronic transaction from mutually determining the appropriate electronic authentication methods for their transaction; or

(b) prevent parties to electronic transactions from having the opportunity to establish before judicial or administrative authorities that their electronic transactions comply with any legal requirements with respect to electronic authentication and electronic signature.

3. Notwithstanding paragraph 2, each Party may require that, for a particular category of transactions, the method of authentication meets certain performance standards or is certified by an authority accredited in accordance with its laws and regulations.

The ASEAN Agreement on Electronic Commerce

Article 7.2 Electronic Authentication and Electronic Signatures

(a) Except in circumstances otherwise provided for under its laws and regulations, a Member State shall not deny the legal validity of a signature solely on the basis that the signature is in electronic form.

(b) Each Member State shall maintain or adopt, as soon as practicable, measures based on international norms for electronic authentication that:

(i) permit participants in electronic transactions to determine the appropriate authentication technologies and implementation models for their electronic transactions;

(ii) do not limit the recognition of authentication technologies and implementation models; and

(iii) permit participants in electronic transactions to have the opportunity to prove that their electronic transactions comply with that Member State's laws and regulations with respect to authentication,

[…]

1.3. Electronic contracts

UNCITRAL

UN Electronic Communications Convention

The UN Electronic Communications Convention (see section 1.1 in this annex) includes the following provision on validity or enforceability of e-contracts:

Article 8. Legal recognition of electronic communications

1. A communication or a contract shall not be denied validity or enforceability on the sole ground that it is in the form of an electronic communication.[95]

UNCITRAL Model Law on Electronic Commerce (1996)

The UNCITRAL Model Law on Electronic Commerce (see section 1.1 in this annex) includes the following provision on validity or enforceability of e-contracts:

Article 11. Formation and validity of contracts

(1) In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.

(2) The provisions of this article do not apply to the following: [...].

SADC

The **SADC Model Law on Electronic Transactions and Electronic Commerce** (see section 1.1 in this annex) includes the following provisions on validity or enforceability of e-contracts. It also contains provisions on time of dispatch of electronic communications, time of receipt of electronic communications, place of dispatch and receipt of electronic communications, time of contract formation and automated message systems.

Section 10: Formation and validity of contracts

(1) Where electronic communications are used in the formation of a contract, that contract shall not be denied legal effect, validity or enforceability on the sole ground that an electronic communication was used to make an offer or to accept an offer for that purpose.

(2) A proposal to conclude a contract made through one or more electronic communications, which is not addressed to one or more specific parties but is generally accessible to parties making use of information systems (including proposals that make use of interactive applications for the placement of orders through such information systems) is to be considered as an invitation to make offers, unless it clearly indicates the intention of the party making the proposal to be bound in case of acceptance.

ECOWAS

Supplementary Act A/SA.2/01/10 on electronic transactions within ECOWAS includes provisions on electronic contract negotiation, transmission of contract information by electronic means, etc.

1.4. Electronic invoicing

ECOWAS

Supplementary Act A/SA.2/01/10 on electronic transactions within ECOWAS includes the following provision on electronic invoicing:

[95] This provision means that "there should be no disparity of treatment between electronic communications and paper documents", indicating that the form in which certain information is presented or retained cannot be used as the only reason for which that information would be denied legal effectiveness, validity or enforceability". However, "this provision should not be misinterpreted as establishing the absolute legal validity of any given electronic communication or of any information contained therein". (Explanatory note by the UNCITRAL secretariat on the United Nations Convention on the Use of Electronic Communications in International Contracts).

Article29: Electronic document accepted for invoicing

An electronic document shall be accepted for invoicing in the same manner as a hard copy, as long as the authenticity of the origin of data contained therein and the integrity of their content can be guaranteed.

UN/CEFACT

The *UN/CEFACT* developed the **Cross Industry Invoice (CII)**, a technical specification on invoice that can be used to create message syntax which can be exchanged globally between trading partners.[96] According to (World Economic Forum, 2017[12]), the EU has decided that all public institutions that accept and may require electronic invoices, must accept the CII as one of the official standards for the submission of electronic invoices.

ISO

Building on the UN/CEFACT's Cross Industry Invoice (CII) data model, *ISO* developed **ISO 20022 Financial Invoice**, a global message, standardized under ISO20022. It covers all current financial identified requirements both in terms of the invoice message itself as well as the integration to other financial messaging such as payment initiation, direct debits, card payments, invoice financing and trade service utility.[97]

Box 3. Example of RTA provisions on electronic invoice

DEPA

Article 2.5: Electronic Invoicing

1. The Parties recognise the importance of E-invoicing which increases the efficiency, accuracy and reliability of commercial transactions. The Parties also recognise the benefits of ensuring that the systems used for E-invoicing within their territory are interoperable with the systems used for E-invoicing in the other Parties' territories.

2. Each Party shall ensure that the implementation of measures related to e-invoicing in its jurisdiction is designed to support cross-border interoperability. For that purpose, Parties shall base their measures related to e-invoicing on international standards, guidelines or recommendations, where they exist.

3. The Parties recognise the economic importance of promoting the global adoption of interoperable e-invoicing systems. To this end, the Parties shall share best practices and collaborate on promoting the adoption of interoperable systems for e-invoicing.

4. The Parties agree to cooperate and collaborate on initiatives which promote, encourage, support or facilitate the adoption of e-invoicing by businesses. To this end, the Parties shall endeavour to:

(a) promote the existence of underlying infrastructure to support e-invoicing; and

(b) generate awareness of and build capacity for e-invoicing.

[96] http://tfig.unece.org/contents/cross-industry-invoice-cii.htm

[97] https://www.finextra.com/blogposting/5108/this-is-iso20022-invoice-message-standard

1.5. Facilitation of e-payments

WTO

Trade Facilitation Agreement (see section 4.1 in this annex) includes the following provision on e-payment. However, this provision only covers e-payment that is used in the context of Customs clearance.

> *ARTICLE 7: RELEASE AND CLEARANCE OF GOODS*
>
> *2 Electronic Payment*
>
> *Each Member shall, to the extent practicable, adopt or maintain procedures allowing the option of electronic payment for duties, taxes, fees, and charges collected by Customs incurred upon importation and exportation.*

OECD

The **OECD Recommendation of the Council on Consumer Protection in E-commerce** (see section 3.1 in this annex) includes the following provision on e-payments.

> *E. Payment*
>
> *40. Businesses should provide consumers with easy-to-use payment mechanisms and implement security measures that are commensurate with payment-related risks, including those resulting from unauthorised access or use of personal data, fraud and identity theft.*
>
> *41. Governments and stakeholders should work together to develop minimum levels of consumer protection for e-commerce payments, regardless of the payment mechanism used. Such protection should include regulatory or industry-led limitations on consumer liability for unauthorised or fraudulent charges, as well as chargeback mechanisms, when appropriate. The development of other payment arrangements that may enhance consumer confidence in e-commerce, such as escrow services, should also be encouraged.*
>
> *42. Governments and stakeholders should explore other areas where greater harmonisation of payment protection rules among jurisdictions would be beneficial and seek to clarify how issues involving cross-border transactions could be best addressed when payment protection levels differ.*

ISO

ISO 20022 was first published in 2004 and is now widely recognized as an interoperable payments standard. The standard currently includes financial transaction categories: Payments, Retail Cards, Trade Service, Foreign Exchange and Securities.

According to 20022Labs.com, ISO 20022 may:

- allow for transmission of more remittance information with a payment, with the flexibility to adapt to a given need or context, which can support innovation that reduce costs and creates value.
- allow the financial services industry to consolidate a variety of existing standards, which will reduce the cost and effort associated with supporting multiple standards, support innovation, and enable third-party service providers
- enhance global interoperability among countries that adopt ISO 20022, which facilitate cross-border payments.[98]

[98] https://20022labs.com/what-is-iso-20022/

As of September 2019, according to asianbankingandfinance.net, ISO 20022 has been adopted by market infrastructures in more than 70 countries, for payments and securities business, and is projected to dominate high-value payments, supporting 79% of the volume and 87% of the value of transactions worldwide by 2024.[99]

Box 4. Example of RTA provisions on e-payment

DEPA

Article 2.7: Electronic Payments[100]

1. Noting the rapid growth of electronic payments, in particular, those provided by new payment service providers, Parties agree to support the development of efficient, safe and secure cross border electronic payments by fostering the adoption and use of internationally accepted standards, promoting interoperability and the interlinking of payment infrastructures, and encouraging useful innovation and competition in the payments ecosystem.

2. To this end, and in accordance with their domestic legislation, Parties recognise the following principles:

(a) Parties shall make regulations on electronic payments, including regulatory approval, licensing requirements, procedures and technical standards, publicly available in a timely manner.

(b) Parties agree to take into account internationally accepted payment standards to enable greater interoperability between payment systems.

(c) Parties agree to promote the use of Application Programming Interface (API) and to encourage financial institutions and payment service providers to make available APIs of their financial products, services and transactions to third party players where possible to facilitate greater interoperability and innovation in the electronic payments ecosystem.

(d) Parties shall endeavour to enable cross-border authentication and electronic knowyour- customer of individuals and businesses using digital identities;

(e) Parties recognise the importance of upholding safety, efficiency, trust and security in electronic payment systems through regulation. The implementation of regulation should where appropriate be proportionate to and commensurate with the risks posed by the provision of electronic payment systems.

(f) Parties agree policies should promote innovation and competition in a level playing field and recognise the importance of enabling the introduction of new financial and electronic payment products and services by incumbents and new entrants in a timely manner such as through adopting regulatory and industry sandboxes.

ASEAN Agreement on Electronic Commerce

Article 9. Electronic Payment

1. Member States recognise the importance of safe and secure, efficient, and interoperable e-payment systems while taking into account the readiness of each Member State in terms of capacity, infrastructure, and regulation f e-payment systems

99 https://asianbankingandfinance.net/co-written-partner/sponsored-articles/iso-20022-common-standard-transform-global-payments

100 Footnote 8: *For greater certainty, nothing in this Article shall be construed to impose an obligation on a Party to modify its domestic rules on payments, including, inter alia, the need to obtain licences or permits or the approval of access applications.*

2. Each Member State shall encourage the use of safe and secure, efficient, and interoperable e-payment systems to facilitate e-commerce in accordance with its laws and regulations.

2. Non-discrimination and liability

2.1. Non-discriminatory treatment of digital products

WTO

The **GATT** requires a Member not to discriminate between its trading partners (most-favoured-nation treatment (Art. 1)) and between its own and foreign products (national treatment (Art. 3)).

The **GATS** also requires that foreign services be accorded most-favoured-nation treatment (Art. 2). However, national treatment (Art. 17) is not required to be accorded unless Members have made specific commitments in their schedules.

Box 5. Example of RTA provisions on non-discriminatory treatment of digital products

USMCA

Article 19.4: Non-Discriminatory Treatment of Digital Products

1. No Party shall accord less favourable treatment to a digital product created, produced, published, contracted for, commissioned, or first made available on commercial terms in the territory of another Party, or to a digital product of which the author, performer, producer, developer, or owner is a person of another Party, than it accords to other like digital products.[101]

2. This Article does not apply to a subsidy or grant provided by a Party, including a government-supported loan, guarantee, or insurance.

Japan-US digital trade agreement

Article 8 Non-Discriminatory Treatment of Digital Products

1. Neither Party shall accord less favourable treatment to a digital product created, produced, published, contracted for, commissioned, or first made available on commercial terms in the territory of the other Party, or to a digital product of which the author, performer, producer, developer, or owner is a person of the other Party, than it accords to other like digital products.[102]

2. This Article does not apply to subsidies or grants provided by a Party, including government-supported loans, guarantees, and insurance.

3. For greater certainty, nothing in this Article prevents a Party from adopting or maintaining measures that limit the level of foreign capital participation in an enterprise engaged in the supply of broadcasting.[103]

[101] Footnote 3: *For greater certainty, to the extent that a digital product of a non-Party is a "like digital product," it will qualify as an "other like digital product" for the purposes of Article 19.4.1 (Non-Discriminatory Treatment of Digital Products).*

[102] Footnote 7: *For greater certainty, to the extent that a digital product of a third country is a "like digital product", it will qualify as an "other like digital product" for the purposes of this paragraph.*

[103] Footnote 8: *For the purposes of this paragraph, for Japan, "broadcasting" means the transmission of telecommunications with the aim of direct reception by the public (paragraph 1 of Article 2 of the Broadcast Law (Law No. 132 of 1950)) and does not include on-demand services including such services supplied over the Internet.*

4. With respect to intellectual property rights, paragraph 1 shall not apply to the extent of any inconsistency with the rights and obligations in any bilateral agreement between the Parties with respect to intellectual property or, if no such bilateral agreement exists, with the rights and obligations in any international agreement with respect to intellectual property to which both Parties are party

2.2. Interactive computer services (limiting non-IP liability for suppliers and users and infringement of persons' rights)

Development of rules on interactive computer services is sensitive and still in a nascent stage. Only few RTAs have included references to principles in this area.

Box 6. Example of RTA provisions on interactive computer service

USMCA

Article 19.17: Interactive Computer Services

1. The Parties recognize the importance of the promotion of interactive computer services, including for small and medium-sized enterprises, as vital to the growth of digital trade.

2. To that end, other than as provided in paragraph 4, no Party shall adopt or maintain measures that treat a supplier or user of an interactive computer service as an information content provider in determining liability for harms related to information stored, processed, transmitted, distributed, or made available by the service, except to the extent the supplier or user has, in whole or in part, created, or developed the information.[104]

3. No Party shall impose liability on a supplier or user of an interactive computer service on account of:

(a) any action voluntarily taken in good faith by the supplier or user to restrict access to or availability of material that is accessible or available through its supply or use of the interactive computer services and that the supplier or user considers to be harmful or objectionable; or

(b) any action taken to enable or make available the technical means that enable an information content provider or other persons to restrict access to material that it considers to be harmful or objectionable.

