



The digital-only trade agreements – what is new?

1 Summary

As trade is becoming more digital, governments grapple with how to best regulate the digital economy and the implications following this development. The most recent regulatory approach is the digital-only trade agreements. They take a much broader approach than digital trade chapters in trade agreements usually do. Are the digital-only trade agreements as new and innovative as some may argue or not? This analysis will contribute to the discussion by looking at the two most recently concluded agreements Digital Economy Partnership Agreement (DEPA) and Digital Economy Agreement (DEA). DEPA is a stand-alone digital-only agreement that was signed in 2020 between New Zealand, Singapore, and Chile while DEA is an updated version of the old e-commerce chapter in the free trade agreement between Australia and Singapore.

DEPA has a “modular structure” which means that the different chapters include a glossary and have no cross-referencing between different chapters. The advantage of this is that countries could take one of the modules and include them in their bilateral agreements, avoiding fragmentation of trade rules. DEPA also covers topics that have previously not been part of trade agreements and it will undoubtedly serve as an inspiration to future digital trade chapters.

The clearest benefit of these agreements to international trade is the broader approach to digital trade covering issues like AI, Fintech, and digital identity. Although the commitments mostly are non-binding and focused on cooperation and dialogue, the value should not be underestimated. It is especially true in areas that are not heavily regulated today but where we see a development towards more rules and regulations. Making the regulatory approaches interoperable and avoiding fragmentation would be truly beneficial for the digital economy.

Another benefit is that they do contain slightly more legally binding and specific commitments on some issues such as paperless trade and e-invoicing. Some of these more ambitious provisions could also potentially be something for EU to include in its digital trade chapters.

Nevertheless, there are some more general drawback of these plurilateral agreements. Firstly, there is a general critique that plurilateral agreements might slow down the willingness to advance multilateral negotiations such as the ongoing e-commerce negotiations in the WTO. This could, in the long run, lead to a more fragmented regulatory system where it is difficult to find global solutions. Secondly, the lack of perspective from the view of a developing country might discourage countries that are not that technologically advanced to join the agreement. This mean that they are left out of the international regulatory development.

2 Background

Trade is becoming increasingly digital. It poses both opportunities and challenges for companies and regulators around the world. Although there is no globally agreed definition of what digital trade is, the OECD uses the definition “digitally-enabled trade in goods or services, whether digitally or physically delivered”. Governments possess multiple valid reasons to regulate the digital economy and digital trade. These include concerns for public security, law enforcement, national security, privacy, consumer protection, free speech, but also in ensuring that the opportunities and benefits from the global digital economy can be realised and shared inclusively. However, some raise worries that certain forms of regulation are essentially disguised restrictions on trade. There is no real consensus globally on how to best regulate the digital economy and how to find a balance between different policy objectives.

Many of the existing WTO rules apply also to digital trade, however, many legal uncertainties on definitions and applications remain. Even though there is some progress on the multilateral level there are also limitations to the existing WTO rules in governing digital trade which is why WTO members have turned to bilateral or plurilateral trade agreements to establish additional legal obligations.

The most recent development in the regulatory approach to digital trade is agreements like Digital Economic Partnership Agreement (DEPA) and Singapore-Australia Digital Economy Agreement (DEA). They represent a new type of trade agreement—one aimed at facilitating trade and

creating a framework for cooperation on digital issues. There is an ongoing discussion of what advantages and disadvantages these digital-only trade agreements have. A better understanding of their content and how it differs from other agreements is therefore important.

3 Aim

Our aim of this analysis is two-folded: To assess the benefit from DEPA and DEA from a trade policy perspective and to identify potential features that could be of use in EU agreements.

4 Scope and methodology

We have chosen to focus on the two most recently concluded digital-only agreements:

- Singapore-Australia Digital Economy Agreement (DEA)
- The Digital Economic Partnership Agreement (DEPA)

To assess the benefit the trade provisions are analysed and, when relevant, compared to other recent EU and non-EU agreements, as well as the most recent text proposals from the WTO JSI e-commerce (e-commerce initiative).¹ The analysis builds on a text comparison and previous mappings and analyses of DEA and DEPA.² The focus is to identify new and novel issues and provisions as well as the level of ambition of the provisions included.

