§ 16
Digital trade

Literature: Andersen, Henrik, Protection of Non-Trade Values in WTO Appellate Body Jurisprudence: Exceptions, Economic Arguments, and Eluding Questions, JIEL (2015), 383; Andrenelli, Andrea/Gourdon, Julien/Moïsé, Evdokia, International Technology Transfer Policies, OECD Trade Policy Papers 2019, https://doi.org/10.1787/7103eabf-en (last accessed: 30 June 2023); Brakman, Steven/Garretsen, Harry/Kohl, Tristan, Consequences of Brexit and Options for a 'Global Britain', Pap Reg Sci. 2017, 55; Burri, Mira, Approaches to Digital Trade and Data Flow Regulation across Jurisdictions, LIEI 2022, 149; Burri, Mira, Data Flows and Global Trade Law, in Burri (ed.), Big Data and Global Trade Law, Cambridge 2021, p. 11; Burri, Mira, Fake News in Times of Pandemic and Beyond: Exploring of the Rationales for Regulating Information Platforms, in Mathis/Tor (eds.), Law and Economics of the Coronavirus Crisis, Berlin 2022, p. 31; Burri, Mira, Interfacing Privacy and Trade, Case W. Res. J. Int'l L. 2021, 35; Burri, Mira, The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation, U.C. Davis L. Rev. 2017, 65; Burri, Mira, The International Economic Law Framework for Digital Trade, ZSR 2015, 10; Burri, Mira, Towards a New Treaty on Digital Trade, JWT 2021, 77; Burri, Mira, Trade Law 4.0: Are We There Yet?, JIEL 2023, 90; Burri, A WTO Agreement on Electronic Commerce: An Inquiry into Its Legal Substance and Viability GJIL 2023; Burri, Mira/Polanco, Rodrigo, Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset, JIEL 2020, 187; Chander, Anupam/Lê, Uyên P., Data Nationalism, Emory L. J. 2015, 677; Choromidou, Anastasia, EU Data Protection under the TCA: The UK Adequacy Decision and the Twin GDPRs, IDPL 2021, 388; Fahey, Elaine, Digital Trade and Data Equivalency: Research Briefing for the Welsh Parliament, Wales 2020; Gao, Henry S., Regulation of Digital Trade in US Free Trade Agreements: From Trade Regulation to Digital Regulation, LIEI 2018, 47; Gibson, Christopher S., Globalization and the Technology Standards Game: Balancing Concerns of Protectionism and Intellectual Property in International Standards, Berkley Tech. L. J. 2007, 1403; Hallak, Issam et al., EU-UK Trade and Cooperation Agreement: An Analytical Overview, EPRS 2021; Henke, Nicolaus/Bughin, Jacques/Chui, Michael/Manyika, James/Saleh, Tamim/Wiseman, Bill/Sethupathy, Guru, The Age of Analytics: Competing in a Data-Driven World, McKinsey Global Institute 2016; Irion, Kristina, AI Regulation in the European Union and Trade Law: How Can Accountability of AI and a High Level of Consumer Protection Prevail over a Trade Discipline on Source Code?, The Institute for Information Law 2021, 1, https://www.ivir.nl/publicaties/download/Irion_study_ai_and_trade_21-01-26-1.pdf (last accessed: 30 June 2023); Irion, Kristina, Algorithms Off-Limits? If Digital Trade Law Restricts Access to Source Code of Software Then Accountability Will Suffer, FAccT '22: 2022 ACM Conference on Fairness, Accountability, and Transparency 2022, 1561, https://doi.org/10.1145/3531146.3533212 (last accessed: 30 June 2023); Irion, Kristina/Yakovleva, Svetlana/Bartl, Marija, Trade and Privacy: Complicated Bedfellows? How to Achieve Data Protection-proof Free Trade Agreements, The Institute for Information Law 2016, 1; Jones, Emily/Kira, Beatriz/Garrido Alves, Danilo B./Sands, Anna, The UK and Digital Trade: Which Way Forward?, BSG-WP 2021, https://doi.org/10.35489/BSG-WP-2021/038 (last accessed: 30 June 2023); Kleimann, David (ed.), EU Preferential Trade Agreements: Commerce, Foreign Policy, and Development Aspects, European University Institute 2013; Mayer-Schönberger, Viktor/Cukier, Kenneth, Big Data: A Revolution That Will Transform How We Live, Work, and Think, New York 2013; Meltzer, Joshua P./Kerry, Cameron F., Cybersecurity and Digital Trade: Getting It Right, The Brookings Institution 2019, https://www.brookings.edu/research/cybersecurity-and-digital-trade-getting-it-right/ (last accessed: 30 June 2023); Natens, Bregt/Zimmermann, Claus D., Prudential Carve-outs for Financial Services in EU FTAs, in Hahn/Van der Loo (eds.), Law and Practice of the Common Commercial Policy, Leiden 2020, 259; Schwartz, Paul M./Solove, Daniel, Reconciling Personal Information in the United States and European Union, Cal. L. Rev. 2014, 877; Słok-Wódkowska, Magdalena/ Mazur, Joanna, Secrecy by Default: How Regional Trade Agreements Reshape Protection of Source Code, JIEL 2022, 91; Weber, Rolf H./Burri, Mira, Classification of Services in the Digital Economy, Berlin 2012; Weiß, Wolfgang, The EU-UK Trade and Cooperation Agreement: an unfinished deal, University of Birmingham Institute of European Law Working Paper 02–202, https://www.birmingham.ac.uk/documents/college-artslaw/law/iel/workingpaper202102.pdf (last accessed: 30 June 2023); Wunsch-Vincent, Sacha, The WTO, the Internet and Digital Products: EC and US Perspectives, Oxford 2006; Yakovleva, Svetlana, Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy, U. Mia L. Rev. 2020, 416; Yakovleva, Svetlana/Irion, Kristina, Pitching Trade against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade, IDPL 2020, 201; Yakovleva, Svetlana/Irion, Kristina, Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation, AJIL Unbound 2020, 10.

A. Introduction

1 With the advanced process of digitisation and the critical importance of data to global economies,[1] digital trade has moved up on the agendas of policymakers in general and trade negotiators in particular. Considering the pre-Internet rules of the World Trade Organization (WTO),[2] and notwithstanding the recent reinvigoration of the e-commerce negotiations following the 2019 Joint Initiative,[3] WTO law has so far not been adjusted to address digital trade. Many of the disruptive changes underpinning the data-driven economy have demanded regulatory solutions outside the multilateral forum of the WTO. States around the world have, in particular, used the venue of **free trade agreements** (FTAs) to keep pace – both by filling in some of the gaps in the WTO framework and by addressing newer **digital trade barriers** and phenomena of the **data-driven economy**, such as data localisation measures.[4] Next to the promotion of cross-border trade, FTAs have also become vehicles for the pursuit of other, not purely economic, objectives, such as personal data and consumer protection.

[1] See e.g. Mayer-Schönberger/Cukier 2013; Henke/Bughin/Chui/Manyika/Saleh/Wiseman/Sethupathy McKinsey Global Institute 2016; WTO, World Trade Report 2018: The Future of World Trade: How Digital Technologies Are Transforming Global Commerce, 2018; WTO, E-Commerce, Trade and the Covid-19 Pandemic, Information Note by the WTO Secretariat, 4 May 2020.

[2] See e.g. Burri ZSR 2015, 10; Burri U.C. Davis L. Rev. 2017, 65; WTO, World Trade Report 2018: The Future of World Trade: How Digital Technologies Are Transforming Global Commerce, 2018.

[3] WTO, Joint Statement on Electronic Commerce, 25 January 2019, WT/L/1056. As of 29 March 2019, 89 WTO Members support the initiative. For details, see Burri J. World Trade 2021, 77; Burri GJIL 2023, 565.

[4] See e.g. United States International Trade Commission (USITC), Digital Trade in the US and Global Economies, Part 1, 2013, Investigation No. 332–531; USITC, Digital Trade in the US and Global Economies, Part 2, 2014, Investigation No 332–540; Chander/Lê Emory L. J. 2015, 677.