4. Nothing in this Article shall:

(a) apply to any measure of a Party pertaining to intellectual property, including measures addressing liability for intellectual property infringement; or

(b) be construed to enlarge or diminish a Party's ability to protect or enforce an intellectual property right; or

(c) be construed to prevent:

(i) a Party from enforcing any criminal law, or

(ii) a supplier or user of an interactive computer service from complying with a specific, lawful order of a law enforcement authority.[105]

[104] Footnote 7: *For greater certainty, a Party may comply with this Article through its laws, regulations, or application of existing legal doctrines as applied through judicial decisions.*

[105] Footnote 8: *The Parties understand that measures referenced in paragraph 4(c)(ii) shall be not inconsistent with paragraph 2 in situations where paragraph 2 is applicable.*

3. Consumer protection

3.1. Online consumer protection

UN

The United Nations Guidelines for Consumer Protection (UNGCP) were first adopted by the General Assembly in resolution 39/248 of 16 April 1985, later expanded by the Economic and Social Council in resolution E/1999/INF/2/Add.2 of 26 July 1999, and revised by the General Assembly in resolution 70/186 of 22 December 2015. The guidelines are "*a valuable set of principles for setting out the main characteristics of effective consumer protection legislation, enforcement institutions and redress systems and for assisting interested Member States in formulating and enforcing domestic and regional laws, rules and regulations that are suitable to their own economic and social and environmental circumstances, as well as promoting international enforcement cooperation among Member States and encouraging the sharing of experiences in consumer protection*" (Preface). More information is available at the UNCTAD website of the Guidelines.

The Guidelines include the following principles on e-commerce:

> *I. Electronic commerce*
>
> *63. Member States should work towards enhancing consumer confidence in electronic commerce by the continued development of transparent and effective consumer protection policies, ensuring a level of protection that is not less than that afforded in other forms of commerce.*
>
> *64. Member States should, where appropriate, review existing consumer protection policies to accommodate the special features of electronic commerce and ensure that consumers and businesses are informed and aware of their rights and obligations in the digital marketplace.*
>
> *65. Member States may wish to consider the relevant international guidelines and standards on electronic commerce and the revisions thereof, and, where appropriate, adapt those guidelines and standards to their economic, social and environmental circumstances so that they can adhere to them, as well as collaborate with other Member States in their implementation across borders. In so doing, Member States may wish to study the Guidelines for Consumer Protection in the Context of Electronic Commerce of the Organization for Economic Cooperation and Development.*

OECD

In 1999, the *OECD Council* adopted the **Recommendation of the Council concerning Guidelines for Consumer Protection in the Context of Electronic Commerce** (1999 Recommendation), the first international instrument for consumer protection in the context of e-commerce. The 1999 Recommendation included the core characteristics of consumer protection for electronic commerce: fair and transparent business and advertising practices, information about businesses, goods and services, transactions, as well as adequate dispute resolution and redress mechanisms, payment protection, privacy, and education.

Given the dramatic expansion of e-commerce that brought about new and emerging trends and challenges since 1999, the OECD Council revised the 1999 Recommendation and the new **Recommendation of the Council on Consumer Protection in E-commerce** was released in 2016 (2016 Recommendation). The 2016 Recommendation addresses the challenges identified and achieve effective consumer protection while stimulating innovation and competition in the market. Key new developments in e-commerce addressed by the 2016 Recommendation include: *Non-monetary transactions, Digital content products, Active consumers, Mobile devices, Privacy and security risks, Payment protection and Product safety*. It also sets forth the need to enhance the ability of consumer protection authorities to exchange information and co-operate in cross-border matters.

Members and non-Members of the OECD adhering to the 2016 Recommendation are recommended to work with stakeholders, such as businesses, consumer representatives and other civil society organisations, to implement the principles set forth in the Recommendation in their policy frameworks for the protection of consumers in e-commerce.

More information is available at the OECD website on OECD Guidelines for Consumer Protection in the Context of Electronic Commerce (1999).

SADC

The SADC Model Law on Electronic Transactions and Electronic Commerce (see section 1.1 in this annex) includes the following provisions:

> *Section 25: Obligations of the supplier*
>
> *(1) A supplier offering goods or services for sale, for hire or for exchange by way of an electronic transaction shall make the following information available to consumers:*
>
> *(…)*
>
> *(2) The supplier shall provide the consumer with an opportunity: –*
>
> *(…)*
>
> *Section 26: Performance*
>
> *(1) The supplier shall execute the order within 30 days after the day on which the supplier received the order, unless the parties have agreed otherwise.*
>
> *(…)*
>
> *Section 27: Cooling-off*
>
> *(1) A consumer is entitled to cancel without reason and without penalty any transaction and any related credit agreement for the supply:*
>
> *a. of goods within seven days after the date of the receipt of the goods; or*
>
> *b. of services within seven days after the date of the conclusion of the agreement.*
>
> *(…)*
>
> *Section 28: Applicability of foreign law*
>
> *(…)*
>
> *Section 29: Non-exclusion*
>
> *(…)*

ISO

ISO standards on consumer protection is under development at *ISO/PC 317 committee* while no standards have been established yet.[106]

[106] https://www.iso.org/committee/6935430.html

Box 7. Example of RTA provisions on consumer protection

CPTPP

Article 14.7: Online Consumer Protection

1. The Parties recognise the importance of adopting and maintaining transparent and effective measures to protect consumers from fraudulent and deceptive commercial activities as referred to in Article 16.6.2 (Consumer Protection) when they engage in electronic commerce.

2. Each Party shall adopt or maintain consumer protection laws to proscribe fraudulent and deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial activities.

3. The Parties recognise the importance of cooperation between their respective national consumer protection agencies or other relevant bodies on activities related to cross-border electronic commerce in order to enhance consumer welfare. To this end, the Parties affirm that the cooperation sought under Article 16.6.5 and Article 16.6.6 (Consumer Protection) includes cooperation with respect to online commercial activities.

USMCA

Article 19.7: Online Consumer Protection

1. The Parties recognize the importance of adopting and maintaining transparent and effective measures to protect consumers from fraudulent or deceptive commercial activities as referred to in Article 21.4.2 (Consumer Protection) when they engage in digital trade.

2. Each Party shall adopt or maintain consumer protection laws to proscribe fraudulent and deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial activities.

3. The Parties recognize the importance of, and public interest in, cooperation between their respective national consumer protection agencies or other relevant bodies on activities related to cross-border digital trade in order to enhance consumer welfare. To this end, the Parties affirm that cooperation under paragraphs 21.4.3 through 21.4.5 (Consumer Protection) includes cooperation with respect to online commercial activities.

EU-Japan EPA

Article 8.78 Consumer protection

1. The Parties recognise the importance of adopting and maintaining transparent and effective consumer protection measures applicable to electronic commerce as well as measures conducive to the development of consumer confidence in electronic commerce.

2. The Parties recognise the importance of cooperation between their respective competent authorities in charge of consumer protection on activities related to electronic commerce in order to enhance consumer protection.

3. The Parties recognise the importance of adopting or maintaining measures, in accordance with their respective laws and regulations, to protect the personal data of electronic commerce users.

ASEAN Agreement on Electronic

Article 7.3. Online Consumer Protection

(a) Member States recognize the importance of adopting and maintaining transparent and effective consumer protection measures for e-commerce as well as other measures conducive to the development of consumer confidence.

(b) Each Member State shall provide protection for consumers using e-commerce that affords a similar level of protection to that provided for consumers of other forms of commerce under its relevant laws, regulations and policies

(c) Member States recognize the importance of cooperation between their respective competent authorities in charge of consumer protection on activities related to e-commerce

3.2. Unsolicited commercial electronic messages/spam

OECD

OECD Recommendation of the Council on Consumer Protection in E-commerce includes the following provision on unsolicited commercial electronic message (see section 3.1 in this annex):

B. Fair Business, Advertising and Marketing Practices

22. Businesses should develop and implement effective and easy-to-use procedures that allow consumers to choose whether or not they wish to receive unsolicited commercial messages, whether by e-mail or other electronic means. When consumers have indicated, at any time, that they do not want to receive such messages, their choice should be respected.

SADC

The SADC Model Law on Electronic Transactions and Electronic Commerce (see section 1.1 in this annex) includes the following provisions on unsolicited commercial communications:

Section 30: Unsolicited commercial communications

(1) Marketing by means of electronic communication shall provide the addressee with:

a. the originator's identity and contact details including its place of business, e-mail, addresses and telefax number(s);

b. a valid and operational opt-out facility from receiving similar communications in future; and

c. the identifying particulars of the source from which the originator obtained the addressee's personal information.

(2) Unsolicited commercial communications may only be sent to addressees where the opt-in requirement is met.

(3) The opt-in requirement will be deemed to have been met where:

a. the addressee's e-mail address and other personal information was collected by the originator of the message "in the course of a sale or negotiations for a sale";

b. the originator only sends promotional messages relating to its "similar products and services" to the addressee;

c. when the personal information and address was collected by the originator, the originator offered the addressee the opportunity to opt-out (free of charge except for the cost of transmission) and the addressee declined to opt-out; and

d. the opportunity to opt-out is provided by the originator to the addressee with every subsequent message.

(4) No contract is formed where an addressee does not respond to an unsolicited commercial communication.

(5) An originator who fails to provide the recipient with an operational opt-out facility referred to in subsections 1b and 3d is guilty of an offence and liable, on conviction, to the penalties prescribed in subsection 8.

(6) Any originator who persists in sending unsolicited commercial communications to an addressee, who has opted out from receiving any further electronic communications from the originator through the originator's opt-out facility, is guilty of an offence and liable, on conviction, to the penalties prescribed in subsection 8.

(7) Any party whose goods or services are advertised in contravention of this section is guilty of an offence and liable, on conviction, to the penalties prescribed in subsection 8.

(8) A person convicted of an offence referred to in this section is liable on conviction to a fine or imprisonment for a period not exceeding five years.

Box 8. Example of RTA provisions on unsolicited commercial electronic messages

CPTPP

Article 14.14: Unsolicited Commercial Electronic Messages[107]

1. Each Party shall adopt or maintain measures regarding unsolicited commercial electronic messages that:

(a) require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages;

(b) require the consent, as specified according to the laws and regulations of each Party, of recipients to receive commercial electronic messages; or

(c) otherwise provide for the minimisation of unsolicited commercial electronic messages.

2. Each Party shall provide recourse against suppliers of unsolicited commercial electronic messages that do not comply with the measures adopted or maintained pursuant to paragraph 1.

3. The Parties shall endeavour to cooperate in appropriate cases of mutual concern regarding the regulation of unsolicited commercial electronic messages.

USMCA

Article 19.13: Unsolicited Commercial Electronic Communications

1. Each Party shall adopt or maintain measures providing for the limitation of unsolicited commercial electronic communications.

2. Each Party shall adopt or maintain measures regarding unsolicited commercial electronic communications sent to an electronic mail address that:

(a) require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages; or

(b) require the consent, as specified in the laws and regulations of each Party, of recipients to receive commercial electronic messages.

3. Each Party shall endeavor to adopt or maintain measures that enable consumers to reduce or prevent unsolicited commercial electronic communications sent other than to an electronic mail address.

4. Each Party shall provide recourse in its law against suppliers of unsolicited commercial electronic communications that do not comply with a measure adopted or maintained pursuant to paragraph 2 or 3.

[107] Footnote 8: *Brunei Darussalam is not required to apply this Article before the date on which it implements its legal framework regarding unsolicited commercial electronic messages.*

5. The Parties shall endeavor to cooperate in appropriate cases of mutual concern regarding the regulation of unsolicited commercial electronic communications.

EU-JAPAN EPA

Article 8.79 Unsolicited commercial electronic messages

1. Each Party shall adopt or maintain measures regarding unsolicited commercial electronic messages that:

(a) require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages; and

(b) require the prior consent, as specified according to its laws and regulations, of recipients to receive commercial electronic messages.

2. Each Party shall ensure that commercial electronic messages are clearly identifiable as such, clearly disclose on whose behalf they are made, and contain the necessary information to enable recipients to request cessation free of charge and at any time.

3. Each Party shall provide recourse against suppliers of unsolicited commercial electronic messages that do not comply with the measures adopted or maintained pursuant to paragraphs 1 and 2.

4. Digital trade facilitation and logistics

4.1. Paperless trading

WTO

In 2013, WTO members concluded negotiations on the **Trade facilitation agreement (TFA)**, which entered into force in February 2017 following its ratification by two-thirds of the WTO membership. It aims to further expedite the movement, release and clearance of goods, including goods in transit, and enhance assistance and support for capacity building of developing and least-developed country Members and promote the effective cooperation among Members on trade facilitation and customs compliance issues (Preamble). More information is available at the WTO website of the agreement.

The TFA contains provisions that would promote paperless trade:

Art. 7.1 Pre-arrival processing

1.2. Each Member shall, as appropriate, provide for advance lodging of documents in electronic format for pre-arrival processing of such documents.

Art. 10.2 Acceptance of Copies

2.1 Each Member shall, where appropriate, endeavour to accept paper or electronic copies of supporting documents required for import, export, or transit formalities.

2.2 Where a government agency of a Member already holds the original of such a document, any other agency of that Member shall accept a paper or electronic copy, where applicable, from the agency holding the original in lieu of the original document.

Art. 10.4 Single Window

4.1 Members shall endeavour to establish or maintain a single window, enabling traders to submit documentation and/or data requirements for importation, exportation, or transit of goods through a single entry point to the participating authorities or agencies. After the examination by the participating authorities

or agencies of the documentation and/or data, the results shall be notified to the applicants through the single window in a timely manner.

UNECE and UN/CEFACT

Recommendations

The *UNECE* (see section 1.2 in this annex) has developed and maintained a series of **recommendations for international trade**. The recommendations reflect best practices in trade procedures and data and documentary requirements. These non-obligatory norm have played a key role to simplify and harmonise international trade procedures and information flows (World Economic Forum, 2017[12]).[108]

For instance, Recommendation 25, which was adapted at the Working Party on Facilitation of International Trade Procedures, a subsidiary body of the UNECE, recommends governments to use the UN/EDIFACT standards "*for international applications of electronic data interchange (EDI) among different parties within the public sector as well as between public authorities on the one hand and parties of the private sector on the other hand*."[109] Recommendation 33 on Single Window also recommends governments to "*actively consider the possibility of implementing a Single Window facility in their country that allows: parties involved in trade and transport to lodge standardized information and documents with a single entry point to fulfil all import, export, and transit-related regulatory requirements. If information is electronic, then individual data elements should only be submitted once*".