The specific provisions are analyzed by looking at the legal enforceability, level of specificity and scope of the provision. The legal enforceability of the provisions is analyzed because even if an issue is covered by the agreement, it might still not be legally enforceable due to unclear or loosely formulated legal language. In general terms, an area is considered legally enforceable if the language used is precise and committing and if it has not been excluded from dispute settlement procedures under the agreement. Hence, just because a chapter is covered by dispute settlement provisions does not mean that it has content that may be meaningfully litigated under the terms of the agreement. Committing language includes terminology like 'shall' and 'will,' while aspirational language frames the issue in terms of future trade,

¹ INF/ECOM/62/Rev.2

² [Peters, Michael, 2022](#); [Duval & Mengjing, 2017](#); [Honey, Stephanie, 2021](#); [Canadian Bar Association, 2021.](#); [Soprana, Marta, 2021.](#); [International and Comparative Law Research Center, 2020](#) [Jones, Kira, Alves, Sands, 2021.](#)

cooperation, ‘the parties shall cooperate. . .’ or ‘dialogue shall be established...’³

The specificity is assessed by looking at how detailed the language is in the provision. For example, by referring to specific standards or setting out detailed exceptions when the provision does not apply. Nevertheless, a more specific language does not always mean stronger liberalizing commitments, instead, it could actually be more trade-restrictive. This must be assessed on a case-by-case basis. A provision can also have broader implications by including for example a sustainability perspective or extending the scope of the provision into new areas. Whether this is positive or not will have to be assessed for each provision.

The analysis is structured as follows: In section five we describe the structure of the DEPA and DEA. Section six contains the analysis of the different trade provisions in DEPA and DEA. Lastly, we present a discussion followed by a conclusion.

5 Structure of DEPA and DEA

5.1 DEPA

The DEPA is the first trade agreement dedicated to digital trade although it has a much wider conception of what constitutes ‘digital trade’ than conventional trade agreements. Other agreements often refer to digital trade as “affect trade by electronic means”, DEPA by contrast includes measures that “affect trade in the digital economy.”

The EU has until recently had a narrow scope on digital trade issues in its trade agreements under the chapter on services, investment, and e-commerce. EU-UK Trade and Cooperation Agreement (TCA) was the first agreement where the EU included a specific chapter on digital trade, even though the difference compared to, e.g. EU-Japan is limited.

DEPA covers areas that are not usually included in digital trade chapters such as artificial intelligence, digital identities, and digital inclusion. On many of these novel issues, the aim of the agreement is to establish a platform for cooperation, and promote mutual recognition rather than to agree on binding rules. Furthermore, DEPA does not include chapters

³ Froese, Marc D. Digital Trade and Dispute Settlement in RTAs: An Evolving Standard? [Microsoft Word - CPSA submission - Final - Froese.docx \(cpsa-acsp.ca\)](#)

that could be found in a comprehensive free trade agreement, such as market access for services and comprehensive rules on intellectual property (IP) and technical barriers to trade (TBT).⁴

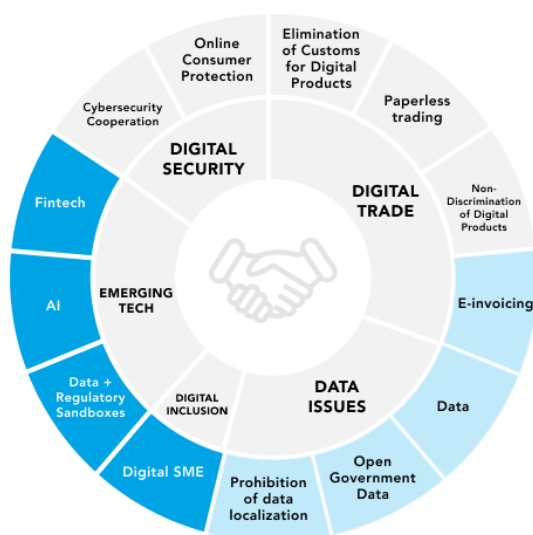


Figure 1. DEPA-modules, APF Canada

The agreement is structured around 16 different modules and has a Joint Committee that oversees the whole agreement. It also has a mechanism to amend and add new issues into the agreement. Each module contains a glossary providing definitions of relevant concepts and there is no cross-referencing between the modules. This means that countries could make use of individual components in their own bilateral or plurilateral agreements, or alternatively, dock on to the agreement as a whole. Furthermore, there is an accession process set out in the agreement and the authority to consider and approve the terms of accession lies with the Joint Committee. DEPA contains a dispute settlement process that is similar to what we usually find in other free trade agreements with some specific provisions excluded.⁵

5.2 DEA

DEA is an agreement entirely devoted to digital trade, but it is not a stand-alone agreement as DEPA. Instead, it is a bilateral agreement that has replaced the old e-commerce chapter in the FTA between Australia and Singapore. The scope of DEA is very similar to DEPA as it targets

⁴ Winters & Borchert, 2021. Addressing Impediments to Digital Trade. [Addressing Impediments to Digital Trade | VOX, CEPR Policy Portal \(voxeu.org\)](#)

⁵ See Annex 14.A.1, DEPA

the digital trade in a wider meaning. However, it excludes some DEPA topics (such as inclusion, logistics and government procurement) but on the other hand brings in a number of additional elements such as articles on standards and conformity assessment, stakeholder engagement, capacity-building and submarine telecommunications cable systems. The agreement is supported by seven memoranda of understanding which facilitate cooperation initiatives on data innovation, artificial intelligence, e-invoicing, e-certification for agriculture experts in imports, trade facilitation, personal data protection, and digital identity. DEA is subject to the general institutional structure and dispute settlement in the wider FTA between Singapore and Australia.