Presently, out of the 384 agreements signed between January 2000 and December 2022, 167 contain provisions on digital trade.[5] These may be found in different parts of the treaties, such as in the chapter on services or intellectual property rights. Increasingly, these provisions are bundled inside dedicated **digital trade chapters**,[6] which have become an important 'laboratory' for new international rulemaking on digital trade. Although the governance framework is highly diverse as to the Parties, the issues covered and the level of commitments,[7] the last five years have marked the emergence of more sophisticated templates on digital trade and dedicated **digital trade agreements** that have created a model with distinct features and wider diffusion. One could also trace the clearer positioning of the key players, such as the United States (US) and the European Union (EU), on issues of digital trade governance. In this context, it is interesting to explore how the TCA's digital trade chapter fits into this landscape. 2

The negotiation history of the TCA clearly reveals the high stakes of digital trade in the post-Brexit arrangements that reflect the growing strategic significance of digital trade and cross-border data flows. This contribution on the TCA digital trade chapter unpacks the regulatory context (→ mn. 4 et seq.), provides a commentary of the substantive provisions (→ mn. 6 et seq.), and offers a comparative analysis of the TCA digital trade chapter with other trade deals of the EU and of other key players (→ mn. 30 et seq.). One of the key issues of the EU-UK negotiations had been calibrating the interplay between the commitments on cross-border data flows and the protection of personal data and privacy, which merits a special focus in this contribution (→ mn. 11 et seq., 25, 29). It is here that the TCA digital trade chapter signifies an interesting new modification of the EU external trade strategy at the interface between trade and privacy,[8] with potentially important consequences for both the EU and the UK. The contribution concludes with an appraisal and an outlook (→ mn. 52). 3

B. Legal context of the Digital Trade Title

The digital trade chapters play a dual role in the landscape of trade rules in the digital era. On the one hand, they represent an attempt to compensate for the lack of progress in the WTO and remedy some of the ensuing uncertainties. These chapters address many of the questions of the **1998 WTO E-Commerce Programme**,[9] which despite their pertinence and the recognition by the WTO membership that adjustments may be needed in the face of the technological changes triggered by the internet, could not be translated into action in the past two decades.[10] On the other hand, the digital trade chapters do also include rules that have not been treated in the context of the WTO negotiations. One can group these rules into two broader categories: (1) rules that seek to **enable digital trade** by addressing the promotion and facilitation of e-commerce in general and by tackling distinct issues, such as paperless trading and electronic authentication; and (2) rules that address **cross-border data** 4

[5] This analysis is based on a dataset of all data-relevant norms in trade agreements (TAPED) administered by the University of Lucerne. See https://unilu.ch/taped (last accessed: 30 June 2023) and Burri/Polanco JIEL 2020, 187.

[6] Depending on the agreement these chapters are titled differently, e.g. e-commerce, electronic or digital trade.

[7] Burri/Polanco JIEL 2020, 187; Burri (2021), 11.

[8] Yakovleva/Irion IDPL 2020, 201.

[9] WTO, Work Programme on Electronic Commerce, 30 September 1998, WT/L/274.

[10] Wunsch-Vincent 2006; Burri GJIL 2023, 565.

flows, new digital trade barriers and newer issues, such as cybersecurity or open government data.

5 The TCA Digital Trade Title (Part Two, Title III) structures the economic relationship and cooperation between the EU and the UK in the area of cross-border digital trade after Brexit and the withdrawal of the UK from the EU single market.[11] The TCA Digital Trade Title could start from an elevated level of **regulatory convergence**, which is not a given in EU external relations with other countries. It is precisely this special relationship the TCA builds on when formalising Title III on Digital Trade of the TCA. The TCA digital trade chapter is considered best in class, although cross-border flows of personal data between the EU and the UK remain contingent on regulatory approval in the form of an adequacy decision (→ mn. 18). This Title holds commitments that to a certain extent emulate the digital trade templates from bilateral and regional trade agreements in the world (→ mn. 37 et seq.). Similar to this new generation of FTAs, the TCA also seeks service liberalisation beyond what has already been achieved under the GATS (GATS-plus). In order to achieve this the TCA combines disciplines that are designed to liberalise the cross-border supply of digital services with commitments that aim for regulatory harmonisation.[12]

C. Key elements

6 With just 16 articles, Title III of Part Two of the TCA concisely covers digital trade issues divided into three chapters. Chapter 1 contains the general provisions that govern Title III, such as the objective, scope, and definitions (Articles 196 to 200 TCA). Chapter 2 on Data Flows and Personal Data Protection holds two sets of interrelated commitments: one on cross-border data flows (Article 201 TCA) and the other on the protection of personal data and privacy (Article 202 TCA). Chapter 3 on Specific Provisions assembles miscellaneous commitments in the field of digital trade that can be grouped in five themes: (1) promoting the cross-border supply of digital services; (2) enabling electronic transactions; (3) online consumer protection; (4) open government data; and (5) cooperation on regulatory issues.

I. Chapter 1: General provisions

7 The TCA's Digital Trade Title has the stated objective 'to facilitate digital trade, to address unjustified barriers to trade enabled by electronic means and to ensure an open, secure and trustworthy online environment for businesses and consumers' (Article 196 TCA). This Chapter applies to measures of a Party affecting trade enabled by electronic means, with the **exception of audiovisual services** (Article 197 TCA). The latter reflects the longstanding practice of the EU to exclude audiovisual services from its international trade agreements, even in deals with like-minded partners on cultural protection issues, as is the case for Canada under the Comprehensive Economic and Trade Agreement (CETA).

8 Definitions that are provided for in Article 124 of Title II on Services and Investment are incorporated into the TCA Digital Trade Title by Article 200. This is how key notions such as 'service', 'cross-border trade in services' and 'service supplier' apply to

[11] UK Government, The Future Relationship with the EU: The UK's Approach to Negotiations, 3 February 2020, para. 58.

[12] Yakovleva/Irion IDPL 2020, 201.

the Digital Trade Title (→ § 13 mn. 29). In this context, Article 212 TCA comes into play by which Parties agree on a common understanding on **computer and related services** for the purpose of liberalising trade in services and investment in accordance with Title II. Other services, even where they are enabled by computer and related services but are not listed in paragraph 1 of Article 212 TCA, are not to be regarded as computer and related services. This understanding adopts a number of definitions of services that shall be henceforth considered as computer and related services, regardless of whether they are delivered via a network, such as the Internet (Article 212 TCA). This concerns various commercial activities surrounding the provision of computers or computer systems as well as computer programmes that are defined as 'the sets of instructions required to make computers work and communicate' (Article 212(1)(b) TCA). Moreover, data processing, data storage, data hosting or database services are generically considered computer services. Such a common understanding on what qualifies as computer and related services can avoid a number of difficult classification issues when it comes to the interpretation of a Party's schedule of commitments, which has been a thorny issue ever since the start of the WTO E-Commerce Programme.[13] In addition, Article 200 TCA introduces a number of definitions and concepts which are mainly used in Chapter 2 of Title III on digital trade in the context of harmonising electronic commerce transactions and some basic tenets of consumer protection.

9 As part of the general provisions, the TCA Parties also reaffirm their **right to regulate** within their territories to achieve legitimate policy objectives (Article 198 TCA). The policy objectives which are explicitly listed in connection with the right to regulate are the protection of public health, social services, public education, safety, the environment including climate change, public morals, social or consumer protection, privacy and data protection, or the promotion and protection of cultural diversity. However, this listing is not exhaustive as the formulation 'such as' indicates. This gives the Parties leeway to maintain and introduce measures on the interface between digital trade and a number of non-economic objectives. It is worth noting that the path to exercising a Party's right to regulate is through the general exceptions (Article 412 TCA) unless a more specific exception of the TCA applies.