As codified information is an integral part of data exchange in international business, the UN/CEFACT also develops, maintains and publishes a number of code lists used extensively in business transactions as Code List Recommendations. Those recommendations encourage participants in international trade the use of certain codes for, for instance, representation of currencies, time, names of countries. All of its recommendations are available at the UNECE website.

Standards

The *UNECE* has also established **standards for data exchange**. For instance, **the United Nations rules for Electronic Data Interchange for Administration, Commerce and Transport (UN/EDIFACT)** is a set of internationally agreed standards, directories, and guidelines for the electronic interchange of structured data, between independent computerized information systems.[110] "UN/EDIFACT was the dominant messaging syntax throughout the 1990s and remains likely the most widely used single standard for data exchange – especially since it is freely available and is regularly updated" (World Economic Forum, 2017[12]). The UN/CEFACT also offers a standardized XML, a syntax provides higher flexibility in the structure, length and format.[111]

UN ESCAP

The Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific was adopted as a UN treaty on 19 May 2016, led by *UN Economic and Social Commission for Asia and the Pacific (ESCAP).*[112] The objective of the framework agreement is "*to promote cross-border paperless trade by enabling the exchange and mutual recognition of trade-related data and documents in electronic form and facilitating*

[108] https://www.unece.org/uncefact/tfrecs.html

[109] https://www.unece.org/fileadmin/DAM/cefact/recommendations/rec25/rec25_95_r1079rev1e.pdf

[110] https://www.unece.org/cefact/edifact/welcome.html

[111] Other organizations, such as International Organization of Standards (ISO) committees, the World Customs Organization (WCO), the International Air Transport Association (IATA), also provide XML standards. (World Economic Forum, 2017[12])

[112] https://www.unescap.org/resources/framework-agreement-facilitation-cross-border-paperless-trade-asia-and-pacific-0#

interoperability among national and subregional single windows and/or other paperless trade systems, for the purpose of making international trade transactions more efficient and transparent while improving regulatory compliance" (Art. 1). The framework agreement, which is wholly dedicated to the facilitation of paperless trade, in particular cross-border, is complementary to the WTO TFA:[113] implementing the regional arrangement is expected to help ESCAP member states to easily meet relevant requirements of the TFA.[114]

The framework agreement stipulates seven general principles (Functional equivalence; Non-discrimination of the use of electronic communications; Technological neutrality; Promotion of interoperability; Improved trade facilitation and regulatory compliance; Cooperation between the public and private sectors; Improving transboundary trust environment) and key provisions (e.g., Facilitation of cross-border paperless trade and development of single-window systems, Cross-border mutual recognition of trade-related data documents in electronic form and International standards for exchange of trade-related data and documents in electronic form).

Article 7

Facilitation of cross-border paperless trade and development of single-window systems

1. The Parties shall endeavour to facilitate cross-border paperless trade by enabling exchange of trade-related data and documents in electronic form, utilizing the existing systems in operation or creating new systems.

2. The Parties are encouraged to develop single-window systems and use them for cross-border paperless trade. In developing single-window systems or upgrading existing ones, the Parties are encouraged to make them consistent with the general principles provided in the present Framework Agreement.

Article 8

Cross-border mutual recognition of trade-related data and documents in electronic form

1. The Parties shall provide for mutual recognition of trade-related data and documents in electronic form originating from other Parties on the basis of a substantially equivalent level of reliability.

2. The substantially equivalent level of reliability would be mutually agreed upon among the Parties through the institutional arrangement established under the present Framework Agreement.

3. The Parties may enter into bilateral and multilateral arrangements to operationalize cross-border mutual recognition of trade-related data and documents in electronic form, in a manner consistent with the principle of the transboundary trust environment and all the other general principles, provided that the provisions of these bilateral and multilateral arrangements do not contradict the present Framework Agreement.

Article 9

International standards for exchange of trade-related data and documents in electronic form

1. The Parties shall endeavour to apply international standards and guidelines in order to ensure interoperability in paperless trade and to develop safe, secure and reliable means of communication for the exchange of data.

2. The Parties shall endeavour to become involved in the development of international standards and best practices related to cross-border paperless trade.

[113] https://www.unescap.org/sites/default/files/FAQ%20on%20the%20Framework%20Agreement_Nov%202016.pdf

[114] https://www.unescap.org/sites/default/files/FAQ%20on%20the%20Framework%20Agreement_Nov%202016.pdf

Box 9. Example of RTA provisions on paperless trading

CPTPP

Article 14.9: Paperless Trading

Each Party shall endeavour to:

(a) make trade administration documents available to the public in electronic form; and

(b) accept trade administration documents submitted electronically as the legal equivalent of the paper version of those documents.

DEPA

Article 2.2: Paperless Trading

1. Each Party shall make publicly available, including through a process prescribed by that Party, electronic versions of all existing publicly available trade administration documents.[115]

2. Each Party shall provide electronic versions of trade administration documents referred to in paragraph 1 in English or any of the other official languages of the WTO, and shall endeavour to provide such electronic versions in a machine-readable format.

3. Each Party shall accept electronic versions of trade administration documents as the legal equivalent of paper documents, except where: (a) there is a domestic or international legal requirement to the contrary; or (b) doing so would reduce the effectiveness of trade administration.

4. Noting the obligations in the WTO Trade Facilitation Agreement, each Party shall establish or maintain a single window that enables persons to submit documentation or data requirements for importation, exportation, or transit of goods through a single entry point to the participating authorities or agencies.

5. The Parties shall endeavour to establish or maintain a seamless, trusted, high availability[116] *and secure interconnection of their respective single windows to facilitate the exchange of data relating to trade administration documents, which may include: (a) sanitary and phytosanitary certificates; (b) import and export data; or (c) any other documents, as jointly determined by the Parties, and in doing so, the Parties shall provide public access to a list of such documents and make this list of documents available online.*

6. The Parties recognise the importance of facilitating, where relevant in each jurisdiction, the exchange of electronic records used in commercial trading activities between the Parties' businesses.

7. The Parties shall endeavour to develop systems to support the exchange of: (a) data relating to trade administration documents referred to in paragraph 5 between the competent authorities of each Party;[117] *and (b) electronic records used in commercial trading activities between the Parties' businesses, where relevant in each jurisdiction.*

8. The Parties recognise that the data exchange systems referred to in paragraph 7 should be compatible and interoperable with each other. To this end, the Parties recognise the role of internationally recognised and, if available, open standards in the development and governance of the data exchange systems.

[115] Footnote 2: *For greater certainty, electronic versions of trade administration documents include trade administration documents provided in a machine-readable format.*

[116] Footnote 3: *For greater certainty, "high availability" refers to the ability of a single window to continuously operate. It does not prescribe a specific standard of availability.*

[117] Footnote 4: *The Parties recognise that the data exchange systems referred to in this paragraph may refer to interconnection of the single windows referred to in paragraph 5.*

9. The Parties shall cooperate and collaborate on new initiatives which promote and advance the use and adoption of the data exchange systems referred to in paragraph 7, including but not limited to, through: (a) sharing of information, experiences and best practices in the area of development and governance of the data exchange systems; and (b) collaboration on pilot projects in the development and governance of data exchange systems.

10. The Parties shall cooperate bilaterally and in international fora to enhance acceptance of electronic versions of trade administration documents and electronic records used in commercial trading activities between businesses.

11. In developing other initiatives which provide for the use of paperless trading, each Party shall endeavour to take into account the methods agreed by relevant international organisations.

ASEAN Agreement on Electronic Commerce

Article 7.1. Paperless trading

Each Member State shall expand the use of electronic versions of trade administration documents and facilitate the exchange of electronic documents through the use of ICT consistent with the provisions of the ASEAN Agreement on Customs signed on 30 March 2012 in Phnom Penh, Cambodia, and other international agreements on paperless trading to with Member States are parties.

4.2. Electronic transferrable records

UNCITRAL

The Model Law on Electronic Transferable Records (MLETR), which was adapted by the UN General Assembly in July 2017, aims to enable the legal use of electronic transferable records both domestically and across borders.[118] The MLETR builds on the principles of non-discrimination against the use of electronic means, functional equivalence and technology neutrality underpinning all UNCITRAL texts on electronic commerce.[119] While electronic transferable records may be particularly relevant for certain business areas such as transport and logistics, they could also promote paperless trade. More information is available at the UNCITEAL website on the Model law.

The MLETR includes, among others, the following provisions:

> *Article 10. Transferable documents or instruments*
>
> *1. Where the law requires a transferable document or instrument, that requirement is met by an electronic record if:*
>
> *(a) The electronic record contains the information that would be required to be contained in a transferable document or instrument; and*
>
> *(b) A reliable method is used:*
>
> > *(i) To identify that electronic record as the electronic transferable record;*
> >
> > *(ii) To render that electronic record capable of being subject to control from its creation until it ceases to have any effect or validity; and*
> >
> > *(iii) To retain the integrity of that electronic record.*

[118] https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records

[119] https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records

Article 11. Control

1. Where the law requires or permits the possession of a transferable document or instrument, that requirement is met with respect to an electronic transferable record if a reliable method is used:

(a) To establish exclusive control of that electronic transferable record by a person; and

(b) To identify that person as the person in control.

Article 19. Non-discrimination of foreign electronic transferable records

1. An electronic transferable record shall not be denied legal effect, validity or enforceability on the sole ground that it was issued or used abroad.

Box 10. Example of RTA provisions on Electronic transferrable records

SADEA

Article 8 Domestic Electronic Transactions Framework

4. The Parties recognise the importance of developing mechanisms to facilitate the use of electronic transferrable records. To this end, in developing such mechanisms, the Parties shall endeavour to take into account, as appropriate, relevant model legislative texts developed and adopted by international bodies, such as the UNCITRAL Model Law on Electronic Transferable Records (2017).

DEPA

Article 2.3. Domestic Electronic Transactions Framework

2. Each Party shall endeavour to adopt the UNCITRAL Model Law on Electronic Transferable Records (2017).

4.3. Customs procedures

WTO

The **TFA** (see section 4.1 in this annex) broadly includes rules and principles to expedite the movement, release and clearance of goods. For instance, Art. 10 stipulates rules on customs procedures regarding formalities and documentation requirements, acceptance of copies (including electronic copies), use of international standards, single window and pre-shipment inspection.

WCO

Key characteristics of e-commerce cross border transactions, such as time-sensitive goods flow, high volumes of small packages, participation of unknown players, return/refund processes, have brought about challenges to Customs administrations with regards to trade facilitation and security, fair and efficient collection of duties and taxes, protection of society. *The World Customs Organization (WCO)*, an independent intergovernmental body whose mission is to enhance the effectiveness and efficiency of Customs administrations, has engaged with all relevant stakeholders with a view to collectively defining the appropriate approach to deal with those challenges.[120] It has developed various tools that support e-commerce, including the followings, which are available at the WCO website.

[120] http://www.wcoomd.org/en/topics/facilitation/activities-and-programmes/ecommerce.aspx

Framework of Standards on Cross-Border E-Commerce[121]

In 2018, the WCO developed **Cross-Border E-commerce Framework of Standards**, which should be used by Customs administrations, other relevant government agencies and e-commerce stakeholders for harmonized implementation. Those global standards support cross-border e-commerce, contributing to national and global economic development, while at the same time ensuring appropriate controls to protect economies, societies and environments that include natural and production areas in both terrestrial and aquatic environments.[122]

Those 15 standards cover the following eight aspects of e-commerce:

- Advance Electronic Data and Risk Management;
- Facilitation and Simplification;
- Safety and Security;
- Revenue Collection;
- Measurement and Analysis;
- Partnerships;
- Public Awareness, Outreach and Capacity Building; and
- Legislative Frameworks.

SAFE Framework[123]

The SAFE Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework) was adopted by the WCO Council in June 2005 to serve as a deterrent to international terrorism, secure revenue collections and promote trade facilitation worldwide.[124] It aims, among other, to establish standards that provide supply chain security and facilitation at a global level to promote certainty and predictability; and strengthen co-operation between Customs administrations, Customs/government agencies and Customs/Business. It is updated every three years to ensure that it remains relevant and reflects new opportunities, challenges and associated solutions.[125]

The SAFE framework consists of four elements:[126]

- harmonizes the advance electronic cargo information requirements on inbound, outbound and transit shipments
- each country that joins the SAFE Framework commits to employing a consistent risk management approach to address security threats
- requires that at the reasonable request of the receiving nation, based upon a comparable risk targeting methodology, the sending nation's Customs administration will perform an outbound inspection of high-risk cargo and/or transport conveyances, preferably using non-intrusive detection equipment such as large-scale X-ray machines and radiation detectors.

121 http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/activities-and-programmes/ecommerce/wco-framework-of-standards-on-crossborder-ecommerce_en.pdf?db=web

122 http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/activities-and-programmes/ecommerce/wco-framework-of-standards-on-crossborder-ecommerce_en.pdf?db=web

123 http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/safe-package/safe-framework-of-standards.pdf?la=en

124 http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/upu/joint-wco-upu-guidelines.pdf?la=en

125 http://www.wcoomd.org/en/media/newsroom/2018/july/wco-publishes-2018-edition-of-safe-framework-of-standards.aspx

126 http://www.wcoomd.org/en/media/newsroom/2018/july/wco-publishes-2018-edition-of-safe-framework-of-standards.aspx

- suggests benefits that Customs will provide to businesses that meet minimal supply chain security standards and best practices.

The 2018 edition of the SAFE Framework includes conditions, requirements and benefits of Authorized Economic Operators (AEO).

UPU

With its 192 member countries, the *Universal Postal Union (UPU)* is the primary forum for cooperation between postal sector players. It helps to ensure a truly universal network of up-to-date products and services. The UPU sets the rules for international mail exchanges and makes recommendations to stimulate growth in mail, parcel and financial services volumes and improve quality of service for customers.[127] The rules established by the UPU include the Universal Postal Convention, its Additional/Final Protocol, and its Regulations, as well as the Postal Payment Services Agreement, its Additional/Final Protocol, and its Regulations.[128] It also develops technical standards and Electronic Data Interchange (EDI) messaging specifications that facilitate the exchange of operational information between postal operators.[129] A catalogue of UPU standards is available at the UPU website.