6 Analysis of the digital trade provisions

6.1 Digital trade

Paperless trade generally refers to the conduct of international trade transactions using electronic rather than paper-based data and documents. This generates significant economy-wide savings, including direct savings to traders in the form of lower compliance costs, as well as indirect savings from faster movement of goods and lower inventory costs.⁶ The Trade Facilitation Agreement (TFA) covers large parts of what is normally discussed on paperless trade, but it does not contain binding commitments on all relevant issues. The TFA is also crafted to take into account individual country situations and capacities to enable developing countries to participate.

Both DEPA and DEA have standalone provisions on paperless trade, with legally binding language where the Parties are obliged to accept electronic versions of documents. Both DEA and DEPA use the same definition for trade administration documents as in the e-commerce initiative. There are limited exceptions if there is “a domestic or international legal requirement to the contrary” or if paperless trading would “reduce the effectiveness of the trade administration process”. In comparison, there is no legally binding language on this in the e-commerce initiative. DEA and DEPA covers more types of documents and adds an obligation that the Parties should provide all publicly available electronic documents in English. The Parties also commit to endeavour to make these documents available in a machine-readable format. The agreement also encourages collaboration which could for example include facilitating cooperation between relevant private entities

⁶ Duval, 2017. Digital Trade Facilitation: [Paperless Trade in Regional Trade Agreements](#).

engaged in paperless trading. One example could be a committee on paperless trade geared towards reviewing implementation issues.⁷

EU agreements usually do not have a standalone provision on paperless trade in its digital chapters, but the EU is a member of the TFA. The EU agreement with Colombia and Peru includes the commitment to endeavor making trade management documents available electronically and to accept electronic documents as the legal equivalent of paper. The agreement with Korea also includes cooperation on implementing paperless trading.⁸

Both DEPA and DEA contain an article that the Parties “shall establish or maintain a **single window**” which also can be found in both the TFA and TCA. DEPA and DEA build on this specifying that the Parties shall endeavour “a seamless, trusted, high-availability and secure interconnection” between their single windows. This is important as it recognizes the practical advantages of compatible and interoperable single window systems and the use of open standards for paperless trading. It specifies “trusted” and “secure” which also are key components for effective single windows.

An **electronic signature (e-signature)** is an electronic indication of a person’s intent to agree to the content of a document or a set of data to which the signature relates. **Digital authentication (e-authentication)** refers to the techniques used to identify individuals, confirm a person’s authority or right, or offer assurance on the integrity of information.⁹ These two processes can be used together to first confirm the user and then signal intent. The most important reason to include such a provision in trade agreements is to encourage the Parties to maintain flexible and technology neutral laws and regulations in this area.

Only DEA has a standalone provision on e-authentication and e-signatures. It states that the parties shall not deny the legal validity of a digital signature or adopt measures that would prevent parties from using e-authentication, and it also encourages interoperable e-authentication systems. This is in line with what has been included in other EU agreements, CPTPP and proposed in the e-commerce initiative.

Another method for incorporating these requirements into national legal frameworks is by encouraging countries to adopt the 1996 UNCITRAL Model Law on Electronic Commerce (MLEC) as well as the UN

⁷ Seen in Japan-Singapore FTA

⁸ [UNECE, Paperless Trade](#)

⁹ [WEF, 2021, Making Deals in Cyberspace](#)

Convention on the Use of Electronic Communications in International Contracts from 2005 (MLETR). The intended aim is to provide a set of model rules for lawmakers to remove obstacles and increase predictability for e-commerce. DEA and DEPA commit to maintain a domestic legal framework consistent with MLEC and MLETR.¹⁰ In contrast to DEPA and the e-commerce initiative DEA says that the Parties will also endeavour to adopt the UNCITRAL Model Law on Electronic Transferable Records from 2017, which builds on previous model laws but is more updated and modern.

Digital identity refers to a broader conception of the information used by a computer system to identify an agent, which is most frequently considered to be an individual but could also be an entity, such as a corporation or a machine. Similarly, online electronic information can be linked to an individual or another entity to offer proof of identity. Like e-authentication, a multinational system for identification and approval would ease administration and promote digital trade. Interoperability is critical in managing digital identity systems; this is no different from the physical, offline world. Passports, for example, are based on standards agreed by the International Civil Aviation Organization to ensure they will be accepted worldwide. DEPA is the first trade agreement to cover the issue of digital identity and it is also included as a Memorandum of Understanding in DEA.

DEPA acknowledges the importance of digital identities. It also highlights interoperability and supports the establishment of a broader international framework. However, the provisions do not contain any legally binding language. Inclusion of digital identity in a trade agreement is seen to be a first step towards establishing a broader international framework.¹¹

An **electronic invoice (e-invoice)** is an invoice that is issued, transmitted, received, processed, and stored electronically using specific document formats. The provisions in DEPA and DEA are similar to those in the latest versions of the e-commerce initiative.¹² However, DEPA and DEA go further by mandating the members to work together in promoting interoperable e-invoicing systems. DEA and DEPA also mention “international standards” while the e-commerce initiative only

¹⁰ UNCITRAL model laws, though not legally binding, are designed to guide states in drafting legislation, while the ECC, as a treaty, is “hard law” that allows for less variation on formal adoption.

