Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities'

Yakovleva, S.

DOI
10.1163/22119000-12340189

Publication date
2020

Document Version
Final published version

Published in
The Journal of World Investment & Trade

BRILL
NIJHOFF

JOURNAL OF WORLD INVESTMENT &
TRADE 21 (2020) 881–919

The Journal of
World
Investment & Trade
Law • Economics • Politics
brill.com/jwit

Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities'

Svetlana Yakovleva
Faculty of Law, University of Amsterdam, Amsterdam, The Netherlands
mail@svyakovleva.com

Abstract

Cross-border flows of personal data have become essential for international trade. European Union (EU) law restricts transfers of personal data to a degree that is arguably beyond what is permitted under the EU's World Trade Organization commitments. These restrictions may be justified under trade law's 'necessity test.' The article suggests that they may not pass this test. Yet, from an EU law perspective, the right to the protection of personal data is a fundamental right. An international transfer of personal data constitutes a derogation from this right and, therefore, must be consistent with another necessity test, the 'strict necessity' test of the derogation clause of the EU Charter of Fundamental Rights. This article shows how a simultaneous application of the trade law and EU Charter 'necessities' to EU restrictions on transfers of personal data creates a catch-22 situation and sketches the ways out of this compliance deadlock.

* Svetlana Yakovleva is a PhD Researcher at the Institute for Information Law (IViR), University of Amsterdam and Senior Legal Adviser at De Brauw Blackstone Westbroek, Amsterdam. She received a degree in law (cum laude) from the National Research University Higher School of Economics (Moscow) in 2005. She also holds an LLM degree in Law and Economics (EMLE) from the Erasmus University, Rotterdam and the University of Hamburg (2007), and a research master degree in Information Law from the Institute for Information Law (IViR), University of Amsterdam (2016). Svetlana's primary research interests lie at the intersection of data privacy and cybersecurity law, human rights and international trade law. Her research has been published in several well-known journals, such as Common Market Law Review, World Trade Review and University of Miami Law Review. Between 2007 and 2014, she worked as a consultant for private enterprises and as legal advisor for the e-Government project of the Russian Government.

Keywords

EU Charter of Fundamental Rights – digital trade – 'necessity test' – personal data protection – World Trade Organization law

1 Introduction

The commercial use of personal data empowers digital trade and contributes to economic growth. It may also generate individual benefits. However, those benefits often seem both remote and indirect when compared to the risks posed to individuals by the (mis)use of their data, such as identity theft, access to data by foreign surveillance and law enforcement authorities, unwanted marketing communications, discrimination, and denied access to essential services, to name just a few. Unlike data, which can simultaneously be present in multiple locations and fall under the jurisdiction of multiple legal regimes, individuals retain a close connection with a particular State through the institutions of citizenship or residency. It is first and foremost that State that must guarantee the individuals' human rights and protect them from actions of other States. Simply put, while trade in data is international, protection of individual rights is local.

While international trade law aims to liberalize data flows to facilitate digital cross-border trade, European Union (EU) data protection law restricts transfers of personal data outside the European Economic Area (EEA). Grounded in the fundamental rights to the protection of personal data under Article 8 of the EU Charter of Fundamental Rights (EU Charter),[1] the rules for transfers of personal data outside the EEA aim to ensure that the level of protection guaranteed in the EU by the General Data Protection Regulation (GDPR)[2] is not undermined as personal data leaves the EEA.[3] As a result, these two bodies of law are in tension and have opposite normative valences. EU law can tolerate cross-border flows of personal data only to the extent that these are compliant with the EU Charter and domestic rules for such flows. In turn, international

1 Charter of Fundamental Rights of the European Union (ratified 7 December 2000) (EU Charter); CJEU, Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650 (*Schrems I*), paras 72–73; CJEU, Opinion 1/15 – EU-Canada Passenger Name Record Agreement, ECLI:EU:C:2017:592, para 214.

2 EU Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (27 April 2016) Regulation (EU) 2016/679 (GDPR) and Repealing Directive 95/46/EC (repealed 24 May 2018) OJ L 119/1.

3 GDPR (n 2) art 44; *Schrems I* (n 1) para 72. See also Gloria González Fuster, 'Un-Mapping Personal Data Transfers' (2016) 2(2) European Data Protection Law Review 160, 168.

trade law can tolerate EU's restrictions on personal data transfers only to the extent such restrictions are compliant with the EU's international trade liberalization commitments including allowable exceptions thereto.