Its **Universal Postal Convention** and **Regulations** include the rules applicable throughout the international postal service and the provisions concerning the letter-post and postal parcels services. These Acts are binding on all member countries, which must ensure that their designated operators (DOs) fulfil the obligations arising from the Convention and its Regulations.[130]

Article 8 of the Universal Postal Convention urges DOs to make efforts to develop a mechanism for sending electronic advanced data (EAD) on international postal shipments, to be used for both customs and aviation security purposes:[131]

> *Article 8 Postal security*
>
> *1 Member countries and their designated operators shall observe the security requirements defined in the UPU security standards and shall adopt and implement a proactive security strategy at all levels of postal operations to maintain and enhance the confidence of the general public in the postal services provided by designated operators, in the interests of all officials involved. This strategy shall include the objectives defined in the Regulations, as well as the principle of complying with requirements for providing electronic advance data on postal items identified in implementing provisions (including the type of, and criteria for, postal items) adopted by the Council of Administration and Postal Operations Council, in accordance with UPU technical messaging standards. The strategy shall also include the exchange of information on maintaining the safe and secure transport and transit of mails between member countries and their designated operators.* (underlining added)
>
> *2 Any security measures applied in the international postal transport chain must be commensurate with the risks or threats that they seek to address, and must be implemented without hampering worldwide mail flows or trade by taking into consideration the specificities of the mail network. Security measures that have a potential global impact on postal operations must be implemented in an internationally coordinated and balanced manner, with the involvement of the relevant stakeholders.*

[127] https://www.upu.int/en/Universal-Postal-Union

[128] https://www.upu.int/en/Universal-Postal-Union/About-UPU/Acts

[129] https://www.upu.int/en/Postal-Solutions/Programmes-Services/Standards

[130] https://www.upu.int/en/Universal-Postal-Union/About-UPU/Acts

[131] http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/upu/joint-wco-upu-guidelines.pdf?la=en

Article 08-002 of the Regulations to the Convention (Implementing provisions for providing electronic advance data) also includes the following provisions:

> *2 Each item for which electronic advance data is provided shall be accompanied by the appropriate UPU customs declaration form.*
>
> *3 The electronic advance data required to meet such requirements shall, in all cases, replicate data documented on the appropriate UPU customs declaration form.*

Other UPU tools and instruments that could be used to design and implement processes involving the exchange of data are provided in **WCO–UPU guidelines on the exchange of electronic advance data (EAD) between designated operators and customs administrations**.[132]

ASEAN

ASEAN Agreement on Customs signed in 2012 and entered into force in November 2014.[133] The agreement is intended to simplify and harmonise Customs valuation, tariff nomenclature and Customs procedures.

Box 11. Example of RTA provisions on customs procedures

EU-Japan EPA

ARTICLE 4.4 Procedures for import, export and transit

1. Each Party shall apply its customs legislation and other trade-related laws and regulations in a predictable, consistent, transparent and non-discriminatory manner.

2. Each Party shall ensure that its customs procedures:

(a) are consistent with international standards and recommended practices applicable to each Party in the area of customs procedures such as those made under the auspices of the World Customs Organization[134] (hereinafter referred to as "the WCO"), including the substantive elements of the Protocol of Amendment to the International Convention on the Simplification and Harmonization of Customs Procedures, done at Brussels on 26 June 1999, the International Convention on the Harmonized Commodity Description and Coding System, done at Brussels on 14 June 1983, and the Framework of Standards to Secure and Facilitate Global Trade of the WCO (hereinafter referred to as "the SAFE Framework");

(b) aim at facilitating legitimate trade, taking into account the evolution of trade practices, while securing compliance with its laws and regulations;

(c) provide for effective enforcement in case of breaches of its laws and regulations concerning customs procedures, including duty evasion and smuggling; and

(d) do not include mandatory use of customs brokers or preshipment inspections.

3. Each Party shall adopt or maintain measures granting favourable treatment with respect to customs controls prior to the release of goods to traders or operators fulfilling criteria specified in its laws and regulations.

---

132 http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/upu/joint-wco-upu-guidelines.pdf?la=en (Accessed on 10 November 2020)

133 https://asean.org/?static_post=asean-agreement-on-customs

134 Footnote 1: *For greater certainty, the WCO was established in 1952 as the Customs Co-operation Council (CCC).*

4. Each Party shall promote the development and use of advanced systems, including those based on information and communications technology, to facilitate the exchange of electronic data between traders or operators and its customs authority and other trade-related agencies.

5. Each Party shall work towards further simplification and standardisation of data and documentation required by its customs authority and other trade-related agencies.

4.4. De minimis

WTO

The TFA includes the following provision on *de minimis*:

> *Art. 7.8.2 (d)*
>
> *(Each Member shall) provide, to the extent possible, for a de minimis shipment value or dutiable amount for which customs duties and taxes will not be collected, aside from certain prescribed goods. Internal taxes, such as value added taxes and excise taxes, applied to imports consistently with Article III of the GATT 1994 are not subject to this provision.*

Box 12. Example of RTA provisions on *de minimis*

USMCA

Article 7.8: Express Shipments

1. Each Party shall adopt or maintain specific expedited customs procedures for express shipments while maintaining appropriate customs controls. These procedures shall […]:

(f) provide that, under normal circumstances, no customs duties or taxes will be assessed at the time or point of importation or formal entry procedures required,[135] on express shipments of a Party valued at or below a fixed amount set out under the Party's law, provided that the shipment does not form part of a series of shipments carried out or planned for the purpose of evading duties or taxes, or avoiding any regulation applicable to the formal entry procedures required by the importing Party. The fixed amount set out under the Party's law shall be at least:[136]

(i) for the United States, US$800,

(ii) for Mexico, US$117 for customs duties and US$50 for taxes, and

(iii) for Canada, C$150 for customs duties and C$40 for taxes.

[135] Footnote 2: *For greater certainty, this subparagraph shall not prevent a Party from requiring informal entry procedures, including applicable supporting documents.*

[136] Footnote 3: *Notwithstanding the amounts set out under this subparagraph, a Party may impose a reciprocal amount that is lower for shipments from another Party if the amount provided for under that other Party's law is lower than that of the Party.*

5. Privacy: Protection of personal information/privacy

OECD

OECD Privacy Guidelines

Data flow governance has been a recurring focus of OECD work for over 40 years. Work in the 1970s led to **the OECD's 1980 Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data ("OECD Privacy Guidelines")**. The Guidelines are designed to ensure the protection of privacy whilst encouraging transborder flows of personal data with trust. They represent the first internationally agreed set of privacy principles that apply to the protection of personal data whether in the public or private sector. The Guidelines are drafted in technologically neutral language and are non-binding. The Guidelines were revised in 2013 to address a profound change of scale in terms of the role of personal data in economies, societies, and daily lives.

The Guidelines laid out principles on: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability.

The Guidelines also recommend states to develop national privacy strategies that reflect a co-ordinated approach across governmental bodies and establish and maintain privacy enforcement authorities. It also encourages states to co-operate on privacy matters and support the development of international arrangements that promote interoperability among privacy frameworks.

The Guidelines continue to be implemented by countries through legislation, enforcement and policy measures, and have influenced developments in privacy law, principle and practice even beyond OECD countries. For instance, the APEC Privacy Framework, which aims at promoting electronic commerce throughout the Asia Pacific region, is consistent with the core values of the OECD Guidelines, and reaffirms the value of privacy to individuals and to the information society. More information is available at the OECD website on the Guidelines.

OECD Recommendation of the Council on Consumer Protection in E-commerce

OECD Recommendation of the Council on Consumer Protection in E-commerce (see section 3.1 in this annex) also includes the following provision on consumer privacy:

> *G. Privacy and Security*
>
> *48. Businesses should protect consumer privacy by ensuring that their practices relating to the collection and use of consumer data are lawful, transparent and fair, enable consumer participation and choice, and provide reasonable security safeguards.*

APEC

APEC Privacy Framework is a principles-based model for national privacy laws that encourages the development of appropriate information privacy protection and ensuring the free flow of information in the Asia Pacific region. The APEC Privacy Framework was first endorsed in 2005 and updated in 2015.

Building on APEC Privacy Framework, member economies have developed the **CBPR System** (Cross-Border Privacy Rules), a government-backed data privacy certification framework that companies can join to demonstrate compliance with agreed privacy protection principles and enforcement mechanisms, allowing them to transfer data between CBPR participating economies with greater trust.[137] The CBPR System is not mandatory for APEC

[137] The APEC CBPR System requires participating businesses to implement data privacy policies consistent with the APEC Privacy Framework, a principles-based model for national privacy laws that encourages the development of appropriate

economies, and even when an economy adheres to it, companies can choose whether to seek certification under the System. However, once a company acquires the CBPR certification, it assumes liability under the CBPR framework.[138] To date, nine economies[139] have participated to the APEC CBPR System and more than 30 companies have acquired the CBPR certifications. More information is available at the APEC website on the CBPR System.

Council of Europe

The **1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**, commonly referred to as **Convention 108 of the Council of Europe**, is a binding treaty protecting the right to privacy of individuals with respect to personal data which is automatically processed. To date, fifty-five states have committed to establish, under their own domestic law, sanctions and remedies for violations of the Convention's provisions. The 2018 Amending Protocol, when it enters into force, will update the provisions on the flow of personal data between signatories (creating what is commonly known as **Convention 108+**). More information is available here.

AU

In 2014, the African Union adopted the **Convention on Cyber Security and Personal Data Protection (Malabo Convention)**. The Convention includes principles on personal data protection, which targets protecting privacy without prejudice to the principle of free flow of personal data. To date, 14 countries have signed the Convention and 5 countries have ratified it, while ratification of 15 countries is required for the Convention to enter into force.[140]

ASEAN

In 2016, ASEAN Member States adopted **ASEAN Framework on Personal Data Protection (ASEAN PDP Framework)**, which sets out principles of personal data protection for the Member States to implement in their domestic laws. In 2018, building on the ASEAN PDP Framework, ASEAN endorsed the **ASEAN Framework on Digital Data Governance** that sets out strategic priorities, principles and initiatives to guide ASEAN Member States in their policy and regulatory approaches towards digital data governance, including for cross border flows of all types of data.

ESCWA

The **ESCWA Cyber Legislation Directives** (see section 1.1 in this annex) includes chapters on:

- The Official Control Agency
- General Conditions for the Processing of Personal Data
- Judicial Recourses, Responsibilities and Sanctions
- The Transfer of Personal Data to Countries outside the Arab Region (Nations Economic and Commission for Western Asia, 2007[26])

information privacy protections and ensuring the free flow of information in the Asia Pacific region. The APEC Privacy Framework was first endorsed in 2005 and updated in 2015.

[138] Non-compliance may result in loss of CBPR certification, referral to the relevant government enforcement authority and penalties.

[139] The United States, Mexico, Japan, Canada, Singapore, Republic of Korea, Australia, Philippines and Chinese Taipei.

[140] https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf

ECOWAS

The Economic Community of West African States (ECOWAS), a grouping of fifteen states,[141] has developed the **Supplementary Act A/SA. 1/01/10 on Personal Data Protection within ECOWAS** in 2010, which is the only binding regional/international data protection agreement yet in force in Africa (Greenleaf and Cottier, 2020[27]). The Supplementary Act provides a legal and institutional framework for personal data protection, including personal data transfer to non-member ECOWAS countries. As of April 2020, eleven out of the fifteen ECOWAS countries[142] have enacted privacy protection laws that are consistent with the Supplementary Act (Greenleaf and Cottier, 2020[27]).

Ibero-American Data Protection Network

In 2017, Ibero-American Data Protection Network approved **Data Protection Standards of the Ibero-American States**, which constitute a set of legally non-binding guidelines that may contribute to the issuance of regulatory initiatives for the protection of personal data in the Ibero-American region. The Standards aim to "establish a set of common principles and rights for the protection of personal data which could be adopted by the Ibero-American States and develop their national legislation thereon, with the goal of having homogenous rules in the region."

International Conference of Data Protection and Privacy Commissioners

At the 31st *International Conference of Data Protection and Privacy Commissioners*, protection authorities of 50 countries adopted "**Madrid Resolution**", a non-binding resolution that includes a series of principles, rights and obligations that any privacy protection legal system must strive to achieve (International Conference of Data Protection and Privacy Commissioners, 2009[28]). It aims to define a set of principles and rights guaranteeing the effective and internationally uniform protection of privacy with regard to the processing of personal data; and to facilitate the international flows of personal data needed in a globalized world.

ISO

In 2019, *ISO* and the *IEC* published **ISO/IEC 27701**, which is a privacy extension to ISO/IEC 27001 and ISO/IEC 27002 (both of them are part of ISO 27000 family (see section 7 in this annex) for privacy management within the context of the organisation. It specifies requirements and provides guidance for Personally Identifiable Information (PII) Controllers and PII Processors to establish, implement, maintain and continually improve a Privacy Information Management System.[143]

Box 13. Example of RTA provisions on privacy

USMCA

Article 19.8: Personal Information Protection

1. The Parties recognize the economic and social benefits of protecting the personal information of users of digital trade and the contribution that this makes to enhancing consumer confidence in digital trade.

[141] Benin, Burkina Faso, Cape Verde, the Ivory Coast, Gambia, Ghana, Guinea, Guinea Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone and Togo

[142] Benin, Burkina Faso, Cape Verde, Senegal, Ghana, Guinea, Ivory Coast, Mali, Niger, Nigeria and Togo.,

[143] https://www.iso.org/standard/71670.html

https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-iso-27701?view=o365-worldwide

2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade. In the development of this legal framework, each Party should take into account principles and guidelines of relevant international bodies,[144] such as the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013).

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

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

5. Each Party shall publish information on the personal information protections it provides to users of digital trade, including how: (a) a natural person can pursue a remedy; and (b) an enterprise can comply with legal requirements.