10 Furthermore, for greater certainty, a reference to the **exceptions** of the TCA is incorporated into the Chapter on digital trade (Article 199 TCA). These are namely the general exceptions for legitimate reasons of public interest (Article 412 TCA), the security exceptions (Article 415 TCA), and the prudential carve-out to ensure the integrity and stability of a Party's financial system (Article 184 TCA). Both the general exceptions and the security exceptions are standard exceptions. Their language is modelled after their respective counterparts in WTO law (GATT Article XX and Article XXI, as well as GATS Article XIV and Article XIV*bis*). Note, however, that reliance on the general exceptions (Article 412 TCA) involves an assessment as to whether a measure achieves a legitimate public interest objective in a least trade-restrictive manner. The security exceptions (Article 415 TCA), by contrast, are largely self-judging as long as a link between a Party's measure and the security objective can objectively be established.[14]

[13] Weber/Burri 2012.
[14] See Meltzer/Kerry The Brookings Institution 2019.

II. Chapter 2: Data flows and personal data protection

11 The core issue – judged by its political-economic contentiousness, as well as its centrality for the contemporary data-driven economy – can be found in Chapter 2 on Data Flows and Personal Data Protection. The combined treatment of cross-border data flows (Article 201 TCA) and the protection of personal data and privacy (Article 202 TCA) is justified in light of their interdependency. Reconciling the economic policy objective of **free cross-border data flows** from the EU to the UK, and vice versa, with the objective of ensuring a **high level of personal data protection** largely follows the established EU template, as discussed below (→ mn. 13 et seq., 30 et seq.).

1. Cross-border data flows

12 The mutual commitments on cross-border data flows that are intended to facilitate trade in the digital economy are laid down in Article 201 TCA. Instead of a general commitment that would liberalise cross-border data flows as such, the Digital Trade Title lists **prohibited restrictions to cross-border data flows**. Article 201 TCA prohibits four specific instances of measures that restrict cross-border data flows: first, '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'; second, 'requiring the localisation of data in the Party's territory for storage or processing'; third, 'prohibiting the storage or processing in the territory of the other Party'; or fourth, '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'. What is interesting about the fourth instance of a prohibited restriction is that it does not only cover the relationship between the EU and the UK but also prohibits a measure that would seek to restrict the ability to transfer data that has been received from the other Party onward. Parties pledge to review the functioning of the provision within three years of the TCA's entry into force. Such a review is also possible upon request from one Party, which makes the commitments dynamic and pliable (Article 201 para. 2 TCA). Note that there is a dedicated commitment for the cross-border movement of information in Section 4 of Chapter Five on Telecommunications Services that operationalises its own rule-exception logic.[15]

2. Protection of personal data and privacy

13 Pursuant to para. 1 of Article 202 TCA, Parties recognise 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'. Article 202 TCA reproduces almost verbatim the European Commission's 'Horizontal Provisions for Cross-border Data Flows and for Personal Data Protection in EU Trade and Investment Agreements' which represent a compromise struck in 2018.[16] The TCA modifies the textual template slightly by dropping the reference to the protection of personal data and privacy as a 'fundamental' right even though this would hold true for the EU and the UK alike: while the Charter of Fundamental Rights of the EU

[15] See Art. 170 para. 3 TCA.

[16] European Commission, Horizontal Provisions for Cross-border Data Flows and for Personal Data Protection, News release of 18 May 2018, https://ec.europa.eu/newsroom/just/items/627665 (last accessed: 30 June 2023); see also Yakovleva/Irion IDPL 2020, 201 (217 et seq.); Yakovleva/Irion AJIL Unbound 2020, 10 (11).

(CFR) enshrines both the right to private life (Article 7 CFR) and a self-standing right to the protection of personal data (Article 8 CFR), the UK incorporates the European Convention on Human Rights (ECHR) via the Human Rights Act of 1998 into its domestic law. Article 8 ECHR guarantees the right to respect for private and family life as an umbrella right that covers the protection of personal data.[17] Ultimately, there are no consequences attached to toning down the language of this declaratory statement if only for the symbolic dimension of dropping a reference to fundamental rights. Should the UK decide to repeal the Human Rights Act and move away from the ECHR this becomes an issue for maintaining an adequacy decision (→ mn. 18).[18]

14 The language used to underscore the value of the protection of personal data and privacy is of declaratory nature ('recognise') and is thus comparable to reaffirming the right to regulate (Article 198 TCA). In this context, also note Article 769 TCA on personal data protection of the Title II on Basis for Cooperation, where the Parties 'affirm their commitment to ensuring a **high level of personal data protection**'. Para. 4 of Article 769 TCA provides that '[w]here this Agreement or any supplementing agreement provide for the transfer of personal data, such transfer shall take place in accordance with the transferring Party's rules on international transfers of personal data'. If, however, bilateral trade agreements are about creating enforceable commitments between the Parties then these declarations are only recognised in connection with an enforceable provision or, alternatively, inside the general exceptions for public interest regulation (Article 412 TCA).

15 The actual counterbalancing provision can be found in para. 2 of Article 202 TCA: '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 for the protection of the data transferred'. This is how, within the TCA, a Party can nevertheless adopt a measure that regulates – and thereby restricts – the cross-border transfer of personal data to the other Party or the onward transfer of the data to yet other countries, even where this **contravenes Article 201** TCA. The language of the provision is crafted quite similarly to the 'prudential carve-out' that is used in the financial services chapters.[19] By trade law standards, this is a very robust design to counterbalance commitments entered into as the legal bar is set much lower in comparison to the general exceptions for legitimate reasons of public interest (Article 412 TCA).

16 A close reading reveals that the application of Article 202 para. 2 TCA has two **requirements**. First, the measure must have as an objective the protection of personal data and privacy, thereby excluding unrelated measures from the scope of the provision. Second, the law of the Party must provide for 'instruments enabling transfers under conditions of general application for the protection of the data transferred' (Article 202 para. 2 TCA). Following an explanatory footnote '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'.[20] In other words, the counter-balancing provision is designed to benefit a generally applicable measure but not an individual measure that would apply to a particular company. The provision creates an exception for the EU's General Data

[17] See e.g. ECHR 27.06.2017 – 931/13, Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland [GC].
[18] Weiß University of Birmingham Institute of European Law Working Paper 02–202 (11).
[19] Art. 184 TCA; Natens/Zimmermann 2020, 259.
[20] Footnote 1 to Art. 202 para. 2 TCA.

Protection Regulation[21] and the UK's **Data Protection Act** of 2018 from the TCA commitments entered into, in particular Article 201 TCA. A party's individual measure, which restricts the cross-border flow of data, including personal data, must seek justification in line with the security exceptions (Article 415 TCA) or the general exceptions for legitimate reasons of public interest (Article 412 TCA).

3. The TCA and the EU's General Data Protection Regulation

17 The EU's external trade policy has carefully woven the fundamental rights to the protection of privacy and personal data into its digital trade strategy in order not to compromise the GDPR approach that affords a high level of protection of personal data and in particular regulates the transfers of personal data to third countries.[22] In its 2021 Trade Policy Review, the European Commission underscores that 'the EU will continue to address unjustified obstacles to data flows while preserving its regulatory autonomy in the area of data protection and privacy'.[23] The outcome is based on the aforementioned 2018 '**Horizontal provisions** for cross-border data flows and for personal data protection in EU trade and investment agreements', which are the result of a comprehensive consultation process among all Member States (at a time when the UK was still an EU Member State) and stakeholders representing businesses, consumers and other interested parties, including academics. As a matter of fact, the Digital Trade Title of the TCA marks the first time that these 'Horizontal provisions' have found their way into an EU bilateral trade agreement. The successful inclusion of the EU template in the TCA is important for the EU's external trade strategy and trade negotiations.

18 Following the conclusion of the TCA (→ mn. 23), the EU granted the UK **adequacy status** under the EU's GDPR.[24] The decision adopted by the European Commission provides that the UK affords adequate protection of personal data.[25] The effect of the decision is that the UK is whitelisted to receive personal data from all 27 EU Member States and the countries of the European Economic Area (EEA), i.e. Iceland, Liechtenstein and Norway. The decision applies for a period of four years and will expire on 27 June 2025, unless extended. Keeping its adequacy status vis-à-vis the EU is of paramount economic importance for the UK in order to continue receiving personal data from the EU Member States and the EEA countries after leaving the EU's internal digital market.