¹¹ [Norberg, Hewett, Ganne, 2021. Super Charging Trade With A Trusted Global Digital Identity System](#)

¹² INF/ECOM/62/Rev.2

refers to “international systems, guidelines or recommendations”. DEA uses the most detailed language in this regard by explicitly mentioning Peppol as one example. The DEPA also sets out the necessity of the Parties to facilitate the usage of e-invoicing by businesses. There is also best endeavor language on capacity building and underlying infrastructure which is not found in the e-commerce initiative. No commitments on e-invoicing can be found in the EU agreements such as TCA.

Electronic payments (e-payment) can be defined as the transfer of value from one payment account to another using digital devices. E-payments are critical to e-commerce as they enable secure, fast, and cheap transactions between buyers and sellers regardless of their physical location or currency. Specific regulatory rules on e-payments remain limited in multi- and bilateral agreements. Very few WTO members have made commitments for electronic payment services in their GATS-schedules and neither DEA nor DEPA contain any further market access commitments.¹³ The TFA contains a very general provision on e-payment relating to payment for duties, taxes, fees, and charges collected by customs.

DEPA recognizes certain principles that would assist in fostering the adopting of e-payment systems. It is the first agreement with provisions in this field. DEA differs notably from the DEPA, as it includes more binding provisions on electronic payments. DEA uses more detailed language including the use of international standards and rules (including ISO 20022), the development of open APIs (application programming interfaces) for national payment companies, and the use of cross-border authentication systems for users.

DEPA also includes new, best endeavor commitments to share best practices **on cross-border logistics regulations** that are specifically relevant to digital trade, such as last-mile deliveries, on-demand and dynamic routing solutions; the use of electric, remote-controlled and autonomous vehicles; and smart lockers that facilitate pick-up of on-line purchases. Both agreements also include more detailed language on expedited customs procedures for **express shipments** (DEA is limited to air express shipments) than the TFA and the e-commerce initiative. In addition, there is commitments for a **de minimis** shipment value or

¹³ World Trade Organization, Economic Research and Statistics Division, [Elevating Services: Services Trade Policy, WTO Commitments, and Their Role in Economic Development and Trade Integration](#) (Staff Working Paper ERSD-2019-018, March 2019).

dutiable amount for which customs duties will not be collected. In the e-commerce initiative the language is much more aspirational.

With regards to the **non-discrimination of digital products**, DEPA includes a basic obligation setting out a principle that countries will treat imported products from signatory countries in the same way as they do to their own. This applies mainly to a new wave of digital products defined in the Agreement as “computer programme, text, video, image, sound recording or other product that is digitally encoded, produced for commercial sale or distribution, and that can be transmitted electronically,” with a big exception for the broadcasting industry.¹⁴

Similar provisions on non-discrimination are found in other agreements such as CPTPP but is not included in EU agreements. DEA differs from DEPA in that it includes non-discrimination of “a digital product” which is in line with the US position in the e-commerce initiative. The use of “digital products” in DEPA and “a digital product” in DEA is also significant for the interpretation of the provision and could have far-reaching consequences for how discrimination is evaluated.¹⁵

The moratorium on the elimination of customs duties on electronic transactions has been extended permanently both in DEA and DEPA. There are ongoing discussions in WTO whether to make the moratorium permanent as well, but divergent positions remain.

DEPA and DEA include provisions on the use of **cryptography** in commercial applications, but it is excluded from the general dispute settlement mechanism. Cryptography and encryption are increasingly important as people and firms put more of their data online and engage with internet-based services. The presence of encryption in commercial applications has value both for safeguarding businesses’ intellectual property rights and protect societal values such as privacy. For goods containing cryptography for commercial applications, the Parties in DEPA agree not to apply technical regulations or conformity assessment procedures that require the manufacturer or supplier, as a condition of market access, to provide access to their technologies, create a joint venture, or use a specific cryptographic algorithm. The provisions also include exceptions for example for law enforcement authorities to access the encryption. Similar language is found in the TBT-chapter of CPTPP but not in EU agreements. However, EU agreements include general commitments to not impose joint venture requirements and gives

¹⁴ 2019/00284-51

¹⁵ [Non-discrimination Provisions in Digital Trade Chapters.](#)

protection for intellectual property in the context of giving access to technology as part of a conformity assessment.