Personal data has become an integral part of digital services and in particular targeted advertising, which requires a constant flow of personal data. Therefore, the risk that EU's international trade law commitments to liberalize the cross-border movement of services, on the one hand, and the protection of the right to the protection of personal data as a fundamental right, of which restrictions on personal data transfers is a constitutional pillar, on the other, will clash is very real. The recent ruling of the Court of Justice of the European Union (CJEU) in the so-called *Schrems II* case,[4] which arguably could *de facto* lead to data localization, puts additional pressure on the EU's domestic policy approach to cross-border data flows from an international trade perspective.[5] This ruling invalidated the EU–US Privacy Shield framework (widely used for transfers of personal data from the EEA to the United States) and clarified that companies may only use Standard Contractual Clauses (SCCs) (the most common mechanism for personal data transfers to any country outside the EEA) if their application can, in practice, ensure the level of data protection – also in the context of national security – 'essentially equivalent' to that in the EU. This requires companies to conduct a comprehensive case-by-case assessment of foreign legal frameworks and policy and take 'supplementary measures' to compensate for the deficiencies of the latter as compared to that of the EU.

A clash between the EU's constitutional protection for personal data (as translated into a framework for cross-border transfers of personal data in the GDPR) and the EU's trade liberalization commitments is not in and of itself a reason to cry foul because both the EU Charter and international trade law contain exceptions that allow each system to tolerate encroachments on their respective rules by the other, within certain limits. As long as the exceptions in both systems are aligned, they can limit the degree of tension between the two systems.

Most international trade agreements provide for a so-called 'general exception' modelled after the one contained in Article XIV of the General

4 CJEU, C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems,* ECLI:EU:C:2020:559 (*Schrems II*).

5 See Kenneth Propp and Peter Swire, 'Geopolitical Implications of the European Court's *Schrems II* Decision' (*Lawfare Blog*, 17 July 2020) <www.lawfareblog.com/geopolitical-implications-european-courts-schrems-ii-decision>; Theodore Christakis, 'After *Schrems II*: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe' (*European Law Blog*, 21 July 2020) <https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/> both accessed 27 July 2020.

Agreement on Trade and Services (GATS).[6] This exception grants parties to an international trade agreement regulatory autonomy to adopt and maintain measures 'necessary' to protect the privacy of individuals in relation to the processing and dissemination of personal data, even if such measures run afoul of the country's international trade commitments (the 'trade "necessity test"'). Article 52(2) of the EU Charter, in turn, allows the EU to limit fundamental rights if this is 'necessary' to meet objectives of general interest of the EU or to protect the rights and freedoms of others (the 'EU Charter "necessity test"'). As interpreted by the CJEU, this provision allows EU bodies to conclude an international agreement, which involves transfers of personal data outside the EEA, if the conditions laid out in this clause, most importantly, the 'necessity test' are fulfilled.[7]

This article argues that, when applied to the fundamental right to the protection of personal data enshrined in Article 8 of the EU Charter, on the one hand, and the obligation to liberalize international trade, on the other hand, the general exception for privacy and data protection in Article XIV GATS (as applied by the WTO adjudicating bodies) and the derogation clause of Article 52(1) of the EU Charter (as interpreted by the CJEU after 2009) can be incompatible. In 2018, the EU proposed model clauses on cross-border data flows for digital trade chapters (discussed in more detail in Section 2.4 below),[8] which include a specific exception for privacy and data protection, modelled after the national security of Article XIV *bis* of the GATS – and much broader than the general exception. Among other things, the proposed exception explicitly states that measures for protection of personal data and privacy allowed under the exception, include rules for the transfers of personal data. The EU has included these model clauses in its proposals for digital trade chapters in the currently negotiated trade agreements with Australia, Indonesia, New Zealand, Tunisia and the UK (following Brexit)[9] as well as into the EU proposal for the WTO rules on electronic

6 Marrakesh Agreement Establishing the World Trade Organization (WTO) (signed 15 April 1994, entered into force 1 January 1995) Annex 1B.

7 Opinion 1/15 (n 1) paras 67, 70.

8 Horizontal Provisions for Cross-Border Data Flows and for Personal Data Protection (in EU Trade and Investment Agreements) <http://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf> accessed 22 May 2020; see also Susan A Aaronson and Patrick Leblond, 'Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO' (2018) 21(2) JIEL 262; Brett Fortnam, 'EU Punts on Data Flow Language in Japan Deal, Leaving Position Unresolved' (*Inside US Trade*, 2017) 35–27 <https://insidetrade.com/inside-us-trade/eu-punts-data-flow-language-japan-deal-leaving-position-unresolved> accessed 19 August 2020.