19 The legal treatment of EU-UK bound transfers of personal data raises an interesting new twist in the way in which the EU's GDPR interacts with international trade agreements. Until recently, commitments entered into by a third country in the field of international trade law have not been revisited by the European Commission

[21] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 [hereinafter GDPR].

[22] Irion/Yakovleva/Bartl The Institute for Information Law 2016, 1.

[23] European Commission, Trade Policy Review: An Open, Sustainable and Assertive Trade Policy, 18 February 2021, COM(2021) 66 final.

[24] European Commission, Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, 11 October 2021, OJ L 360. See also Choromidou IDPL 2021, 388.

[25] European Commission, Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, 11 October 2021, OJ L 360.

when assessing whether a third country ensures an adequate level of protection that qualifies this third country to receive personal data of EU individuals without further safeguards.[26] There is, however, a growing recognition that, if the UK enters into different commitments on cross-border data flows and personal data protection with trading partners other than the EU, this may compromise relations with the EU.[27] First signs of the eminent recognition can be found during the procedure leading to the adoption of the EU adequacy decision for the UK. In its resolution of 21 May 2021 on the adequate protection of personal data by the UK,[28] the European Parliament was rightly concerned about the potential onward transfer of personal data from EU citizens and residents in the event that the UK will enter into far-reaching commitments on the cross-border flows of data in any future trade agreements. The European Parliament specifically mentioned the UK's request to join the Comprehensive and Progressive Agreement for Transpacific Partnership (CPTPP) and a prospective US-UK trade agreement.[29] In this sense, the European Parliament and the European Data Protection Supervisor (EDPS) call on the European Commission to consider commitments made in international trade agreements when assessing the adequate level of protection of personal data of the UK.[30] This issue will be interesting to follow when the next assessment of the UK's adequacy decision is due, especially considering the repositioning of the UK, not only with its **CPTPP membership** but also the 2022 UK-Singapore Digital Economy Agreement, as discussed below.

4. UK championing international data flows

In 2020, the UK adopted its **post-Brexit National Data Strategy**, which, as one of its missions, endorses '[c]hampioning the international flow of data'.[31] The premise of this mission is to 'remove unnecessary barriers to international data flows'[32] across two interrelated policy areas: (1) in external trade policy, the UK is poised to seek 'ambitious data provisions in our trade negotiations'[33] with third countries and influence data-active trade rules at the level of the WTO; (2) the UK government announced plans to leverage 'an ambitious programme of adequacy assessments'[34] to **20**

[26] Art. 45 GDPR.

[27] Fahey 2020, 12.

[28] European Parliament, Resolution of 21 May 2021 on the adequate protection of personal data by the United Kingdom, 2021/2594(RSP).

[29] European Parliament, Resolution of 21 May 2021 on the adequate protection of personal data by the United Kingdom, 2021/2594(RSP), paras 22–23.

[30] European Parliament, Resolution of 21 May 2021 on the adequate protection of personal data by the United Kingdom, 2021/2594(RSP), para. 24; EDPS, Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom, para. 94, https://edpb.europa.eu/system/files/2021-04/edpb_opinion142021_ukadequacy_gdpr.pdf_en.pdf (last accessed: 30 June 2023).

[31] UK Government, National Data Strategy: Policy Paper, updated 9 December 2020, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy#data-2-5 (last accessed: 30 June 2023).

[32] UK Government, National Data Strategy: Policy Paper, updated 9 December 2020, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy#data-2-5 (last accessed: 30 June 2023).

[33] UK Government, National Data Strategy: Policy Paper, updated 9 December 2020, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy#data-2-5 (last accessed: 30 June 2023).

[34] UK Department of Digital, Culture, Media and Sport, Data: A New Direction – Government Response to Consultation, 17 June 2022, https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation#ch3 (last accessed 30 June 2023).

whitelist third countries under its domestic data protection law.[35] The UK's approach to international data flows which harnesses both international trade law and domestic regulation signpost its ambition to strike international data flow arrangements.[36]

21 For the UK government, digital trade is one of its strategic priorities. New trade agreements that feature ambitious digital trade chapters are a way to compensate for the **UK's exit from the EU** internal digital market by integrating UK businesses into the global digital economy.[37] While the TCA Digital Trade Title is ambitious within reason, the question is how far the UK is prepared to go with trading partners other than the EU. Meanwhile, the UK signed FTAs with Australia and New Zealand that both feature digital trade chapters, including provisions on 'Cross-Border Transfer of Information by Electronic Means'.[38] The provisions contain a commitment not to 'prohibit or restrict the cross-border transfer of information by electronic means, including personal information, if this activity is for the conduct of the business of a covered person'. Both FTAs contain identically worded exceptions for measures inconsistent with aforementioned commitment, which are subject to stricter legal requirements as compared to Article 202 para. 2 TCA. Moreover, the UK is in trade talks with Canada and the US, while its accession to the CPTPP is now completed (→ mn. 39 et seq.).[39] As the UK presses ahead with realising its international data flows ambitions, some caution would be in order: Sands et al. emphasise, for instance, 'the need for a robust, evidence-based approach to digital trade policy that takes into account the perspectives of a wide range of UK stakeholders'.[40]

22 Within its domestic data protection framework, the UK plans to put in place an **'autonomous UK international transfers regime'**[41] by which it recognises third countries' ability to receive personal data from the UK (analogue to the European Commission's adequacy decisions pursuant to the GDPR). The first such recognition was for South Korea,[42] and other countries are expected to follow suit.[43] In order to distinguish them from the EU adequacy decisions, the UK calls them **'data bridges'**. Going even further, in mid-2022 the UK government submitted a new legislative proposal for a Data Protection and Digital Information Bill to the UK Parliament.[44] If adopted this bill will introduce a series of amendments, including a risk-based

[35] UK Department of Digital, Culture, Media and Sport, Guidance: International Data Transfers: Building Trust, Delivering Growth and Firing Up Innovation, 26 August 2021, https://www.gov.uk/government/publications/uk-approach-to-international-data-transfers/international-data-transfers-building-trust-delivering-growth-and-firing-up-innovation (last accessed 30 June 2023).

[36] Choromidou IDPL 2021, 388.

[37] Brakman/Garretsen/Kohl Pap Reg Sci. 2017, 55 (55); UK Department for International Trade, Digital Trade Objectives: Policy Paper, 20 September 2021, https://www.gov.uk/government/publications/digital-trade-objectives-and-vision/digital-trade-objectives (last accessed: 30 June 2023).

[38] UK–Australia FTA, Chapter 14, Art. 14.10; UK–New Zealand FTA, Chapter 15, Art. 15.14.

[39] Jones/Kira/Garrido Alves/Sands BSG-WP 2021, 1 (4).

[40] Jones/Kira/Garrido Alves/Sands BSG-WP 2021, 1 (51 et seq).

[41] UK Department of Digital, Culture, Media and Sport, Data: A New Direction – Government Response to Consultation, 17 June 2022, https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation#ch3 (last accessed: 30 June 2023).

[42] UK, The Data Protection (Adequacy) (Republic of Korea) Regulations 2022, https://www.legislation.gov.uk/uksi/2022/1213/made (last accessed: 30 June 2023).

[43] UK Department of Digital, Culture, Media and Sport, Guidance: International Data transfers: Building Trust, Delivering Growth and Firing Up Innovation, 26 August 2021, https://www.gov.uk/government/publications/uk-approach-to-international-data-transfers/international-data-transfers-building-trust-delivering-growth-and-firing-up-innovation (last accessed: 30 June 2023).