Some governments have adopted policies that seek to mandate the sharing of **source code** or algorithms (typically from foreign firms) who enter into certain sectors. Such rules are positioned as security or regulatory mechanisms. Besides from regulatory demands, source code and algorithm mandates might act as a form of forced technology transfer. Source code rules in trade agreements seek to prevent forced technology transfer and protect sensitive commercial interests. Rules such as the CPTPP included only requirements on source code, but this has been enlarged to include algorithms in recent agreements such as the USMCA and DEA (as algorithms become more relevant to operation of products and services). DEPA does not contain a general clause against the mandatory disclosure of source code as a condition to conduct business, but DEA does.¹⁶ Recent agreements negotiated by the EU have included provisions banning forced disclosure of source code and software but have not gone as far as the language in DEA and USMCA to explicitly include algorithms in the scope of the provision. EU agreements also include a broader carve-out allowing Parties to require software or source code disclosure “to achieve a legitimate public policy objective”. Commitments on not disclosing source code are also included in the e-commerce initiative and discussions are ongoing on whether algorithms should be explicitly mentioned. The challenge with these kinds of provisions is to strike the right balance between protecting intellectual property, security concerns and algorithmic transparency.

DEPA also contains one of the strongest stand-alone carve-outs on **taxation** of any trade agreement, providing an almost total exception for tax measures. This means that there is nothing in the agreement hindering the Parties from introducing for example a digital service tax.

6.1.1 Conclusions on Digital Trade

Paperless trade

- DEPA and DEA contain more legally binding and more specific language on accepting electronic versions of documents than the e-commerce initiative and EU-FTAs. More legally binding commitments on these issues are positive for trade.

¹⁶ [Slok-Wodkowska & Mazur, 2022. Secrecy by default](#)

- Referencing to UNICTRAL Model Law on Electronic Transferable Records 2017 has a benefit as it contains more updated rules on paperless trade.

Single window

- DEA and DEPA specify how the single window for trade administration should function which promotes interoperability and trust between different systems. Possible further cooperation could include the development of a single window with cross-referencing between the e-commerce and customs chapters.

Digital identification and signatures

- DEPA and DEA do not go much further on e-authentication and e-signature compared to the e-commerce initiative, instead, it includes the novel issue of digital identity. The construction of a global standard for digital identities for firms and people seems difficult to achieve but could facilitate trade.

E-invoicing

- DEA and DEPA have more detailed language referring to specific standards that should be used compared to the e-commerce initiative. This topic is not included in EU agreements. This could potentially promote compatible and interoperable e-invoice systems.

Non-discrimination of digital products

- This is of great importance for digital trade and is not included in EU agreements. Including provisions like those in DEA and DEPA, practically resolves the issue around the classification of digital products and thereby eliminates the possibility of discrimination.

Cryptography & Source Code

- Cryptography is a privacy and IP protecting tool and is used in nearly all ICT products. Prohibiting governments to require encryption keys before market access is a step forward for protecting privacy, IP, and other commercial sensitive information from otherwise only prohibiting the disclosure of source code.

- DEA expands the scope of not requiring disclosure of source code to explicitly cover algorithms, this is currently discussed in the e-commerce initiative and is not included in EU-agreements. Future provisions need to find the right balance between protection of IP-rights, security, and other societal interests.

6.2 Data issues

The provisions relating to **data flows** in both DEA and DEPA are modelled on the CPTPP and commit the Parties to allow the cross-border transfer of information and ban data localisation measures. Both commitments are subject to an exception for “legitimate public policy” measures (which are not further defined) that pass a necessity test. Cross-border data transfer, including personal data, in a commercial context (this contrasts with the EU, where such transfers are generally forbidden). In addition, the Parties shall endeavour to cooperate on data-sharing projects, including data sandboxes to provide data-driven innovation. The Parties in both DEPA and DEA have also agreed to prohibit data localization requirements to ensure free data flows.

DEPA contains provisions on **personal information protection** that are similar to provisions found in CPTPP. It states that “each party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce and digital trade.” This article is followed by the caveat that each party may take different “legal approaches” to protect personal information and outlines a set of guiding principles for promoting the interoperability of standards. This is slightly more extensive than CPTPP. It sets out principles that should underpin a “robust legal framework” and requires countries to promote compatibility and interoperability between their different regimes for protecting personal information and provides some possible mechanisms to achieve this comparability.

The agreement encourages the use of data protection trust marks, that are used to verify conformance to personal data protection standards and best practices. Members shall also endeavor to mutually recognize the other members’ trust marks as a mechanism to facilitate cross-border information transfers. To simplify the conduct of business, the Parties undertake to publish open access manuals for businesses to ensure that their activities comply with the requirements of the legislation. To support fair business, it is proposed to introduce a special category of “trusted companies” that comply with personal data protection standards. DEA is not quite as ambitious but contains provisions that recognize and

promote the APEC Cross-border Privacy Rules (CBPR) and OECD guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data. In DEA the Parties commit to publishing information on the personal data protection it provides to users of e-commerce, including how individuals can pursue remedies and how businesses can comply with any legal requirements.