6. Recognizing that the Parties may take different legal approaches to protecting personal information, each Party should encourage the development of mechanisms to promote compatibility between these different regimes. The Parties shall endeavor to exchange information on the mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them. The Parties recognize that the APEC CrossBorder Privacy Rules system is a valid mechanism to facilitate cross-border information transfers while protecting personal information.

SADEA

Article 17 Personal Information Protection

1. The Parties recognise the economic and social benefits of protecting the personal information of persons who conduct or engage in electronic transactions and the contribution that this makes to enhancing consumer confidence in electronic commerce.

2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of persons who conduct or engage in electronic transactions. In the development of its legal framework for the protection of personal information, each Party shall take into account the principles and guidelines of relevant international bodies, such as the APEC Cross-Border Privacy Rules ("CBPR") System and the OECD Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data.[145]

3. To this end, the key principles each Party shall take into account when developing its legal framework include limitation on collection, data quality, purpose specification, use limitation, security safeguards, transparency, individual participation and accountability.

4. Each Party shall adopt non-discriminatory practices in protecting persons who conduct or engage in electronic transactions from personal information protection violations occurring within its jurisdiction.

[144] Footnote 4: *For greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy.*

[145] Footnote 11: *For greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as comprehensive privacy, personal information or personal data protection laws, sector- specific laws covering data protection or privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to data protection or privacy.*

5. Each Party shall publish information on the personal information protections it provides to persons who conduct or engage in electronic transactions, including how: (a) a natural person can pursue remedies; and (b) business can comply with any legal requirements.

6. Each Party shall encourage enterprises in its territory to publish, including on the Internet, their policies and procedures related to protection of personal information.

7. Recognising that the Parties may take different legal approaches to protecting personal information, each Party shall encourage the development of mechanisms to promote compatibility between these different regimes. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks. To this end, the Parties shall endeavour to exchange information and share experiences on any such mechanisms applied in their jurisdictions and explore ways to promote compatibility between them.

8. The Parties recognise that the CBPR System is a valid mechanism to facilitate cross-border information transfers while protecting personal information.[146]

9. The Parties shall endeavour to jointly promote the CBPR System, with the aim to improving awareness of, and participation in, the CBPR System, including by industry.

EU-UK Trade and Cooperation Agreement

Article DIGIT.7 Protection of personal data and privacy

1. Each Party recognises that individuals have a right to the protection of personal data and privacy and that high standards in this regard contribute to trust in the digital economy and to the development of trade.

2. Nothing in this Agreement shall prevent a Party from adopting or maintaining measures on the protection of personal data and privacy, including with respect to cross-border data transfers, provided that the law of the Party provides for instruments enabling transfers under conditions of general application[147] *for the protection of the data transferred.*

3. Each Party shall inform the other Party about any measure referred to in paragraph 2 that it adopts or maintains.

6. Flow of Information

6.1. Cross-border transfer of information by electronic means

OECD

The OECD Privacy Guidelines (see section 5 in this annex) includes the following data flow governance provisions:

> *(16). A data controller remains accountable for personal data under its control without regard to the location of the data.*
>
> *(17). A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient*

[146] Footnote 12: *The Parties acknowledge that the CBPR System does not displace or change a Party's laws and regulations concerning the protection of personal information.*

[147] Footnote 34*: For greater certainty, "conditions of general application" refer to conditions formulated in objective terms that apply horizontally to an unidentified number of economic operators and thus cover a range of situations and cases.*

safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines.

(18). Any restrictions to trans-border flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.

APEC

APEC Privacy Framework (see section 5 in this annex) includes the following paragraphs, which is built on OECD Privacy Guidelines:

III. Cross-border privacy mechanisms

65. APEC recognized the importance of protecting privacy while maintaining the free flow of personal information across borders and has encouraged member economies to implement the Framework to provide conditions in which information can flow safely and accountably, for instance through the use of the CBPR system.

66. Member economies will endeavor to support the development and recognition or acceptance of cross-border privacy mechanisms for use by organizations to transfer personal information across the APEC region, recognizing that organizations would still be responsible for complying with the local privacy requirements, as well as with all applicable laws. Such mechanisms should apply the APEC Information Privacy Principles.

67. To give effect to paragraph 65, member economies have developed the CBPR system, which provides a practical mechanism for participating economies to implement the APEC Privacy Framework in an international, cross-border context, and to provide a means for organizations to transfer personal information across borders in a manner in which individuals may trust that the privacy of their personal information is protected.

68. Member economies worked with appropriate stakeholders to develop the PRP system to complement the CBPR system to help personal information processors demonstrate their ability to provide effective implementation of a personal information controller's obligations related to the processing of personal information.

IV. Cross-border transfers

69. A member economy should refrain from restricting cross border flows of personal information between itself and another member economy where (a) the other economy has in place legislative or regulatory instruments that give effect to the Framework or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures (such as the CBPR) put in place by the personal information controller to ensure a continuing level of protection consistent with the Framework and the laws or policies that implement it.

70. Any restrictions to cross border flows of personal information should be proportionate to the risks presented by the transfer, taking into account the sensitivity of the information, and the purpose and context of the cross border transfer.

As abovementioned, building on APEC Privacy Framework, APEC member economies have developed the **CBPR System**, which provides "a means for organizations to transfer personal information across borders in a manner in which individuals may trust that the privacy of their personal information is protected".

Council of Europe

The current **Convention 108** includes the following provisions on cross-border flow of personal data:[148]

> *Article 12 – Transborder flows of personal data and domestic law*
>
> *1 The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.*
>
> *2 A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.*
>
> *3 Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:*
>
> *a. insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;*
>
> *b. when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.*

Convention 108+ will replace the above with the following provisions (new Art. 14) when entering into force:[149]

> *1 A Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorisation the transfer of such data to a recipient who is subject to the jurisdiction of another Party to the Convention. Such a Party may, however, do so if there is a real and serious risk that the transfer to another Party, or from that other Party to a non-Party, would lead to circumventing the provisions of the Convention. A Party may also do so if bound by harmonised rules of protection shared by States belonging to a regional international organisation.*
>
> *2 When the recipient is subject to the jurisdiction of a State or international organisation which is not Party to this Convention, the transfer of personal data may only take place where an appropriate level of protection based on the provisions of this Convention is secured.*
>
> *3 An appropriate level of protection can be secured by:*
>
> *a. the law of that State or international organisation, including the applicable international treaties or agreements; or*
>
> *b ad hoc or approved standardised safeguards provided by legally-binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing.*
>
> […]

ASEAN

ASEAN PDP Framework includes the following provisions on flow of personal data (also see a data flow provision in ASEAN Agreement on Electronic Commerce in Box 14):

> *Transfers to Another Country or Territory*

[148] https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/108 (Accessed on 10 November 2020)

[149] https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/223 (Accessed on 11 November 2020)

6 (f) Before transferring personal data to another country or territory, the organisation should either obtain the consent of the individual for the overseas transfer or take reasonable steps to ensure that the receiving organisation will protect the personal data consistently with these Principles.

Box 14. Example of RTA provisions on cross-border transfer of information by electronic means

CPTPP

Article 14.11: Cross-Border Transfer of Information by Electronic Means

1. The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.

2. Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.

3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:

(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

(b) does not impose restrictions on transfers of information greater than are required to achieve the objective.

USMCA

Article 19.11: Cross-Border Transfer of Information by Electronic Means

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

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

(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

(b) does not impose restrictions on transfers of information greater than are necessary to achieve the objective.[150]

ASEAN Agreement on Electronic Commerce

Article 7.4. Cross-border Transfer of Information by Electronic Means

(a) Member States recognise the importance of allowing information to flow across borders through electronic means, provided that such information shall be used for businetss purposes, and subject to their respective laws and regulations.

(b) Member States agree to facilitate cross-border e-commerce by working towards eliminating or minimising barriers to the flow of information across borders, including personal information, subject to appropriate

[150] Footnote 5: *A measure does not meet the conditions of this paragraph if it accords different treatment to data transfers solely on the basis that they are cross-border in a manner that modifies the conditions of competition to the detriment of service suppliers of another Party.*

safeguards to ensure security and confidentiality of information, and when other legitimate public policy objectives so dictate.

(c) Subparagraphs (a) and (b) shall not apply to financial services and financial service suppliers as defined in the Annex on Financial Services of GATS.

EU-UK Trade and Cooperation Agreement

Article DIGIT.6 Cross-border data flows

1. The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted between the Parties by a Party:

(a) requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of a Party;

(b) requiring the localisation of data in the Party's territory for storage or processing;

(c) prohibiting the storage or processing in the territory of the other Party; or

(d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Parties' territory or upon localisation requirements in the Parties' territory.

2. The Parties shall keep the implementation of this provision under review and assess its functioning within three years of the date of entry into force of this Agreement. A Party may at any time propose to the other Party to review the list of restrictions listed in paragraph 1. Such a request shall be accorded sympathetic consideration.

6.2. Location of computing facilities

Rules on location of computing facilities have been developed through RTAs.

Box 15. Examples of RTA provisions on location of computing facilities

CPTPP

Article 14.13: Location of Computing Facilities

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

3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:

(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

(b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.

USMCA

Article 19.12: Location of Computing Facilities

No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.[151]

ASEAN Agreement on Electronic Commerce

Art. 7.6: Location of Computing Facilities

(a) Member States recognise that each Member State may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications

(b) Member States agree not to require, subject to their respective laws and regulations, a juridical person of another Member State and its affiliated companies to locate their computing facilities in their respective territories as a requirement for operating a business in their respective territories.

(c) Subparagraph (a) and (b) shall not apply to financial services and financial service suppliers as defined in the Annex on Financial Services of GATS.[152]

6.3. Location of financial computing facilities

Although no rules or principles related to the location of financial computing facilities have been as yet developed across international fora, a few RTAs include rules on location of financial computing facilities.

Box 16. Examples of RTA provisions on location of financial computing facilities

USMCA

Article 17.18: Location of Computing Facilities

1. The Parties recognize that immediate, direct, complete, and ongoing access by a Party's financial regulatory authorities to information of covered persons, including information underlying the transactions and operations of such persons, is critical to financial regulation and supervision, and recognize the need to eliminate any potential limitations on that access.

2. No Party shall require a covered person to use or locate computing facilities in the Party's territory as a condition for conducting business in that territory, so long as the Party's financial regulatory authorities, for regulatory and supervisory purposes, have immediate, direct, complete, and ongoing access to information processed or stored on computing facilities that the covered person uses or locates outside the Party's territory.[153]

[151] General exceptions apply to this provision (USMCA, Art. 32.1.2).

[152] General exceptions apply to this provision (ASEAN e-commerce agreement, Art.14).

[153] Footnote 9: *For greater certainty, access to information includes access to information of a covered person that is processed or stored on computing facilities of the covered person or on computing facilities of a third-party service supplier. For greater certainty, a Party may adopt or maintain a measure that is not inconsistent with this Agreement, including any measure consistent with Article 17.11.1 (Exceptions), such as a measure requiring a covered person to obtain prior authorization from a financial regulatory authority to designate a particular enterprise as a recipient of that information, or a measure adopted or maintained by a financial regulatory authority in the exercise of its authority over a covered person's business continuity planning practices with respect to maintenance of the operation of computing facilities.*

3. Each Party shall, to the extent practicable, provide a covered person with a reasonable opportunity to remediate a lack of access to information as described in paragraph 2 before the Party requires the covered person to use or locate computing facilities in the Party's territory or the territory of another jurisdiction.[154]

4. Nothing in this Article restricts the right of a Party to adopt or maintain measures to protect personal data, personal privacy and the confidentiality of individual records and accounts, provided that these measures are not used to circumvent the commitments or obligations of this Article.

SADEA

Article 25 Location of Computing Facilities for Financial Services

1. For the purposes of this Article, for a Party ("the relevant Party"), a "covered financial person" means:

(a) a "financial institution", as defined in Article 1(e) (Definitions) of Chapter Party (the relevant Party), a covered financial person means: (a) 9 (Financial Services), including a branch, located in the territory of the relevant Party that is controlled by persons of either Party; or

(b) a "cross-border financial service supplier of a Party" as defined in Article 1(b) (Definitions) of Chapter 9 (Financial Services), that is subject to regulation, supervision, licensing, authorisation, or registration by a financial regulatory authority of the relevant Party.

2. Neither Party shall require a covered financial person to use or locate computing facilities in the Party's territory as a condition for conducting business in that territory, provided that 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 the covered financial person uses or locates outside the Party's territory.

3. Each Party shall, to the extent practicable, provide a covered financial person with a reasonable opportunity to remediate any lack of access to information described in paragraph 2 before the Party requires the covered person to use or locate computing facilities in the Party's territory or the territory of a non-Party..

7. Cybersecurity

UN and international law

The UN Charter and existing international law could apply to State use of ICTs. The consensus report of the United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security,[155] which was adopted in 2015 (A/70/174), states: "*[i]n considering the application of international law to State use of ICTs, the Group Identified as of central importance the commitments of States to the following principles of the Charter and other international law: sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of*

[154] Footnote 10: *For greater certainty, so long as a Party's financial regulatory authorities do not have access to information as described in paragraph 2, the Party may, subject to paragraph 3, require a covered person to use or locate computing facilities either in the territory of the Party or the territory of another jurisdiction where the Party has that access.*

[155] https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/ (Accessed on 10 November 2020) This UN GGE was replaced with Group of Governmental Experts (GGE) on Advancing responsible State behaviour in cyberspace in the context of international security.

the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States."

It is also argued by international law experts that existing (pre-cyber era) international law, including general international law principles (e.g., the principle of sovereignty), human rights law and air and space law, also applies to cyberspace.[156]

OECD

Since the early 1990s, *the OECD* has been addressing the digital security issue based on the perspective that it is essential for the digital transformation to work for economic and social prosperity, and to ensure society's resilience. The OECD has developed non-binding Recommendations on this topic:

OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity

The OECD adopted **OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity** and its companion Document in 2015, which provides "*guidance for a new generation of national strategies on the management of digital security risk aimed to optimise the economic and social benefits expected from digital openness*" (OECD, 2015[29]). Members and non-Members adhering to this Recommendation are recommended to: implement the eight principles set out in Section 1 at all levels of government and in public organisations; and adopt a national strategy for the management of digital security risk as set out in Section 2 of the Recommendation (OECD, 2015[29]).