[44] UK Parliament, Data Protection and Digital Information Bill, https://bills.parliament.uk/bills/3322.

approach to the adequacy mechanism for international transfers of personal data.[45] While most of the amendments must be considered modest and the fate of the proposed bill is still unclear, there are concerns about risking the adequacy status with the EU (→ mn. 18).[46]

5. Transitional mechanism

The provisions of Title 3 are supplemented by the **transitional provision** of Article 782 TCA. It includes a so-called 'bridging mechanism' by which the applicability of mandatory data transfer mechanisms intended for third-country data transfers is delayed for up to six months following the entry into force of the Agreement, or until the European Commission adopts an adequacy decision. 'As part of the TCA, which is based on Article 217 TFEU, the mechanism outranks secondary law, such as the GDPR, but must be consistent with primary law, such as the EU Charter of Fundamental Rights'.[47] With the European Commission's decision to adopt the adequate protection of personal data in favour of the UK,[48] the transitional provision has become obsolete again. Nevertheless, the EU has set a precedent whereby the exchange of personal data can, at least temporarily, be made possible with the help of a free trade agreement. **23**

Randnummern ab hier neu durchgezählt, ggf. Verweise anpassen

III. Chapter 3: Specific provisions

Chapter 3 on Specific Provisions assembles miscellaneous issues, which can be grouped under five headings: (1) Enabling cross-border digital service; (2) Facilitation of electronic transactions; (3) Online consumer protection; (4) Open government data; and (5) Regulatory cooperation. In this chapter, the definitions and terms provided for in Article 200 TCA are used in the order of their appearance.[49] **24**

1. Enabling digital services and protecting software source code

The first group of provisions seeks to shield the cross-border provision of digital services from being treated less favorably than other services. Customs duties on electronic transmissions shall not be imposed (Article 203 TCA). Moreover, parties should not require prior authorisation of the provision of a service by electronic means solely on the ground that the service is provided online (Article 204 TCA). These provisions ensure **technological neutrality** and can also be seen as a reaction to ongoing efforts **25**

[45] UK Department of Digital, Culture, Media and Sport, Guidance: International Data transfers: Building Trust, Delivering Growth and Firing Up Innovation, 17 June 2022, https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation#ch3 (last accessed: 30 June 2023).

[46] See e.g. Parliamentary Question E-002789/2022 to the European Commission, Answer by Mr. Reinders on behalf of the European Commission, 6 October 2022, https://www.europarl.europa.eu/doceo/document/E-9-2022-002789-ASW_EN.html (last accessed: 30 June 2023).

[47] Hallak et al. EPRS 2021; see also Irion/Yakovleva/Bartl The Institute for Information Law 2016, 1 (16 et seq.).

[48] European Commission, Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, 11. October 2021, OJ L 360.

[49] I.e. 'consumer', 'direct marketing communication', 'electronic authentication', 'electronic registered delivery service', 'electronic seal', 'electronic signature', 'electronic time stamp', 'electronic trust service', 'government data', 'public telecommunications service' and 'user'.

under the WTO Joint Statement Initiative to make the moratorium on customs duties on electronic transmissions permanent. The EU has a distinct approach in this regard to avoid definitional issues around the coverage of the moratorium by defining electronic transmissions as services.[50]

26 Article 207 TCA on the protection of **source code of software** is a relatively new addition to international trade law that has diffused across newer FTAs, as discussed below. This commitment seeks to protect the source code of software against a Party's measure 'that requires the transfer of, or access to, the source code of software owned by a natural or legal person of the other Party'.[51] The language of the source code commitment in Article 207 TCA shows some evolution in the rule-exception-logic that is more layered and conditioned compared to the EU-Japan Economic Partnership Agreement. The commitment does not prevent discovery by a court in judicial proceedings or investigations by regulatory bodies or administrative tribunals.[52] A Party can justify mandating access to software source code in the context of a **certification procedure** subject to meeting the requirements of the general exceptions and the security exceptions contained in the agreement.[53] This refers, for example, to legally required conformity assessments of products that are placed on the EU internal market.

27 The protection of source codes in digital trade law is intended to avert the risk of a forced technology transfer.[54] However, neither the EU and its Member States nor the UK have so far been implicated with practices that would amount to forced technology transfer. While legal certainty can be an important motivation to inject a commitment on source code of software, there are also risks that the new commitment overreaches its stated objective. In particular, concerns have been voiced that such a commitment restricts the EU's right to regulate in the field of Artificial Intelligence (AI) and its striving to ensure algorithmic accountability of digital services.[55] As digitisation leads to more and more digital artefacts made of software source code, it has been noted that the commitment on software source code could stand in the way of domestic digital policies that promote interoperability, accountability and verifiability of digital technologies and **artificial intelligence**.[56] Furthermore, the relationship with intellectual property rights, such as copyright protection of software source code, and trade secret laws are not well defined; nor is the need for the additional protection fully justified.[57]

2. Facilitation of electronic commerce transactions

28 Facilitating electronic commerce in the cross-border context calls for a certain amount of harmonisation between the Parties to enable **electronic transactions**. Pursuant to Article 205 TCA, each Party shall ensure that contracts may be concluded by electronic means. A range of legal relationships are exempted from this general rule, namely: (a) broadcasting services; (b) gambling services; (c) legal representation services; (d) the services of notaries or equivalent professions involving a direct and

[50] For comparison with other approaches, see Burri/Polanco JIEL 2020, 187 (198 et seqq.).
[51] Art. 207 para. 1 TCA.
[52] Art. 207 para. 3 lit. (a) TCA.
[53] Art. 207 para. 2 lit. (a) TCA.
[54] See Andrenelli/Gourdon/Moïsé OECD Trade Policy Papers 2019.
[55] See Irion FAccT '22: 2022 ACM Conference on Fairness, Accountability, and Transparency 2022, 1561; Irion The Institute for Information Law 2021, 1; Słok-Wódkowska/ Mazur JIEL 2022, 91.
[56] Irion The Institute for Information Law 2021, Słok-Wódkowska/ Mazur JIEL 2022, 91.
[57] Irion The Institute for Information Law 2021, 1 (61).

specific connection with the exercise of public authority; (e) contracts that require witnessing in person; (f) contracts that establish or transfer rights in real estate; (g) contracts requiring by law the involvement of courts, public authorities or professions exercising public authority; (h) contracts of suretyship granted, collateral securities furnished by persons acting for purposes outside their trade, business or profession; or (i) contracts governed by family law or by the law of succession.[58] This can be seen as an extension of the EU's right to regulate and averts demands for legal changes in these distinct areas, which are often not fully harmonised at EU level either.

Pursuant to Article 206 TCA, the parties to an electronic transaction are free to mutually determine the appropriate **electronic authentication** methods for their transaction and the TCA Parties cannot adopt or maintain measures that restrict this freedom.[59] Furthermore, no measures can be adopted that hinder parties to an electronic transmission from proving to judicial and administrative authorities that the use of electronic authentication or an electronic trust service in that transaction complies with the applicable legal requirements.[60] The general obligation contained in paragraph 1 of Article 206 spells out that no Party can deny the legal effect and admissibility as evidence in legal proceedings of an electronic document, an electronic signature, an electronic seal or an electronic time stamp, or of data sent and received using an electronic registered delivery service, solely on the ground that it is in electronic form.[61] Article 200 TCA provides the definitions of terms used in this commitment, which clearly contributes to cutting the red tape in transactional relationships and providing for technological neutrality. **29**

3. Online consumer protection

Provisions on online consumer protection have been common to the last generation of free trade agreements. The EU has had a distinct approach in this regard that does not only promote a narrow understanding of consumer protection but an environment of trust. This recognition of consumer protection interests and the various ways that they can be affected in cross-border electronic commerce has been an important political objective for European consumer protection organisations[62] and is in line with the EU's wish to build consumer trust within EU borders and beyond, also as a way to boost the EU digital economy.[63] Two commitments of the Digital Trade Title seek to protect consumers from **fraudulent and deceptive commercial practices** in electronic commerce as well as from **unsolicited commercial communications**. Article 208 TCA on online consumer trust is framed as a hard obligation that requires Parties to ensure effective protection of consumers engaging in electronic commerce transaction and provides some examples of what such measures may entail – such as requiring compliance with *bona fide* trading practices,[64] heightened transparency, including providing accurate information on the goods or services and the terms of the **30**

[58] Art. 205 para. 2 lit. (a) to (i) TCA.