These issues are also discussed as a part of the e-commerce initiative in the WTO, but no text has been consolidated yet. EU takes quite a different approach to data flows and privacy in their trade agreements and prefers to have data transfers outside of trade agreements. In TCA the Parties agree to a list of specific data flow restrictions that will be prohibited. In all agreements except TCA the EU also specifically sets out privacy as a fundamental right. There is no requirement for Parties to show that the measure to protect privacy is necessary, non-discriminatory, nor the least trade-restrictive option. Hence, the TCA provides much greater regulatory autonomy than DEA and DEPA as privacy measures are not subject to any trade-related tests.

Open government data policies can help domestic and foreign businesses, including SMEs, identify new business opportunities. Both DEPA and DEA include provisions that say the Parties “shall endeavour” to make government data available. In EU agreements, it has been added that the Parties “shall endeavour, to the extent practicable” which is marginally weaker. DEA contains some more specific language on how the data should be made more publicly available. The text in the e-commerce initiative and TCA also requires members, to the extent practicable, ensure that government data they choose to make digitally and publicly available meets particular characteristics to make it easier to use, and to endeavour to avoid imposing certain conditions on such data.

DEPA has also introduced non-binding disciplines on the novel IP-topic of **public domains** where they recognise the importance of a rich and accessible public domain, and of informational materials, such as publicly accessible databases of registered intellectual property rights that assist in the identification of subject matter that has fallen into the public domain. However, DEPA offers no binding commitments on how to ensure accessibility of the public domain. Whilst possibly economically beneficial, the trade implications are unclear.

6.2.1 Conclusions on Data Issues

Privacy protection

- DEPA takes a middle ground approach compared to agreements such as CPTPP and EU agreements, as it sets out principles that underpin “a robust legal framework” of privacy. DEPA also includes examples of legitimate public policy objectives when exemptions can be made, that provide guidance for the Parties and more certainty for businesses.
- Provisions that reference international guidelines and recommendations from OECD and APEC are used as a basis for framing domestic data protection laws will ensure that there is consistency in digital trade frameworks across economies, this differs from EU agreements and the e-commerce initiative.
- In a new approach, DEPA recognises possible data transfer mechanisms such as the CBPR and data protection trust marks. This could ease barriers for businesses, increase digital trust and facilitate digital trade integration between the participants.

Open Government Data

- DEPA and DEA contain marginally more binding language on open government data compared to EU agreements and the e-commerce initiative.

6.3 Digital inclusion and SME

A novel issue addressed in DEPA addresses is small and medium-sized enterprises (SMEs), specifically in relation to digital trade. DEPA includes a module that aims to enhance trade and investment opportunities for SMEs through increased cooperation among the Parties, greater transparency, and outreach activities aimed at promoting the benefits of the agreement. DEPA includes an obligation to disseminate the relevant information by uploading and displaying it on a website set up specifically for this purpose. DEA has a similar article on SMEs which includes cooperation on regional capacity building. These kinds of provisions are also included in EU trade agreements but without a specific focus on digital trade and digital issues. The main difference is that EU-provisions are exempt from the general dispute settlement mechanism, which commitments in DEA and DEPA are not.

What is new is that DEPA also prescribes the creation of an additional format of cooperation, a so-called Digital SME Dialogue. Private sector aside, the representatives of non-commercial organizations, scholars and other interested persons are expected to participate in the dialogue. This format is envisaged to lead to the expansion of the benefits arising from the DEPA for the Parties' small and medium enterprises.

DEPA also introduces disciplines on digital inclusion, a novel issue that even DEA does not address. The Parties will cooperate to remove barriers to the participation in the digital economy of women, rural populations, vulnerable socioeconomic groups, and indigenous peoples; promote inclusive and sustainable economic growth; share experiences and best practices on digital inclusion; and develop programmes to promote participation of all groups in the digital economy. Although being in 'best endeavour' language, it can still be an important signal that the Parties to the DEPA consider digital inclusion an important aspect of the development of the digital economy. DEA on the other hand highlights the importance of stakeholder engagement by establishing a Digital Economy Dialogue.

6.3.1 Conclusions on Digital Inclusion and SME

- The SME-chapter in DEPA and DEA has a specific focus on digital trade issues and is subject to the dispute resolution in contrast to EU agreements. This makes commitments more enforceable, and therefore more impactful.
- The commitments on digital inclusion in DEA and DEPA are novel and take a broader approach to digital inclusion which can contribute to better cooperation and collaboration on a new and important issue.

6.4 Digital security

The provisions on **consumer protection** in DEPA is especially tailored for protecting consumers in the e-commerce space and it requires the Parties to maintain laws for this purpose. For instance, "fraudulent, misleading or deceptive conduct" is defined to include "advertising goods or services for supply without intention to supply" to include online fraudulent and misleading advertising. The consumer protection

law is required to “at the time of delivery, goods and services provided to be of acceptable and satisfactory quality, consistent with the supplier’s claims regarding the quality of the goods and services”.