OECD Recommendation on Digital Security of Critical Activities

Against the background that greater occurrence and severity of digital security incidents affecting critical activities are anticipated, the OECD adopted the **OECD Recommendation on Digital Security of Critical Activities** in 2019, which replaced the 2008 OECD Recommendation on the Protection of Critical Information Infrastructure (OECD, 2020[30]). The Recommendation sets out a range of policy recommendations to ensure that policies targeting operators of critical activities focus on what is critical for the economy and society without imposing unnecessary burdens on the rest.

OECD Recommendation of the Council on Consumer Protection in E-commerce

The OECD Recommendation of the Council on Consumer Protection in E-commerce (see section 3.1 in this annex) also include the following recommendation on digital security for the purpose of consumer protection:

> *G. Privacy and Security*
>
> *49. Businesses should manage digital security risk and implement security measures for reducing or mitigating adverse effects relating to consumer participation in e-commerce.*

Council of Europe

The Convention on Cybercrime of the Council of Europe (the Budapest Convention), which entered into force in 2004, is the first international treaty on crimes committed via the Internet and other computer networks and the only binding international instrument on cybercrime. The convention aims to pursue "*a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation*" (Preamble). It requires parties to adopt legislative measures that establish as criminal offences illegal access, illegal interception, data interference, etc. The Convention also includes series of powers and procedures such as the search of computer networks and interception. As of September 2020, it has been ratified by

[156] https://ccdcoe.org/research/tallinn-manual/

65 countries, including Members and Non-Members of Council of Europe. More information is available the Council of Europe website on the Convention.

AU

AU's Malabo Convention (see section 5 in this annex) includes rules to promote cyber security and combat cybercrime, such as rules on cyber security measures to be taken at national level.

ESCWA Cyber Legislation Directives

The ESCWA Cyber Legislation Directives (see section 1.1 in this annex) includes chapters on cybercrime, such as crimes whose target is data and crimes whose target is information systems (Nations Economic and Commission for Western Asia, 2007[26]).

ECOWAS

In 2011, the *ECOWAS* developed the **Directive C/DIR/1/08/11 on Fighting Cyber Crime within ECOWAS** to adapt the substantive criminal law and procedures of the Member States to address cybercrime (Art.2). The Directive includes provisions on offences specifically related to ICT, incorporation of traditional offences into ICT offences, and sanctions. The Directive is in compliance with the Budapest Convention and AU's Malabo Convention (ECOWAS Commission, 2017[25]).

The Wassenaar Arrangement

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is a multilateral export control regime, which has been established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies. Under this arrangement, participating States are required to apply export controls to all items set forth in the List of Dual-Use Goods and Technologies and the Munitions List so as to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities that undermine the above goals. As of September 2020, 42 States participate in the Arrangement. More information is available at the website of the Arrangement.

Its List of Dual-Use Goods and Technologies and the Munitions List[157] includes, for instance, "software" specially designed or modified for the conduct of military offensive cyber operations or IP network communications surveillance systems or equipment.[158]

ISO/IEC

ISO and *IEC* established the **ISO/IEC 27000 family**, which provide information security standards, helping to protect IT systems and ensures the free flow of data in the virtual world. It lays out best practice recommendations in the implementation, maintenance and continual improvement of controls of information security management with in the

[157] https://www.wassenaar.org/app/uploads/2019/12/WA-DOC-19-PUB-002-Public-Docs-Vol-II-2019-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-19.pdf

[158] 39The Wassenaar Arrangement, List of Dual-Use Goods and Technologies and Munitions List, WA-LIST (19) 1 ML21.b.5 ("Software" specially designed or modified for the conduct of military offensive cyber operations) and Categories 5.A.1.j (IP network communications surveillance systems)

context of an overall information security management system (ISMS).[159] The ISO/IEC 27000 family includes standards related to "information technology - security techniques," such as:

- ISO/IEC 27000:2018 provides the overview of ISMS. It also provides terms and definitions commonly used in the ISMS family of standards.[160]
- ISO/IEC 27001:2013 is widely known, providing requirements for an ISMS. Using them enables organizations of any kind to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties.[161]
- ISO/IEC 27002:2013 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environments.[162]

In contrast to ISO/IEC 27000, **IEC 62443** – an indispensable series of standards that establishes precise cyber security guidelines and specifications applicable to a wide range of industries and critical infrastructure environments – is designed to keep operational technology systems running in the physical world. The IECEE (IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components) includes a programme that provides certification to Standards within the IEC 62443 series. IEC 62443 is well known to cyber security experts for adopting a layered, defence-indepth approach. The series is also used in the transport sector while the International Maritime Organization (IMO) refers to IEC 62443 in a set of cyber security guidelines for ships. Shift2Rail, an initiative that brings together key European railway stakeholders, has selected IEC 62443 for the railway sector. This series is also compatible with the US National Institute of Standards and Technology (NIST) cyber security framework.[163]

In addition to generic and flexible horizontal standards, ISC has developed vertical standards that cater to very specific needs of specific sectors. For instance, IEC TC 57 develops, among many others, the **IEC 61850** series of publications for communication networks and systems for power utility automation, and the **IEC 60870** series for telecontrol equipment and systems.[164]

IETF

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.[165] It has developed many standards and protocols for internet security, such as protocols on IP Security (RFC2411), Transport Layer Security (RFC2246).[166]

IEEE

The Institute of Electrical and Electronics Engineers (IEEE) is the world's largest technical professional society, designed to serve professionals involved in all aspects of the electrical, electronic, and computing fields and related

[159] https://basecamp.iec.ch/download/brochure-cyber-security-en/

[160] https://www.iso.org/standard/73906.html

[161] https://www.iso.org/isoiec-27001-information-security.html

[162] https://www.iso.org/standard/54533.html

[163] https://basecamp.iec.ch/download/brochure-cyber-security-en/

[164] https://basecamp.iec.ch/download/brochure-cyber-security-en/

[165] https://www.ietf.org/about/who/

[166] https://www.rfc-editor.org/bcp/bcp61.txt

areas of science and technology that underlie modern civilization.[167] The IEEE has also established standards on the above fields and areas. With regards to cybersecurity, it has developed, for instance, 1686-2013 - IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities[168] and 1686-2007 - IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities.[169]

Box 17. Examples of RTA provisions on cybersecurity

CPTPP

Article 14.16: Cooperation on Cybersecurity Matters

The Parties recognise the importance of:

(a) building the capabilities of their national entities responsible for computer security incident response; and

(b) using existing collaboration mechanisms to cooperate to identify and mitigate malicious intrusions or dissemination of malicious code that affect the electronic networks of the Parties.

USMCA

Article 19.15: Cybersecurity

1. The Parties recognize that threats to cybersecurity undermine confidence in digital trade. Accordingly, the Parties shall endeavor to:

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

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

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

ASEAN Agreement on Electronic Commerce

Art. 8. CYBERSECURITY:

Member States recognise the importance of:

(a) building the capabilities of their national entities responsible for cybersecurity including through the exchange of best practices; and

(b) using existing collaboration mechanisms to cooperate on matters related to cybersecurity

[167] https://www.ieee.org/about/ieee-history.html

[168] https://standards.ieee.org/standard/1686-2013.html

[169] https://standards.ieee.org/standard/1686-2007.html

8. Telecoms: Updating the telecommunications reference paper

WTO

GATS principles apply to telecommunication services. Additionally, principles that are established in the **Annex on telecommunications** of GATS, which provides guarantees for reasonable access to and use of public telecommunications, also apply.

Key principles are also provided in the **Telecommunications Reference Paper**, which sets out regulatory principles on basic telecommunications. These include competitive safeguards, interconnection, universal service, public availability of licensing criteria, interdependent regulators and allocation and use of scarce resources. The principles are designed to ensure that dominant market positions of monopoly suppliers are not used to the detriment of new entrants on the telecommunications markets (Bronckers and Larouche, 2012[21]). 103 WTO Member governments have undertaken these additional commitments. More information is available at the WTO website on telecommunication services.

ITU

While the WTO mainly focuses on regulatory aspects of telecommunication services, *the International Telecommunication Union (ITU)* mainly takes care of more technical issues, including frequency allocation and standardization. The ITU has developed international standards known as **ITU-T Recommendations,** which act as defining elements in the global infrastructure of ICTs.[170] Those standards secure interoperability of ICTs and enable global communications by ensuring that countries' ICT networks and devices are speaking the same language.[171] More information is available at the ITU website.

ISO/IEC

ISO and *IEC* also takes care of technical issues. For instance, ISO/IEC JTC 1/SC 6 Telecommunications and information exchange between systems (SC6) is a subcommittee of the Joint Technical Committee ISO/IEC JTC 1 of the ISO. IEC.SC6 "*has worked on standardization in the field of telecommunications dealing with the exchange of information between open systems, including system functions, procedures, parameters as well as the conditions for their use. This standardization encompasses protocols and services of lower layers including physical, data link, network, and transport as well as those of upper layers including but not limited to Directory and ASN.1: MFAN, NFC, PLC, Future Networks and OID*".[172] So far, it has published 289 ISO standards.[173]

Other standard setting organizations

Industry associations and other standard setting organisations have also played active roles in developing standards for telecommunication. The following are the examples of those associations:

Telecommunication Industry Association (TIA)

Telecommunication Industry Association (TIA) is an industry association with a global membership of more than 400-member companies including ICT manufacturers and suppliers, network operators and service enablers,

[170] https://www.itu.int/en/ITU-T/about/Pages/default.aspx

[171] https://www.itu.int/en/ITU-T/about/Pages/default.aspx

[172] https://www.iso.org/committee/45072.html

[173] As of 1 September, 2020.

distributors and system integrators.[174] Accredited by the American National Standards Institute (ANSI) as a standards developing organization (SDO), TIA operates nine engineering committees that develop guidelines for private radio equipment, cellular towers, VOIP equipment, structured cabling, satellites, telephone terminal equipment, accessibility, data centers, mobile device communications, vehicular telematics, smart device communications, and smart utility mesh networks.[175]

The European Telecommunications Standards Institute (ETSI)

The European Telecommunications Standards Institute (ETSI) is a European Standards Organization (ESO), the recognized regional standards body dealing with telecommunications, broadcasting and other electronic communications networks and services. It produces standards for ICT-enabled systems, applications and services deployed across all sectors of industry and society.[176]

The Internet Engineering Task Force (*IETF)*

The *IETF* develops Internet standards based on open and well-documented processes.[177]

9. Customs duties; Customs duties on electronic transmissions

WTO

Since 1998, WTO Members have regularly extended a Moratorium on imposing customs duties on electronic transmissions. Most recently, at the General Council meeting in December 2019, Members agreed to maintain that practice until the 12th Ministerial Conference (MC12).[178]

[174] https://tiaonline.org/about/

[175] https://tiaonline.org/what-we-do/standards/

[176] https://www.etsi.org/

[177] https://www.ietf.org/standards/

[178] https://www.wto.org/english/news_e/news19_e/gc_10dec19_e.htm

Box 18. Examples of RTA provisions on customs duties on electronic transactions

CPTPP

Article 14.3: Customs Duties

1. No Party shall impose customs duties on electronic transmissions, including content transmitted electronically, between a person of one Party and a person of another Party.

2. For greater certainty, paragraph 1 shall not preclude a Party from imposing internal taxes, fees or other charges on content transmitted electronically, provided that such taxes, fees or charges are imposed in a manner consistent with this Agreement.

USMCA

Article 19.3: Customs Duties

1. No Party shall impose customs duties, fees, or other charges on or in connection with the importation or exportation of digital products transmitted electronically, between a person of one Party and a person of another Party.

2. For greater certainty, paragraph 1 does not preclude a Party from imposing internal taxes, fees, or other charges on a digital product transmitted electronically, provided that those taxes, fees, or charges are imposed in a manner consistent with this Agreement.

10. Access to internet and data

10.1. Open government data

G8

In June 2013, G8 leaders signed the **Open Data Charter**, which sets out five strategic principles that all G8 members will act on.[179] These principles include Open Data by Default, Quality and Quantity, Usable by All, Releasing Data for Improved Governance, Releasing Data for Innovation. It also contains a Technical annex, which identifies best practices and collective actions that G8 members will use to meet the above principles. The charter also specifies 14 high-value areas, from education to transport and from health to crime and justice, from which G8 members will release data.

OECD

In 2008, the OECD Council adopted the **Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information**. The Recommendation provides policy guidelines that are designed to improve access and increase use of public sector information through greater transparency, enhanced competition and more competitive pricing.[180] It recommends that governments, in establishing or reviewing their policies regarding access and use of public sector information, take due account of and implement principles such as openness, access and transparent conditions for re-use, quality, pricing, competition and international access and use.

[179] https://www.gov.uk/government/publications/open-data-charter/g8-open-data-charter-and-technical-annex

[180] http://www.oecd.org/sti/ieconomy/oecdrecommendationonpublicsectorinformationpsi.htm#:~:text=The%20OECD%20Recommendation%20on%20public,Council%20on%2030%20April%202008

Box 19. Examples of RTA provisions on open government data

USMCA

Article 19.18: Open Government Data

1. The Parties recognize that facilitating public access to and use of government information fosters economic and social development, competitiveness, and innovation.

2. To the extent that a Party chooses to make government information, including data, available to the public, it shall endeavor to ensure that the information is in a machine-readable and open format and can be searched, retrieved, used, reused, and redistributed.

3. The Parties shall endeavor to cooperate to identify ways in which each Party can expand access to and use of government information, including data, that the Party has made public, with a view to enhancing and generating business opportunities, especially for SMEs.

DEPA

Article 9.5: Open Government Data

1. The Parties recognise that facilitating public access to and use of government information may foster economic and social development, competitiveness, and innovation.

2. To the extent that a Party chooses to make government information, including data, available to the public, it shall endeavor to ensure that the information is made available as open data.

3. The Parties shall endeavor to cooperate to identify ways in which Parties can expand access to and use of open data, with a view to enhancing and generating business opportunities.