[59] Art. 206 para. 2, lit. (a).

[60] Art. 206 para. 2, lit. (b). Art. 206 para. 3 permits certain exceptions that may require certification by an accredited authority or compliance with certain performance standards, which must be objective, transparent and non-discriminatory.

[61] Art. 206 para. 1 TCA.

[62] See BEUC, WTO E-Commerce Negotiations BEUC Recommendations, 2019, https://www.beuc.eu/position-papers/wto-e-commerce-negotiations-beuc-recommendations (last accessed: 30 June 2023).

[63] See European Commission, New Consumer Agenda; Strengthening Consumer Resilience for Sustainable Recovery, 13 November 2020, COM(2020) 696 final.

[64] Art. 208 para. 1 lit. (b) TCA.

contract,[65] as well as redress opportunities.[66] Paragraph 3 of Article 208 includes some institutional elements in that the Parties recognise the importance of functioning consumer protection agencies with adequate enforcement powers and the cooperation between these agencies. Article 209 covers unsolicited **direct marketing communications** – such a provision on spam has become common in FTAs as well as in domestic legal frameworks and is unlikely to demand any additional implementation efforts.

4. Open government data

31 Article 210 of the Digital Trade Title includes an aspirational provision on **open government data**. The notion of 'government data' is defined as 'data owned or held by any level of government and by non-governmental bodies in the exercise of powers conferred on them by any level of government'.[67] The TCA does not create a binding commitment to open up government-held data for open access and re-use but seeks to contribute to the **shared understanding of the role of open government data**: 'The Parties to the agreement recognise that facilitating public access to, and use of, government data contributes to stimulating economic and social development, competitiveness, productivity and innovation'.[68] Importantly, the provision also sets out certain modalities that can enable the use of government data – such as that it is machine-readable, with descriptive metadata, and that it is regularly updated.[69] Whether open government data should be the subject matter of international trade law is doubtful but it is in line with the recent development that FTAs increasingly regulate aspects of the data-driven economy.

5. Regulatory cooperation

32 Article 211 of the Digital Trade Title lays down the basis for **regulatory cooperation** between the EU and the UK in relation to digital trade. The Parties agree to exchange information on regulatory issues related to digital trade. Specifically mentioned is the exchange of information related to the recognition and facilitation of interoperable electronic authentication services and electronic trust services, the treatment of direct marketing communications, and consumer protection. In addition, any other matters relevant to the development of digital trade, including new technologies, are covered. Regulatory cooperation does not extend to a Party's rules and safeguards for the protection of personal data and privacy, including cross-border transfers of personal data. The exclusion of data protection law from regulatory cooperation underlines once again the special protection that this regulation enjoys in the EU.

D. Comparative analysis of the TCA with other digital trade chapters

I. Comparing the TCA with other EU FTAs

33 The EU template with regard to digital trade has not been very coherent, especially in comparison to the clear stance taken by the US and other legal entrepreneurs in the field, such as Singapore and New Zealand. The EU template has also developed

[65] Art. 208 para. 1 lit. (c) TCA.
[66] Art. 208 para. 1 lit. (d) TCA.
[67] Art. 200 para. 2 lit. (i) TCA.
[68] Art. 210 para. 1 TCA.
[69] Art. 210 para. 2 lit. (a), (b) and (e) TCA.

and changed over time. This can be explained by the EU's new **emphasis on digital technologies** as part of its innovation and growth strategy and by its new foreign policy orientation subsequent to the Lisbon Treaty, which includes FTAs as an essential strategic element.[70]

34 The agreement with Chile (signed in 2002) was the first to include substantial e-commerce provisions. However, its language was still cautious and limited to soft cooperation pledges in the services chapter[71] and in the fields of information technology, information society and telecommunications.[72] In more recent agreements, such as the EU–South Korea FTA (signed in 2009), the language is much more concrete and binding. It imitates some of the US template provisions and confirms the applicability of the WTO Agreements to measures affecting electronic commerce, as well as subscribes to a permanent duty-free moratorium on electronic transmissions. As it is particularly insistent on data protection policies, the EU has also sought commitment of its FTA partners to comply with the international standards of data protection.[73] Cooperation is also increasingly framed in more concrete terms and includes mutual recognition of electronic signatures certificates, coordination on Internet service providers' liability, online consumer protection, and paperless trading.[74]

35 The 2016 EU agreement with Canada (**CETA**) goes a step further. The CETA provisions concern commitments ensuring (a) clarity, transparency and predictability in their domestic regulatory frameworks; (b) interoperability, innovation and competition in facilitating electronic commerce; as well as (c) facilitating the use of electronic commerce by small and medium sized enterprises.[75] The EU has succeeded in deepening the privacy commitments and the CETA has a specific norm on trust and confidence in electronic commerce, which obliges the Parties to adopt or maintain laws, regulations or administrative measures for the protection of personal information of users engaged in electronic commerce in consideration of international data protection standards.[76] Yet, there are no deep commitments on digital trade; nor are there any rules on data and data flows.

36 Overall, the EU has been cautious with regard to digital trade commitments in general and has not gone substantially beyond the GATS-level of liberalisation for a long period of time. Further, the EU has been particularly careful with regards to inserting rules on data flows in its FTAs. It is only relatively recently that the EU made a step towards such rules, whereby Parties have agreed to consider in future negotiations commitments related to cross-border flow of information. Such a clause is found in the 2018 EU-Japan EPA[77] and in the 2018 modernisation of the trade part of the EU-Mexico Global Agreement.[78] In the latter two agreements, the Parties commit to 'reassess' within three years of the entry into force of the agreement, the need for inclusion of provisions on the free flow of data into the treaty.

37 This signaled a repositioning of the EU on the issue of **data flows**, which is now fully endorsed in the EU's currently negotiated deals with Australia and Tunisia, and

[70] Kleimann European University Institute 2013.

[71] Art. 102 EU–Chile FTA. The agreement states that '[t]he inclusion of this provision in this Chapter is made without prejudice of the Chilean position on the question of whether or not electronic commerce should be considered as a supply of services'.

[72] Art. 37 EU–Chile FTA.

[73] Art. 7.48 EU–South Korea FTA.

[74] Art. 7.49 EU-South Korea FTA.

[75] Art. 16.5 CETA.

[76] Art. 16.4 CETA.

[77] Art. 8.81 EU-Japan EPA.

[78] Art. 12 EU-Mexico FTA (text adopted in principle).

the 2022 agreement with New Zealand, which include in their digital trade chapters norms on the free flow of data and data localisation bans. This repositioning and newer commitments are, however, also linked to high levels of data protection.[79]

38 As indicated from the discussion of the TCA's Digital Trade Title, the EU wishes to permit data flows only if coupled with the high data protection standards of the GDPR. In its most recent trade deals, as well as in the EU proposal for WTO rules on electronic commerce,[80] the EU follows a distinct model of endorsing and protecting privacy as a fundamental right. On the one hand, the EU and its partners seek to **ban data localisation measures** and thus subscribe to a free data flow. On the other hand, however, these commitments are conditioned. First, by a dedicated article on data protection, which clearly states that: 'Each Party recognises that the protection of personal data and privacy is a *fundamental right* and that high standards in this regard contribute to trust in the digital economy and to the development of trade'.[81] This is followed by a paragraph on data sovereignty: 'Each Party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data. Nothing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards'.[82] The EU also wishes to retain the right to see how the implementation of the FTA with regard to data flows impacts the conditions of privacy protection, so there is a review possibility within three years of the entry into force of the agreement and parties remain free to propose to review the list of restrictions at any time.[83] In addition, there is a broad carve-out under the right to regulate.[84] The EU thus reserves ample **regulatory leeway** for its current and future data protection measures. The exception fundamentally differs from the objective necessity test under the CPTPP and the USMCA, as discussed below, or the respective provisions under WTO law, because it is subjective and safeguards the EU's right to regulate.[85]

39 The TCA does confirm the new EU approach with regard to cross-border data flows and data protection, albeit with some textual differences. It is also evident that the EU digital trade template has substantially expanded to include rules on online consumer trust, source code and open government data. Yet, it should be noted that the EU also appears likely to tailor its template depending on the trade partner – for instance, the currently negotiated deal with Indonesia includes merely a place-holder for rules on data flows. The agreement with Vietnam, which entered into force on 1 August 2020, has only few cooperation provisions on electronic commerce as part of the services chapter and no reference to either data or privacy protection is made.