The TCA includes quite a strong language on consumer protection compared to earlier EU agreements but is not especially focused on e-commerce. The TCA stipulates in detail the nature of the consumer protection measures that the Parties will adopt. The Parties also “recognise the importance of entrusting their consumer protection agencies or other relevant bodies with adequate enforcement powers” and the importance of cooperation between these agencies to protect consumers and enhance online consumer trust.

DEPA and DEA, compared to the e-commerce initiative, contain more detailed language on what constitutes fraudulent behaviour and also try to address the lack of a cross-border redressal mechanism for consumers. On top of that, DEPA states that the Parties shall undertake to explore alternative dispute resolution mechanisms for electronic commerce transactions.

One area where the EU provisions are slightly more detailed than both the e-commerce initiative as well as DEPA and DEA is **SPAM**, where EU agreements typically require the prior consent of recipients to receive commercial electronic messages and provide the possibility of recourse.

Both DEPA and DEA have novel provisions on the broader issue of **online safety and security** where the Parties address issues such as harmful content and recognize that governments and technology providers and users have a shared responsibility. Other EU and non-EU agreements as well as the e-commerce initiative do not have this broad approach but instead include several provisions on related issues such as intermediate liability and network neutrality.

Both DEPA and DEA include a provision on **cybersecurity** but do not develop commitments compared to what is proposed in the e-commerce initiative.¹⁷ The issue of cybersecurity is not dealt with in any detail in EU agreements except TCA where there are specific provisions as part of the broader agreement cooperation agreement with the UK, which is not specifically related to trade. The USMCA is quite unique in this regard as it includes a recognition of the importance of taking a risk-based

¹⁷ A trade agreement that does go further is USMCA that 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

approach to cybersecurity instead of proscriptive approaches, including risk-based approaches that rely on consensus-based international standards and best practices.

6.4.1 Conclusions on Digital Security

Consumer protection:

- On consumer protection, TCA has more explicit provisions than both DEPA and DEA.

SPAM

- EU has very strong provisions on SPAM in its trade agreements. DEPA and DEA do not bring much benefit compared to TCA or the e-commerce initiative.

Online trust

- DEPA takes a comprehensive approach to online safety and security which is positive from a trade perspective since trust in the online environment is important for advancing digital trade.

Cyber security

- DEPA and DEA do not contain more ambitious language than what can be found in the e-commerce initiative.

6.5 Emerging technologies

The DEPA dedicates an entire module to the issue of emerging trends and technologies, establishing disciplines on a number of topics also covered by DEA, namely promotion of cooperation on **financial technology** (Fintech), **artificial intelligence**, and **competition policy** in the digital markets, **data innovation**, as well as **digitisation of procurement processes**.

On AI, DEPA establishes that the Parties shall endeavour to promote the adoption of AI Governance Frameworks taking into consideration internationally recognised principles or guidelines, including explainability, transparency, fairness, and human-centered values. Never before has an international trade agreement addressed issues related to a specific type of technology underpinning the digital economy.

The provisions regarding AI are using “best endeavour” language while the provisions on financial technology and on government procurement contain more specific language. The Parties shall promote cooperation between firms in the Fintech sectors, endorse the development of Fintech solutions for business or financial sectors, and cooperate to better understand how greater digitisation of procurement processes, and of goods and services impacts on. On competition policy, the Parties “shall consider” to undertake cooperation activities.

Both agreements also include provisions on data innovation where they recognize the need for “regulatory sandboxes” where data including personal data can easily be shared between businesses.

DEA also has a provision specifically on standards where the Parties recognize the role of standards and mechanisms which facilitate the cross-border recognition of conformity assessment. Future cooperation relating to standards and conformity assessment could include exchanging best practices and identifying joint initiatives in the field of standards. It could also involve co-operation between governmental and non-governmental bodies, including research or test-bedding projects. This is a sort of regulatory cooperation which is beneficial to create more coherent global trade rules.

6.5.1 Conclusions on Emerging Tech

- Even though the language is not legally binding in DEPA or DEA it contains important commitments to cooperate and work together on regulations and standards in fast-evolving areas. This could contribute to more harmonized rules which would be beneficial for digital companies.

7 Discussion

The clearest benefit of DEPA and DEA compared to other digital trade chapters and agreements is the more comprehensive approach to digital trade, demonstrating that many issues have implications beyond trade.

DEPA and DEA include completely novel commitments on issues such as AI, Fintech and digital identity which is clear innovation compared to other trade agreements. This development is significant even though they only use “best endeavour” language and have a focus on cooperation and dialogue. It might even be better to have the possibility to choose

different regulatory approaches while ensuring interoperability as it makes it possible to cooperate on complex issues that are not yet heavily regulated such as AI.