4. Cooperation under this Article may include activities such as:

(a) Jointly identifying sectors where open data sets, particularly those with global value, can be used to, among other things, facilitate technology transfer, talent formation and innovation.

(b) Encouraging the development of new products and services based on open data sets; and

(c) Fostering the use and develop open data licensing models in the form of standardized public licenses available online, which will allow open data to be freely accessed, used, modified and shared by anyone for any purpose permitted by local law, and which rely on open data formats.

10.2. Access to the Internet

Internet standards - agreed-upon technical specifications that underpin the infrastructure of the Internet - have been developed by Internet-related standard setting bodies, including the *Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA), IETF, the Internet Architecture Board (IAB), the World Wide Web Consortium (W3C),* and *the Internet Society*. These bodies are taking an open-Internet standards approach, which allows anyone to participate in the process of developing Internet standards. One of the challenges that these bodies face is lack of government recognition, where open standards are not referenced by domestic laws and regulations.[181]

[181] https://www.internetsociety.org/policybriefs/openstandards/

Box 20. Example of RTA provisions on Access to the Internet

CPTPP

Article 14.10: Principles on Access to and Use of the Internet for Electronic Commerce

Subject to applicable policies, laws and regulations, the Parties recognise the benefits of consumers in their territories having the ability to:

(a) access and use services and applications of a consumer's choice available on the Internet, subject to reasonable network management;[182]

(b) connect the end-user devices of a consumer's choice to the Internet, provided that such devices do not harm the network; and

(c) access information on the network management practices of a consumer's Internet access service supplier.

10.3. Access to online platforms/competition

ICN

The *International Competition Network (ICN)*, which was launched in 2001 by antitrust authorities from 14 jurisdictions, is an informal, project-oriented network of antitrust agencies from developed and developing countries. The ICN's membership currently has 140 member authorities from 129 jurisdictions.

As a global body devoted exclusively to competition law enforcement, the ICN provides competition authorities with "a specialized yet informal venue for maintaining regular contacts and addressing practical competition concerns", which allows for "a dynamic dialogue that serves to build consensus and convergence towards sound competition policy principles across the global antitrust community".[183] While the ICN does have a mandate to establish binding rules, the ICN has developed recommendations, or "best practices" on competition policies based on consensus of its members. Individual competition authorities then decide whether and how to implement these recommendations, through unilateral, bilateral or multilateral arrangements, as appropriate. To date, ICN has developed 7 Recommended Practices and 8 Recommendations on competition policies and competition law enforcement – although none are focused specifically on digital markets.

More information is available at the ICN website.

OECD

After a first recommendation in 1967, followed by a series of revisions, the *OECD Council* adopted in September 2014 **Recommendation concerning International Co-operation on Competition Investigations and Proceedings**, which calls for governments to foster their competition laws and practices so as to promote further international co-operation among competition authorities and to reduce the harm arising from anticompetitive practices and from mergers with anticompetitive effects.[184] It recommend, among others, co-ordination of competition investigations or proceedings, exchange of information in competition investigations or proceedings and investigative assistance, which could be useful in the context of dealing with market distortions caused by digital business.

[182] Footnote 7: *The Parties recognise that an Internet access service supplier that offers its subscribers certain content on an exclusive basis would not be acting contrary to this principle.*

[183] https://www.internationalcompetitionnetwork.org/about/

[184] https://www.oecd.org/daf/competition/2014-rec-internat-coop-competition.pdf

Co-ordination of Competition Investigations or Proceedings

VI. RECOMMENDS that where two or more Adherents investigate or proceed against the same or related anticompetitive practice or merger with anticompetitive effects, they should endeavour to co-ordinate their investigations or proceedings where their competition authorities agree that it would be in their interest to do so.

Exchange of Information in Competition Investigations or Proceedings

VII. RECOMMENDS that in co-operating with other Adherents, where appropriate and practicable, Adherents should provide each other with relevant information that enables their competition authorities to investigate and take appropriate and effective actions with respect to anticompetitive practices and mergers with anticompetitive effects.

Investigative Assistance to Another Competition Authority

VIII. RECOMMENDS that regardless of whether two or more Adherents proceed against the same or related anticompetitive practice or merger with anticompetitive effects, competition authorities of the Adherents should support each other on a voluntary basis in their enforcement activity by providing each other with investigative assistance as appropriate and practicable, taking into account available resources and priorities.

International co-operation agreements on competition law enforcement

As business activities have been globalised, effective co-operation and co-ordination in competition law enforcement is needed for effective action against anti-competitive practices with a cross-border connotation. Although authorities can work together informally, many of them have developed formal cooperation instruments in order to strengthen the scope and degree of cooperation. Among the various formal co-operation instruments, **co-operation agreements**, which are concluded between two or more jurisdictions or competition authorities, are the tools more commonly used and relied upon by competition authorities.[185] These agreements often include provisions on enforcement co-operation and investigative assistance, the exchange of information and the co-ordination of investigations and proceedings. More information is available at OECD inventory of international co-operation agreements on competition.

Box 21. Example of RTA provisions on Competition

DEPA

Article 8.4: Cooperation on Competition Policy

1. Recognizing that the Parties can benefit by sharing their experience in enforcing competition law and in developing and implementing competition policies to address the challenges that arise from the digital economy, the Parties shall consider undertaking mutually agreed technical cooperation activities, subject to available resources, including:

(a) exchanging information and experiences on development of competition policies in the digital markets;

(b) sharing best practices on promotion of competition in digital markets;

(c) providing advice or training, including through the exchange of officials, to assist a Party build necessary capacities to strengthen competition policy development and competition law enforcement in the digital markets.

2. Each Party shall cooperate, as appropriate, on issues of competition law enforcement in digital markets, including through notification, consultation and the exchange of information.

[185] http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=daf/comp/wp3(2015)12/rev1&docLanguage=En

3. The Parties agree to cooperate in a manner compatible with their respective laws, regulations and important interests, and within their reasonably available resources.

11. Business trust

11.1. Source code

WTO

TRIPS Agreement

Source code enjoys protection provided by the **WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement)** where it falls under patent, copy right or trade secrets protection. For instance, the TRIPS Agreement stipulates that "[c]omputer programs, whether in source or object code, shall be protected as literary works under the Berne Convention (1971)" (Article 10(1)).

TBT Agreement

WTO agreement of technical barriers to trade (TBT Agreement) aims to ensure that technical regulations and standards and procedures for assessment of conformity with technical regulations and standards do not create unnecessary obstacles to international trade. These rules would also apply to regulations, standards and conformity assessment procedures on ICT products including software. Under the TBT Agreement, WTO Members are allowed to set technical specifications for products embedded with software provided such specifications are not "more trade-restrictive than necessary to fulfil a legitimate objective" (Art. 2.2). WTO Members also have the right to assure that imported products embedded with software conform to such technical specifications based on the rules in the Agreement (Art.5).

Box 22. Examples of RTA provisions on Source code

EU-Japan EPA

8.73 Source code

1. A Party may not require the transfer of, or access to, source code of software owned by a person of the other Party.[186] *Nothing in this paragraph shall prevent the inclusion or implementation of terms and conditions related to the transfer of or granting of access to source code in commercially negotiated contracts, or the voluntary transfer of or granting of access to source code for instance in the context of government procurement.*

2. Nothing in this Article shall affect:

(a) requirements by a court, administrative tribunal or competition authority to remedy a violation of competition law;

(b) requirements by a court, administrative tribunal or administrative authority with respect to the protection and enforcement of intellectual property rights to the extent that source codes are protected by those rights; and

(c) the right of a Party to take measures in accordance with Article III of the GPA.

[…]

[186] Footnote 1: *For greater certainty, "source code of software owned by a person of the other Party" includes source code of software contained in a product.*

Japan-UK EPA

ARTICLE 8.73 Source code

1. A Party shall not require the transfer of, or access to, source code of software owned by a person of the other Party, or the transfer of, or access to, an algorithm expressed in that source code, as a condition for the import, distribution, sale or use of that software, or of products containing that software, in its territory.

[…]

11.2. ICT products that use cryptography

WTO

The abovementioned **TRIPS Agreement** and **TBT Agreement** could also apply to ICT products using cryptography.

OECD

Recognising that cryptography can be effective to secure information and communication networks and systems while its misuse can adversely affect the operation of e-commerce, protection of privacy, etc., the OECD established the **Guidelines for Cryptography Policy** in 1997.[187] They include the following principle on lawful access:

> *6. Lawful Access*
>
> ***National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible.***
>
> *If considering policies on cryptographic methods that provide for lawful access, governments should carefully weigh the benefits, including the benefits for public safety, law enforcement and national security, as well as the risks of misuse, the additional expense of any supporting infrastructure, the prospects of technical failure, and other costs. This principle should not be interpreted as implying that governments should, or should not, initiate legislation that would allow lawful access.*
>
> *Where access to the plaintext, or cryptographic keys, of encrypted data is requested under lawful process, the individual or entity requesting access must have a legal right to possession of the plaintext, and once obtained the data must only be used for lawful purposes. The process through which lawful access is obtained should be recorded, so that the disclosure of the cryptographic keys or the data can be audited or reviewed in accordance with national law. Where lawful access is requested and obtained, such access should be granted within designated time limits appropriate to the circumstances. The conditions of lawful access should be stated clearly and published in a way that they are easily available to users, keyholders and providers of cryptographic methods.*
>
> *Key management systems could provide a basis for a possible solution which could balance the interest of users and law enforcement authorities; these techniques could also be used to recover data, when keys are lost. Processes for lawful access to cryptographic keys must recognise the distinction between keys which are used to protect confidentiality and keys which are used for other purposes only. A cryptographic key that provides for identity or integrity only (as distinct from a cryptographic key that verifies identity or*

187 https://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm#:~:text=The%20OECD%20Recommendation%20Concerning%20Guidelines,for%20which%20they%20were%20developed. (Accessed on 10 November 2020)

integrity only) should not be made available without the consent of the individual or entity in lawful possession of that key.

ISO

ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques* developed **ISO/IEC 18033**, which specifies encryption systems (ciphers) for the purpose of data confidentiality.[188]

Box 23. Example of RTA provisions on *ICT Products that Use Cryptography*

USMCA

Article 12.C.2: ICT Goods that Use Cryptography

1. This Article applies to ICT goods that use cryptography[189] This Article does not apply to:

(a) a Party's law enforcement authorities requiring service suppliers using encryption they control to provide unencrypted communications pursuant to that Party's legal procedures;

(b) the regulation of financial instruments;

(c) a requirement that a Party adopts or maintains relating to access to networks, including user devices, that are owned or controlled by the government of that Party, including those of central banks;

(d) a measure taken by a Party pursuant to supervisory, investigatory, or examination authority relating to financial institutions or financial markets; or

(e) the manufacture, sale, distribution, import, or use of the good by or for the government of the Party.

2. With respect to an ICT good that uses cryptography and is designed for commercial applications, no Party shall require a manufacturer or supplier of the good, as a condition of the manufacture, sale, distribution, import, or use of the good, to:

(a) transfer or provide access to any proprietary information relating to cryptography, including by disclosing a particular technology or production process or other information, for example, a private key or other secret parameter, algorithm specification, or other design detail, to the Party or a person in the Party's territory;

(b) partner or otherwise cooperate with a person in its territory in the development, manufacture, sale, distribution, import, or use of the product; or

(c) use or integrate a particular cryptographic algorithm or cipher.

Japan-UK EPA

Article 8.86 Commercial information and communication technology products[190] that use cryptography[191]

188 https://www.iso.org/standard/37972.html#:~:text=An%20encryption%20algorithm%20is%20applied,except%2C%20perhaps%2C%20its%20length; https://www.iso.org/obp/ui/#iso:std:iso-iec:18033:-1:ed-2:v1:en

189 Footnote 6: *[f]or greater certainty, for the purposes of this Annex, an ICT good does not include a financial instrument*.

190 *"[C]ommercial information and communication technology product" (commercial ICT product) means a product, including software, that is designed for commercial applications and whose intended function is information processing and communication by electronic means, including transmission and display, or electronic processing applied to determine or record physical phenomena, or to control physical processes (Art. 8.71)*

191 Footnote 1: *[f]or greater certainty, this Article does not affect the rights and obligations of a Party under Article 8.73.*

1. A Party shall not require a manufacturer or supplier of a commercial ICT product that uses cryptography, as a condition of the manufacture, sale, distribution, import or use of the commercial ICT product, to:

(a) transfer or provide access to any proprietary information relating to cryptography, including by disclosing a particular technology or production process or other information, for example, a private key or other secret parameter, algorithm specification or other design detail, to that Party or a person in the territory of that Party;

(b) partner or otherwise cooperate with a person in the territory of that Party in the development, manufacture, sale, distribution, import or use of the commercial ICT product; or

(c) use or integrate a particular cryptographic algorithm or cipher.

2. This Article shall not preclude a regulatory body or judicial authority of a Party from requiring a manufacturer or supplier of a commercial ICT product that uses cryptography:

(a) to preserve and make available[192] any information to which subparagraph 1(a) applies for an investigation, inspection, examination, enforcement action or judicial proceeding, subject to safeguards against unauthorised disclosure; or

(b) to transfer or provide access to any information to which subparagraph 1(a) applies for the purpose of imposing or enforcing a remedy granted in accordance with that Party's competition law following an investigation, inspection, examination, enforcement action or judicial proceeding.

3. Notwithstanding paragraph 4 of Article 8.70, this Article applies to commercial ICT products that use cryptography.[193] This Article does not apply to:

(a) a Party's law enforcement authorities requiring service suppliers using encryption to provide access to encrypted and unencrypted communications pursuant to that Party's legal procedures;

(b) the regulation of financial instruments;

(c) a requirement that a Party adopts or maintains relating to access to networks, including user devices, that are owned or controlled by that Party, including those of central banks;

(d) measures by a Party adopted or maintained pursuant to supervisory, investigatory or examination authority relating to financial service suppliers or financial markets; or

(e) the manufacture, sale, distribution, import or use of a commercial ICT product that uses cryptography by or for a Party.