---

[79] See European Commission, Horizontal Provisions for Cross-border Data Flows and for Personal Data Protection, News release of 18 May 2018, https://ec.europa.eu/newsroom/just/items/627665 (last accessed: 30 June 2023); see also Yakovleva/Irion IDPL 2020, 201.

[80] WTO, Joint Statement on Electronic Commerce, EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce, Communication from the European Union, 26 April 2019, INF/ECOM/22.

[81] See e.g. Art. 6 para. 1 draft EU-Australia FTA (emphasis added). The same wording is found in the EU-New Zealand and the draft EU-Tunisia FTA.

[82] See e.g. Art. 6 para. 2 draft EU-Australia FTA. The same wording is found in the EU-New Zealand and draft the EU-Tunisia FTA.

[83] See e.g. Art. 5 para. 2 draft EU-Australia FTA. The same wording is found in the draft EU-New Zealand and the EU-Tunisia FTAs.

[84] See e.g. Art. 2 draft EU-Australia FTA. The same wording is found in the draft EU-New Zealand and the EU-Tunisia FTAs.

[85] Yakovleva U. Mia L. Rev. 2020, 416 (496).

II. Comparing TCA with other digital trade templates

While it is only with the TCA and the 2022 EU-New Zealand FTA that the EU has adopted agreements with important substantive provisions on digital trade and data flows in particular, much has happened in other FTAs. The TCA Digital Trade Title does, in this sense, imitate some of these other agreements' rules and is not to be taken as innovative. **40**

The US has been an important legal entrepreneur since the 2001 **'Digital Agenda'** endorsed by the US Congress.[86] The US agreements reached since then with Australia, Bahrain, Chile, Morocco, Oman, Peru, Singapore, the Central American countries, Panama, Colombia, South Korea, and the updated NAFTA, all contain critical WTO-plus and WTO-extra provisions in the broader field of digital trade. Importantly, the diffusion of the US template is not limited to US agreements but can be found in other FTAs as well, such as Singapore–Australia, Thailand–Australia, New Zealand–Singapore, Japan–Singapore, and South Korea–Singapore. Many developing countries, such as Chile, have become active in the area of data governance. Even China, as a typically protective economy, has adopted, albeit with notable differences, some elements of the US template as part of the recent Regional Comprehensive Economic Partnership (**RCEP**).[87] The next sections compare the TCA's Digital Trade Title with some discrete and far-reaching templates developed in the recent years – in particular those of the CPTPP, the USMCA and the Digital Economy Partnership Agreement. **41**

1. The Comprehensive and Progressive Agreement for Trans-Pacific Partnership

The 2018 Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) was agreed between eleven countries in the Pacific Rim.[88] At the time, the CPTPP chapter on e-commerce created the most comprehensive template in the landscape of FTAs and included a number of new features. Despite the fact that the US withdrew from the agreement at the start of the Trump administration, the chapter still reflects the US efforts to secure obligations on digital trade and is a verbatim reiteration of the Transpacific Partnership Agreement (TPP) chapter. **42**

Similarly to the TCA Digital Trade Title, the scope of the CPTPP e-commerce chapter clarifies that it applies 'to measures adopted or maintained by a Party that affect trade by electronic means'.[89] Audiovisual services are not excluded but government procurement is.[90] There are also a number of similarities in that the CPTPP addresses some of the leftovers of the WTO E-Commerce Programme and seeks to facilitate online commerce. In this sense, Article 14.3 CPTPP bans the imposition of customs duties on electronic transmissions, including content transmitted electronically, and Article 14.4 endorses the non-discriminatory treatment of digital products,[91] which are defined broadly pursuant to Article 14.1. Here the CPTTP Parties' obliga- **43**

[86] US Congress, Bipartisan Trade Promotion Authority Act of 2001, H. R. 3005, 3 October 2001; see also Gao Leg. Issues Econ. Integr. 2018, 47.

[87] See Burri Leg. Issues Econ. Integr. 2022, 149.

[88] Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Vietnam.

[89] Art. 14.2 para. 2 CPTPP.

[90] Art. 14.2 para. 3 CPTPP.

[91] The obligation does not apply to subsidies or grants, including government-supported loans, guarantees and insurance, nor to broadcasting. It can also be limited through the rights and obligations specified in the IP chapter. See Art. 14.2 para. 3 CPTPP.

tions go beyond the TCA and the EU's stance of defining electronic transmissions as services. Article 14.5 CPTPP is meant to shape the domestic electronic transactions framework by including binding obligations for the Parties to follow the principles of the UNCITRAL Model Law on Electronic Commerce 1996 or the UN Convention on the Use of Electronic Communications in International Contracts. Parties must endeavor 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.[92] The provisions on paperless trading and electronic authentication and electronic signatures complement this by securing the equivalence of electronic and physical forms.[93] Paperless trading is also included[94] – a provision that is oddly missing from the TCA.

44 The remainder of the provisions found in the CPTPP e-commerce chapter tackle the emergent issues of the data economy. Most importantly, the CPTPP explicitly seeks to restrict the use of data localisation measures. Article 14.13(2) prohibits the parties from requiring a 'covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory'.[95] There is also a hard rule on free data flows in that: '[e]ach 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'.[96] The rule clearly has a broad scope and most data transferred over the Internet is likely to be covered, although the word 'for' may suggest the need for some causality between the flow of data and the business of the covered person. The explicit reference to personal data is also noteworthy. In comparison to the TCA, this is also a self-standing obligation that is not coupled with the prohibition of certain data flow restrictions, as discussed above under Article 201 TCA.

45 Under the CPTPP, measures restricting digital flows or implementing localisation requirements are permitted only if they do not amount to 'arbitrary or unjustifiable discrimination or a disguised restriction on trade' and do not 'impose restrictions on transfers of information greater than are required to achieve the objective'.[97] These non-discriminatory conditions are similar to the test formulated under Article XIV GATS and Article XX GATT 1994 – a test that is aimed at balancing trade and non-trade interests by 'excusing' certain violations (but is also extremely hard to pass, as known from existing WTO jurisprudence).[98] The CPTPP test differs from the WTO norms in one significant element: while there is a list of public policy objectives in GATT and GATS, the CPTPP provides no such enumeration and speaks merely of a 'legitimate public policy objective'.[99] This permits some regulatory autonomy for the CPTPP signatories but it differs decisively from the explicitly formulated safeguards provided by the TCA.

[92] Art. 14.5 para. 2 CPTPP.
[93] Art. 14.6 CPTPP.
[94] Art. 14.9 CPTPP.
[95] The ban on localisation measures is softened with regard to financial services and does not apply to government procurement.
[96] Art. 14.11 para. 2 CPTPP (emphasis added).
[97] Art. 14.11 para. 3 CPTPP.
[98] See e.g. Andersen JIEL 2015, 383.
[99] Art. 14.11 para. 3 CPTPP.