9 EU Proposal for the Digital Trade Chapter of EU–New Zealand FTA (25 September 2018) <http://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157581.pdf>; European

commerce,[10] which are intended to co-exist with the general exception for privacy and data protection modelled after Article XIV(c)(ii) GATS included in the same agreement.[11] The proposed digital trade chapters clarify, or contain a placeholder for such a provision, that the general exception, security exception and prudential carve out also apply to the digital trade chapter.[12]

The focus of this article is, nevertheless, on the existing general exception – and not on the exception for privacy and data protection proposed for digital trade chapters – for a number of reasons. First, because of the breadth of the exception in model clauses, challenging the EU restrictions on personal data transfers under the specific clause on cross-border data flows is more difficult for the EU's trading partners than under existing trade in services provisions. One could argue that the proposed clauses constitute *lex specialis* in relation to the general exception in the same agreement. However, given the two exceptions exempt exactly the same public policy interests, such approach would render the general exception for data protection redundant and, therefore could be contrary to the 'general rule of interpretation', which does not allow an interpreter to 'adopt a reading that would result in reducing whole

Commission, 'Draft Text of the Agreement on the New Partnership with the United Kingdom' (18 March 2020) <https://ec.europa.eu/info/sites/info/files/200318-draft-agreement-gen.pdf>; EU Proposal for the Digital Trade Chapter of EU–Australia FTA (10 October 2018) <http://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157570.pdf>; EU Proposal for the Digital Trade Chapter of EU–Tunisia (9 November 2018) <https://trade.ec.europa.eu/doclib/docs/2019/january/tradoc_157660.%20ALECA%202019%20-%20texte%20commerce%20numerique.pdf>; European Commission, 'Report of the 5th Round of Negotiations for a Free Trade Agreement Between the European Union and Indonesia' (9–13 July 2018) <http://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157137.pdf>; EU Proposal for Digital Trade Chapter for a Modernised EU–Chile Association Agreement (released on 5 February 2018) <https://trade.ec.europa.eu/doclib/docs/2018/february/tradoc_156582.pdf> all accessed 22 May 2020. The latter proposal only contains a placeholder for provisions on data flows.

10 EU proposal for WTO Disciplines and Commitments Relating to Electronic Commerce (EU Communication, 26 April 2019) INF/ECOM/22 <http://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf> accessed 22 May 2020.

11 See eg EU Proposal for Chapter X 'Exceptions' of the EU–New Zealand FTA (25 June 2019) art X.1(2) <https://trade.ec.europa.eu/doclib/docs/2019/july/tradoc_158278.pdf> accessed 22 May 2020. This provision includes a general exception for privacy and data protection modelled after the general exception in the General Agreement on Trade in Services (1 January 1995) (GATS) art XIV(c)(ii); EU proposals for an exceptions chapter for other FTAs discussed in this article are not available as of the time of writing.

12 See EU Proposal EU–Australia FTA (n 9) art 3; EU Proposal EU–New Zealand FTA (n 9) art 3; EU Proposal EU–Tunisia FTA (n 9) art 3.

clauses or paragraphs of a treaty to redundancy or inutility.'[13] This means that the applicability of the specific exception could be limited by the scope of the digital trade chapter. Hence, the EU protection framework for personal data could be challenged by the EU's trading partners, both in exiting agreements (notably the GATS) and in bilateral agreements, even if those would contain the specific exception clause, under the services chapter and would still have to be justified under the general exception. Second, it is unclear whether the EU's proposal will be adopted in any future trade agreement, and, third, even if it would – there will remain multiple agreements, to which the EU is a party, containing just a general exception for data protection.

The article develops the argument that the EU restrictions on transfers of personal data are potentially in conflict with the EU's non-discrimination commitments under the GATS and post-GATS trade agreements. It contends that such restrictions are unlikely to meet the trade 'necessity test' even in its most lenient interpretation because they arguably go beyond the limits set by the GATS provisions and the general exception. An important contribution of the article to this debate is that the requirement of free cross-border flow of (personal) data that can be deduced from the EU's existing trade liberalization commitments in the context of digitally provided services is not only inconsistent with the GDPR, but is also unlikely to be justified under Article 52(1) of the Charter as a necessary and proportionate derogation from the fundamental right to the protection of personal data. This analysis exposes EU's constitutional constraints on implementing such requirement for cross-border flow of personal data into the GDPR, which may lead to a catch-22 compliance deadlock for the EU. The article then argues that adjustments of both international trade and EU data protection rules are necessary to overcome this deadlock.

The article proceeds as follows. Section 2 explains why domestic regulation on personal data protection is increasingly relevant in the context of international obligations to liberalize trade in services. It also puts the discussion in the context of recent developments in the EU legal system and international trade law. Section 3 juxtaposes the interpretation of the trade 'necessity test' and the 'EU Charter necessity' and explains why there is a risk of a catch-22 type of compliance deadlock for the EU when the two 'necessity tests' are applied simultaneously. Section 4 outlines ways out of the potential deadlock. Section 5 concludes.