On more traditional digital trade issues DEPA and DEA have more legally binding language in some cases (e.g., paperless trade, single window, and open government data), use more detailed language (e.g., e-payment and logistics) and broadens the scope (e.g., e-invoicing and source code) compared to the e-commerce initiative and other trade agreements. However, this is not the case in every aspect as there are issues where EU agreements or the e-commerce initiative are at least as good or more ambitious. Still, DEPA and DEA can serve as an inspiration to how future EU or multilateral agreements on e-commerce could be developed.

As DEPA only covers digital trade, it lacks market access commitments and comprehensive IPR- and TBT-commitments, which clearly have a significant bearing on digital trade. In that sense, DEPA falls short of what could potentially be achieved in a more comprehensive free trade agreement. On the other hand, it could also be argued that excluding market access commitments makes it easier for some countries to sign on to digital trade rules as negotiations can focus on a more limited number of issues as opposed to more comprehensive agreements.

DEPA is also said to be an “open agreement” that all countries can join if they can meet its standards. Nevertheless, capacity-building disciplines are almost completely missing from the agreement (only mentioned in relation to e-invoicing). This is probably because all the signatories are developed economies with a high level of digital readiness. However, this might discourage developing and least developed countries to join. In this regard, DEA is a better inspiration with more focus on capacity building.

The modular approach of DEPA has been celebrated for being innovative and flexible. There are certainly advantages of this approach as the modules could serve as an inspiration to other bilateral and multilateral agreements. However, in contrast to what sometimes has been argued, countries will need to sign up to the agreement as a whole and there is not much possibility to renegotiate the agreement when joining. That said, modules can be copied by countries wishing to take inspiration from the DEPA, making it a vehicle for regulatory development. However, this raises the question on whether increasing plurilateral agreements are

beneficial on a global level because it advances cooperation, or if it will increase regulatory fragmentation.

The World Trade Report 2011 phrased this problem as *“in the absence of multilateral participation through a consensus-based process, a risk exists that a subset of the membership could shape rules from which they benefitted, but at the expense of members that were not part of the critical mass.”*

Nevertheless, rules on far-reaching interoperability, compatibility and mutual recognition will probably never be achieved on a multilateral level. Hence, agreements like DEPA, DEA and other digital partnerships could in this regard have an added value. This means that agreements like DEPA and DEA could be seen as a complementary aspect of an increasingly complex and sophisticated global trade architecture – one in which bilateral, regional, and multilateral agreements coexist and cohere in a kind of “multispeed” system.

It is also important that agreements like DEPA do not create inconsistencies in the global trade framework or lead to more fragmentation of digital trade rules. Both DEA and DEPA try to overcome this by promoting international standards, in particular open standards, and model laws. Being a bilateral agreement DEA has more emphasis on compatibility setting out specific standards and more focus on mutual recognition. DEPA focuses more on interoperability where it acknowledges that countries can have different systems technically but that there needs to be coherence through for example API's. The standalone article in DEA on “Standards and Conformity Assessment for Digital Trade” shows that the compatibility of standards, the development of common standards and the use of international standards are prioritized. Promoting the use of international standards through agreements like DEPA and DEA is positive, but it is important to be aware of the definition of an “international standard” or “open standard”. International standard implies that it is decided in a process that it is open to stakeholders of WTO members and has been decided in consensus through a formal standardisation organisation (such as ISO/IEC) in accordance with the WTO principles on standardisation. Even if these requirements are not interpreted uniformly as e.g., ISO or IEC standards, foremost by the USA, a shift towards open standards comes with a risk of further fragmentation. References to “open standards” might be problematic since there is no globally agreed definition. Open standards may mean that the process follows other requirements and that open standards can also be developed in different fora or consortia without

necessarily following standardization principles such as open participation and therefore might not always be developed in accordance with the TBT-agreement

8 Conclusions

DEPA and DEA do add some more legally binding and specific language on some topics but are not as “innovative and novel” as some have argued compared to the e-commerce initiative and other trade agreements. The lack of capacity-building provisions in DEPA is also problematic from a developing country perspective. Nevertheless, cooperation and regulatory dialogue should not be underestimated especially on issues such as AI or digital identity where more regulation is likely to come. Promoting interoperability through these kinds of agreements are truly beneficial although doing so in an open and inclusive way is important.

There are several issues and commitments in DEPA and DEA that could potentially be included in digital chapters in EU agreements, including:

- Binding provision on paperless trading and establishing a multistakeholder cooperation framework to identify implementation issues.
- Binding commitments on working towards making single windows interoperable.
- Commitments to adhere to UNICTRAL model laws when developing legal frameworks of e-transactions.
- Encouraging the use of international standards for example when developing digital identity frameworks.
- Commitments on e-invoices.
- Cooperation on emerging technologies and digital inclusion.

Ärendet har avgjorts av enhetschef Pernilla Trägårdh i närvaro av utredarna Sophia Tannergård, Felinda Wennerberg, Anders Karlsson, Emma Wallfelt, ämnesrådet Anna Egardt samt ämnesrådet Emma Sävenborg, föredragande.

Pernilla Trägårdh

Emma Sävenborg