For the first time, the CPTPP addressed in FTAs **software source code**.[100] Its relevant provision, albeit with different exceptions,[101] is now replicated in the TCA. The rule, largely inserted under pressure from the US IT industry, aims to protect software companies and address their concerns about loss of intellectual property, in particular trade secrets protection, or cracks in the security of their proprietary code. Furthermore, it may also be interpreted as a reaction to China's demands to access to source code from software producers selling in its market.[102] As earlier noted, its utility for the TCA Parties can be questioned and the included in the TCA flexibilities should be welcome. **46**

Apart from these similarities between the TCA and the CPTPP digital trade rules, there are important differences. The most **striking divergence** is in the area of privacy and data protection. Paragraph 2 of Article 14.8 requires every CPTPP Party to 'adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce'. Yet, there are no standards or benchmarks for the legal framework specified, except for a general requirement that CPTPP Parties 'take into account principles or guidelines of relevant international bodies'.[103] A footnote provides some clarification in saying that: '… a Party may comply with the obligation […] by adopting or maintaining measures such as a 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'.[104] Parties are also invited to promote compatibility between their data protection regimes, by essentially treating lower standards as equivalent.[105] The goal of these norms can be interpreted as a prioritisation of trade over privacy rights. This has been pushed by the US during the TPP negotiations, as the US subscribes to a relatively weak and patchy protection of privacy.[106] Timewise, this push came also at the phase when the US was wary that it could lose the privilege of transatlantic data transfers, as a consequence of the judgment of the Court of Justice of European Union (CJEU) that struck down the EU–US Safe Harbor Agreement.[107] In hindsight this had been a legitimate concern considering the follow-up decision of *Schrems II*[108] and the ongoing difficulties to reach a lasting **transatlantic data privacy framework**, even under the Biden administration. The differences between the TCA and CPTPP on data protection become also critical as the UK advances its accession to the CPTPP. When this happens, the UK's commitments under the CPTPP may undermine the pledges made under the TCA. **47**

[100] Art. 14.17 CPTPP.

[101] The prohibition applies only to mass-market software or products containing such software. This means that tailor-made products are excluded, as well as software used for critical infrastructure and those in commercially negotiated contracts.

[102] See e.g. USTR, Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974, 22 March 2018; Gibson Berkley Tech. L. J. 2007, 1403.

[103] Art. 14.8 para. 2 CPTPP.

[104] Art. 14.8 para. 2 CPTPP, at footnote 6.

[105] Art. 14.8 para. 5 CPTPP.

[106] See e.g. Burri Case W. Res. J. Int'l L. 2021, 35.

[107] CJEU 6.10.2015 – Case C-362/14, ECLI:EU:C:2015:650, Maximillian Schrems v Data Protection Commissioner (Schrems I).

[108] The later EU-US Privacy Shield arrangement, which replaced the Safe Harbor, was also rendered invalid by a follow-up judgment: CJEU 16.7.2020 – Case C-311/18, ECLI:EU:C:2020:559, Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (Shrems II).

48 Next to the data protection norms, the CPTPP also includes provisions on consumer protection[109] and spam control.[110] These are, however, fairly weak. The same is true for the rules on cybersecurity[111] as well as for the rules on net neutrality.[112] The last two provisions are missing from the TCA, while rules on open Internet access can be found in some EU deals, such as the modernised agreement with Mexico.[113]

2. The United States-Mexico-Canada Agreement and the United States-Japan Digital Trade Agreement

49 After the US withdrawal from the TPP, there was some uncertainty as to the direction the US will follow in its trade deals in general and on matters of digital trade in particular. The renegotiated NAFTA, which is now referred to as the 'United States-Mexico-Canada Agreement' (**USMCA**), cast the doubts aside. The USMCA has a comprehensive 'Digital Trade' chapter, which follows all critical lines of the CPTPP and even goes beyond it.

50 Beyond the similarities with the CPTPP, the USMCA introduces some novelties. Important to note when comparing it with the TCA is that while the USMCA Parties still give priority to trade over privacy protection, they also pledge to take into account principles and guidelines of relevant international bodies. Mentioned are in particular the **APEC Privacy Framework** and the 2013 OECD Recommendation of the Council concerning Guidelines governing the **Protection of Privacy and Transborder Flows of Personal Data**.[114] The Parties also recognise key principles of data protection, which include: limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability,[115] and aim to provide remedies for any violations.[116] This is interesting because it may go beyond what the US may have in its national laws on data protection and also because it reflects some of the principles the EU has advocated for in the domain of personal data protection.

51 Three further novel provisions of the USMCA may be mentioned. The first one, now also included in the TCA, regards **open government data**.[117] The second refers to the inclusion of '**algorithms**' as part of the ban on requirements for the transfer or access to source code in Article 19.16, which extends its scope of application. The third novum refers to '**interactive computer services'** and the pledge of the Parties to insulate them from liability,[118] which reflects the US domestic approach towards platform regulation under Section 230 of the Communications Decency Act. This may potentially clash with the intermediaries' liability regime of the EU, as well as efforts to regulate platforms in light of negative phenomena in free speech online, such as fake news, hate speech and other instances of illegal content.[119]

52 The US stance towards digital trade issues has also been confirmed by the **US-Japan Digital Trade Agreement** (DTA), signed on 7 October 2019, alongside the US-Japan Trade Agreement. The US-Japan DTA can be said to replicate almost all

[109] Art. 14.17 CPTPP.
[110] Art. 14.14 CPTPP.
[111] Art. 14.16 CPTPP.
[112] Art. 14.10 CPTPP.
[113] Art. 10 EU-Mexico FTA.
[114] Art. 19.8 para. 2 USMCA.
[115] Art. 19.8 para. 3 USMCA.
[116] Art. 19.8 paras 4 and 5 USMCA.
[117] Art. 19.8 USMCA.
[118] Art. 19.17 para. 2 USMCA.
[119] See e.g. Burri (2022), 31.

provisions of the USMCA and the CPTPP, including the new USMCA rules on open government data,[120] source code[121] and interactive computer services.[122] Notably, the DTA covers also financial and insurance services as part of its scope of application, thereby rendering its impact much broader. The US-Japan DTA can also be said to be the first of the new generation of dedicated Digital Economy Agreements (DEAs) that tackle diverse issues of the data-driven economy and seek enhanced cooperation – a trend that the UK has also joined with the 2022 UK-Singapore DEA.

3. The Digital Economy Partnership Agreement

The 2020 Digital Economy Partnership Agreement (**DEPA**) between Chile, New Zealand and Singapore, which are all also parties to the CPTPP, is not purely conceptualised as a trade agreement. Instead, it is also meant to address broader issues of the digital economy. In this sense, its scope is wide, open and flexible, and covers several emerging issues. The agreement is also not a closed deal but one that is open to other countries.[123] The DEPA follows a unique **modular approach**, which next to common topics of digital trade, albeit with deeper commitments, addresses new areas, such as the creation a wider trust environment (Module 5); digital Identities (Module 7) and digital inclusion (Module 11); emerging trends and technologies (Module 8); and innovation and the digital economy (Module 9). **53**

The DEPA is overall a future-oriented agreement with much stronger demands on cooperation between the Parties – such as, for instance, on ethical and governance frameworks that support the trusted, safe and responsible use of AI technologies.[124] Such a forward-looking approach with closer cooperation initiatives in the area of the data-driven economy is completely missing from the TCA and other EU trade agreements, while the UK actively follows this path. **54**

E. Conclusion

The Digital Trade Title forms an important part of the TCA and confirms the EU approach for comprehensive rules on digital trade and for a careful calibration of the interplay between free cross-border data flows and personal data protection. In the former sense, the Digital Trade Title is substantially different from previous EU FTAs, whereas not necessarily very innovative, when compared with other FTAs and dedicated digital trade agreements, such as the DEPA. With regard to data protection, the EU has ensured sufficient safeguards for the protection of EU citizens' data and the UK is thus also bound to these high standards. This may be problematic for the UK, as it endorses its global strategy and seeks to enter into agreements with the CPTPP Parties and the US, which are more liberal in nature and clearly do not provide levels of data protection that are essentially equivalent to those of the EU. The TCA Digital Trade Title may in this sense trigger new dynamics when interfacing these different regimes, which may also prompt reactions from the EU, as contestation and geopolitical repositioning in the domain of digital trade rulemaking continue.[125] **55**

[120] Art. 20 US-Japan DTA.
[121] Art. 17 US-Japan DTA.
[122] Art. 18 US-Japan DTA.
[123] Art. 16.2 DEPA.
[124] Art. 8.2 paras 2 and 3 DEPA.
[125] See e.g. Burri JIEL 2023, 90.