12. Market Access

12.1. Services market access

WTO

Services market access is based on **specific commitments for service sectors and modes of supply that countries schedule under the GATS**. Service sectors under the GATS Schedules of Specific Commitments [194] that are relevant

[192] Footnote 1: *[t]he Parties understand that this making available shall not be construed to negatively affect the status of any proprietary information relating to cryptography as a trade secret.*

[193] Footnote 2: *[f]or greater certainty, for the purposes of this Article, a commercial ICT product does not include a financial instrument.*

[194] WTO, MTN. GNS/W/120

to digital trade might include computer services, telecommunication distribution services and other services that could be digitally provided (e.g., financial services, professional services, tourism and travel related services, or audio-visual services). With regards to mode of supply, for instance, commitments made for cross-border supply (Mode 1) are relevant where services are supplied digitally from abroad.

12.2. Goods market access

WTO

GATT and TBT Agreement

Agreed tariffs and other rules under the **GATT** apply to all trade in goods including those that are digitally ordered. Other WTO agreements, such as **TBT Agreement**, also deal with non-tariff measures on these goods.

ITA

The Information Technology Agreement (ITA), concluded by 29 participants at the Singapore Ministerial Conference in December 1996, requires each participant to completely eliminate tariffs on IT products covered by the Agreement. A large number of high technology products are covered by the ITA, including computers, telecommunication equipment, semiconductors, semiconductor manufacturing and testing equipment, software, scientific instruments, as well as most of the parts and accessories for these products. Since 1996, the number of participants has grown to 82, representing about 97 per cent of world trade in IT products and accounting for an estimated US$ 1.6 trillion in 2013. The tariff elimination under the Agreement is implemented on a Most-Favoured Nation (MFN) basis.

At the Nairobi Ministerial Conference in December 2015, over 50 WTO Members concluded the expansion of the Agreement, covering an additional 201 products valued at over $1.3 trillion per year, and accounting for approximately 7% of total global trade. The new Agreement covers new generation semiconductors, semiconductor manufacturing equipment, optical lenses, GPS navigation equipment, and medical equipment such as magnetic resonance imaging products and ultra-sonic scanning apparatus.[195] Participating WTO Members agreed to remove tariffs on those products by 2024.[196]

[195] https://www.wto.org/english/tratop_e/inftec_e/itaintro_e.htm; https://www.wto.org/english/tratop_e/inftec_e/inftec_e.htm

[196] https://www.piie.com/blogs/trade-investment-policy-watch/ita-2-success-nairobi

Annex B: Country breakdown

Annex B is a spreadsheet that has been uploaded on the Trade Portal. It comprises a sheet on "international instruments" and another on "RTAs". These cover all WTO Members as well as a number of observers and non-Members (particularly those that have signed at least one international instruments or RTA.

The "international instruments" datasheet maps jurisdictions that have ratified, signed, adhered to or are influenced by specific international instruments across the different issues covered by the Inventory.[197] Jurisdictions are coded as "1" if they have ratified or adhered to a particular instrument, and "2" if they have signed but not yet ratified a particular instrument. Jurisdictions are also coded 1 where one or more of their states or territories are influenced by specific instruments. Coding is based on the information collected from public source including the websites of the different instruments (these links are included in the datasheet).

The "RTAs" datasheet maps jurisdictions that have signed RTAs that include provisions related to the different issues covered by the Inventory. Coding in the RTAs datasheet is based on the TAPED dataset (and Codebook) which was last updated on the 8th of June 2020.[198] This implies that it does not include some of the most-recent RTAs such as the Regional Comprehensive Economic Partnership (RCEP) or the Japan-UK Comprehensive Economic Partnership Agreement (Japan-UK EPA). The TAPED dataset provides three levels of coding: "1" refers to "yes (soft)", "2" to "yes (mixed)" and "3" to "yes (hard)".[199] If a jurisdiction has signed RTAs with different codes for a certain provision, the highest degree is coded in the datasheet (e.g., if a jurisdiction X has signed both RTAs with "soft" and "hard" consumer protection provisions, the jurisdiction will be coded as "3" under consumer protection provision). The RTA datasheet also includes the "TAPED dataset index", which refers to indices for each provision that are provided in the TAPED dataset and Codebook.

[197] The international instrument datasheet is up to date as of the 1st of October 2020 (unless otherwise specified).

[198] Codes for the UK were therefore given based on the fact the EU's RTAs still applied to the UK as of the 8th of June 2020 (during the transition period) (WT/GC/206).

[199] Although the TAPED dataset does not provide definitions of "soft", "mixed" and "hard", "hard" appears to refer to a provision that includes denser rules or binding-elements while "soft" refers to a provision that include less dense rules or non-binding elements.

Annex C: Supporting Tables

Annex Table C1. Adherence to different international instruments varies

Specific areas	Rules	jurisdictions	JSI participants
Paperless trading	Trade Facilitation Agreement	153	86
Goods market access	Information Technology Agreement	81	68
Updating the telecommunications reference paper	WTO Telecommunications Reference Paper	103	66
Cybersecurity	The Council of Europe Budapest Convention	68	52
Goods market access	Expanded Information Technology Agreement	53	52
Protection of personal information/Cross-border information transfer	Council of Europe Convention 108	55	43
Electronic transaction frameworks	ratified or influenced by either of the UN Electronic Communication Convention or the UNCITRAL Model law on Electronic Commerce (including through RTA referencing them)	91	41
Access to online platforms/competition	OECD Recommendation concerning International Co-operation on Competition Investigations and Proceedings	40	40
Online consumer protection	OECD Recommendation on Consumer Protection in E-commerce	39	39
Cybersecurity	OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity	39	39
Cybersecurity	OECD Recommendation on Digital Security of Critical Activities	38	38
Open government data	OECD Recommendation on Public Sector Information	38	38
Protection of personal information/Cross-border information transfer	OECD Privacy Guidelines	37	37
ICT products that use cryptography	OECD Guidelines for Cryptography Policy	37	37
Electronic transaction frameworks	UNCITRAL Model Law on Electronic Commerce	74	31
Protection of personal information/Cross-border information transfer	APEC Privacy Framework	21	19
Electronic transaction frameworks	UN Electronic Communications Convention	26	14
E-authentication and e-signatures	UNCITRAL Model Law on Electronic Signatures	33	13
Protection of personal information/Cross-border information transfer	Data Protection Standards of the Ibero-American States	10	9

Protection of personal information/Cross-border information transfer	APEC CBPR systems	9	9
Protection of personal information/Cross-border information transfer	ASEAN PDP Framework	10	8
Open government data	G8 Open Data Charter	8	8
Customs procedures	ASEAN Agreement on Customs	7	6
Electronic transaction frameworks	ESCWA Cyber Legislation Directives	20	5
E-authentication and e-signatures /. Electronic contracts/ Electronic invoicing	ECOWAS Supplementary Act A/SA.2/01/10 on electronic transactions	15	4
Protection of personal information/Cross-border information transfer	ECOWAS Supplementary Act A/SA. 1/01/10 on Personal Data Protection	15	4
Cybersecurity	ECOWAS Directive C/DIR/1/08/11 on Fighting Cyber Crime	15	4
Paperless trading	UN ESCAP Framework Agreement	7	2
Protection of personal information/Cross-border information transfer	AU Malabo Convention	19	1
Electronic transferrable records	UNCITRAL Model Law on Electronic Transferable Records	1	1
Electronic transaction frameworks/consumer protection	SADC Model Law	16	0

Note: Descending order of JSI participants. WTO rules applying to all WTO members, such as GATT, GATS and the TBT agreement, are excluded from the table.
Source: based on author's analysis based on information in Annex C.

Annex Table C2. A wide variety of fora have established relevant rules

forum	Specific area	Rules	jurisdictions	JSI participants
APEC	Protection of personal information/Cross-border information transfer	APEC Privacy Framework	21	19
	Protection of personal information/Cross-border information transfer	APEC CBPR systems	9	9
ASEAN	Customs procedures	ASEAN Agreement on Customs	7	6
	Protection of personal information/Cross-border information transfer	ASEAN PDP Framework	10	8
AU	Protection of personal information/Cross-border information transfer	AU Malabo Convention	19	1
Bilateral/plurilateral governmental agreement	Access to online platforms/competition	Bilateral or Plurilateral Co-operation agreements on competition		
Council of Europe	Protection of personal information/Cross-border information transfer	Council of Europe Convention 108	55	43
	Cybersecurity	Council of Europe Budapest Convention	68	52
ECOWAS	E-authentication and e-signatures /. Electronic contracts/ Electronic invoicing	ECOWAS Supplementary Act A/SA.2/01/10 on electronic transactions	15	4
	Protection of personal information/Cross-border information transfer	ECOWAS Supplementary Act A/SA. 1/01/10 on Personal Data Protection	15	4
	Cybersecurity	ECOWAS Directive C/DIR/1/08/11 on Fighting Cyber Crime	15	4
G8	Open government data	Open Data Charter	8	8
Ibero-American Data Protection Network	Protection of personal information/Cross-border information transfer	Data Protection Standards of the Ibero-American States	10	9
ICN	. Access to online platforms/competition	ICN Recommended Practices and Recommendations		
Industry associations	Cybersecurity	IEEE standards on cybersecurity		
	Updating the telecommunications reference paper	Standards by TIA, ETSI, IETF		
	Access to the internet	Standards by IEEE-SA, IETF, IAB, W3C, Internet society		
ISO/IEC	Facilitation of e-payments	ISO 20022		
	E-authentication and e-signatures	ISO 14553		
	Protection of personal information	ISO/IEC 27701		
	Cybersecurity	ISO/IEC 27000 family / IEC 62443		
	Updating the telecommunications reference paper	ISO/IEC standards on telecommunications		
	ICT products that use cryptography	ISO/IEC 18033		
ITU	Updating the telecommunications reference paper	ITU-T Recommendations		
OECD	Online consumer protection	OECD Recommendation on Consumer Protection in E-commerce	39	39
	Protection of personal information/Cross-border information transfer	OECD Privacy Guidelines	37	37
	Cybersecurity	OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity	39	39
	Cybersecurity	OECD Recommendation on Digital Security of Critical Activities	38	38
	Open government data	OECD Recommendation on Public Sector Information	38	38

	Access to online platforms/competition	OECD Recommendation concerning International Co-operation on Competition Investigations and Proceedings	40	40
	ICT products that use cryptography	OECD Guidelines for Cryptography Policy	37	37
SADC	Electronic transaction frameworks	SADC Model Law	16	0
UN	Cybersecurity	UN Charter and international law		
UN ESCAP	Paperless trading	UN ESCAP Framework Agreement	7	3
UN ESCWA	Electronic transaction frameworks	ESCWA Cyber Legislation Directives	20	5
UNCITRAL	Electronic transaction frameworks	UN Electronic Communications Convention	26	14
	Electronic transaction frameworks	UNCITRAL Model Law on Electronic Commerce	74	31
	E-authentication and e-signatures	UNCITRAL Model Law on Electronic Signatures	33	13
	Electronic transferrable records	UNCITRAL Model Law on Electronic Transferable Records	3	3
UNECE (incl. UN/CEFACT)	E-authentication and e-signatures	UN/CEFACT recommendation		
	Electronic invoicing	UN/CEFACT Cross Industry Invoice		
	Paperless trading	UN/EDIFACT standards for data exchange		
	Paperless trading	UNECE recommendations for international trade		
UNCTAD	Online consumer protection	UN Guidelines for Consumer Protection		
UPU	Customs procedures	UPU the Universal Postal Convention and its Regulations		
Wassennar Arrangement	Cybersecurity	The Wassenaar Arrangement	42	40
WCO	Customs procedures	WCO SAFE Framework / WCO Cross-Border E-commerce Framework of Standards		
WTO	Paperless trading	TFA	153	86
	Updating the telecommunications reference paper	WTO Telecommunications Reference Paper	103	69
	Goods market access	Information Technology Agreement	81	68
	Goods market access	Expanded Information Technology Agreement	53	52

Note: Empty cells reflect either lack of adoption or of publicly available information on adoption.
Source: based on author's analysis based on information in Annex A and B.

Annex Table C3. RTAs cover many areas

Specific areas	RTA provisions	WTO Members	JSI participants
Category I: provisions that more than 75% of JSI participants have included in their RTAs			
Protection of personal information/privacy	including a provision on data protection	103	79
	including provisions on data protection recognizing certain international standards	78	60
Online consumer protection	including a provision on consumer protection	98	76
Unsolicited commercial electronic messages/spam	including a provision on unsolicited commercial electronic messages	91	73
Customs duties on electronic transmissions	including provisions on the non-imposition of custom duties	90	70
Paperless trading	including a provision on paperless trading	78	70
E-authentication and e-signatures	including a provision on e-authentication and e-signature	87	66
Electronic transaction frameworks	mentioning avoiding unnecessary barriers to ecommerce, or to minimise the regulatory burden on electronic commerce	72	66
Category II: provisions that more than or about 50% of JSI participants have included in their RTAs			
Cybersecurity	including provisions on cyber security	66	61
Cross-border transfer of information by electronic means	including a provision on cross-border data flow	72	55
Electronic transaction frameworks	including a principle of technological neutrality	50	50
Access to the internet	including provisions on access to the Internet	46	44
Source code	including provisions on source code	42	41
Category III: provisions that more than or about 20% of JSI participants have included in their RTAs			
Non-discriminatory treatment of digital products	including a provision on national treatment or MFN treatment in e-commerce	35	29
Electronic transaction frameworks	referencing the UNCITRAL Model Law on Electronic Commerce	22	19
Location of computing facilities	including a provision on location of computing facilities	19	17
Category IV: provisions that are nascent (fewer than 20% of JSI participants have included in their RTAs)			
Electronic transaction frameworks	referencing the UN Electronic Communications Convention	15	12
Open government data	including provisions on open government data	7	7
ICT products that use cryptography	including provisions on cryptography	5	5
Interactive computer services	including a provision on interactive computer service	4	4

Note: Descending order of JSI participants. Data on RTA provisions related to Electronic invoicing, Facilitation of e-payment, Electronic transferrable records, Customs procedures, de minimis, location of financial computing facilities, telecommunications, online platform/competition are not provided in the TAPED dataset.
Source: author's calculation based on the TAPED dataset.