13 WTO, *United States – Standards for Reformulated and Conventional Gasoline*, Report of the Appellate Body (20 May 1996) WT/DS2/AB/R, 23.

2 EU Data Protection and International Trade Law

2.1 *The Role of (Personal) Data Flows in International Trade*

Cross-border trade in digital goods and services is increasingly dependent on personal data and its flows across borders. Globalization and the decentralization of production and distribution value chains have made the cross-border movement of information – commercial, machine-generated and personal – crucial for the production and provision of services, both online and offline[14] as well as the day-to-day management of companies. Projecting this economic reality, promising unprecedented efficiency gains, economic development and growth, on the world's legal landscape divided into multiple compartments shaped by national legal systems, is a sobering exercise. When set against the unidimensional economic benefits driving globalization, domestic legal systems must consider how these benefits fit into a broader set of national and regional priorities, such as national security, fundamental rights protection, industrial policy, and reflecting cultural values, to name just a few. Differences in the relative weight accorded each of priorities vis-à-vis the economic and political gains from cross-border data flows have resulted in a diversity of domestic rules governing the cross-border flows of information, especially when it relates to identified or identifiable individuals (that is, the definition of personal data in the GDPR). As a result, facing the challenges of compliance with several data protection regimes and rules for cross-border transfers of personal data in several countries has become a reality for companies doing business globally.

Perceiving domestic restrictions on cross-border flows of personal data as barriers to reaping the benefits of global digital trade,[15] an increasing volume of literature, discussed in Section 2.3 below, highlights the risk of their inconsistency with the rules of the WTO; indeed, as Section 2.4 shows, the elimination of such restrictions has become one of the contentious issues of most recent trade negotiations in North America, Europe and Asia.

14 Natali Helberger, Frederik Zuiderveen Borgesius and Augustin Reyna, 'The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law' (2017) 54(5) CML Rev 1427, 1430–31.

15 For a discussion on how data protection is being framed as digital trade barrier in digital trade discourse, see Svetlana Yakovleva, 'Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy' (2020) 74 U Miami L Rev 416, 473–82.

2.2 *The EU Regime for Transfers of Personal Data Outside the EEA*

Just as personal data has both economic and societal value, the European data protection regime, first introduced by the 1995 Data Protection Directive,[16] has a dual objective: protecting the fundamental rights and freedoms of individuals, in particular their right to the protection of personal data, and ensuring the free flow of personal data within the EEA.[17] Conflicting at first glance,[18] these objectives are easier to reconcile if seen as cause and effect, or as the 'why' and the 'how': The harmonization of data protection rules was a prerequisite for the free flow of personal data without undermining the individuals' rights to protection of such data originating from EU Member States affording a higher level of protection (the 'why').[19] The fundamental rights approach – 'the how' – sets the level of protection of personal data, which the EU-wide personal data protection framework should attain.

Since 2009 (when the EU Charter took effect), the right to the protection of personal data is a binding fundamental right in the EU (Article 8 of the Charter), separate from the fundamental right to privacy (Article 7 of the EU Charter). The constitutionalization of the EU has put the economic needs that necessitated the creation of the EU-wide data protection framework in the first place to the background and emphasized the non-economic goals of the current European data protection law.[20]

When it comes to transfers of personal data outside of the EEA, the EU's framework is one of the most restrictive in place in any democratic jurisdiction. For the purposes of cross-border transfer of personal data, the GDPR divides countries in two groups: those that have been afforded a so-called 'adequacy decision' by the European Commission, stating that they ensure an adequate level of personal data protection (currently 12 countries[21] including

16 EU Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Directive 95/46/EC (24 October 1995) OJ L281/31 (Data Protection Directive).

17 GDPR (n 2) art 1(1); Data Protection Directive (n 16) art 1.

18 See eg Milda Macenaite, 'The "Riskification" of European Data Protection Law Through a Two-Fold Shift' (2017) 8 EJRR 506, 506–07.

19 Francisco Costa-Cabral and Orla Lynskey 'Family Ties: The Intersection Between Data Protection and Competition in EU Law' (2017) 54 CML Rev 11, 17.

20 Orla Lynskey, 'From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection's Identity Crisis' in Serge Gutwirth and others (eds), *European Data Protection: Coming of Age* (Springer 2013) 59–84.

21 European Commission, 'Adequacy of the Protection of Personal Data in Non-EU Countries' <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en> accessed 22 May 2020.

the mutual adequacy arrangement with Japan[22] and excluding the EU–US Privacy Shield framework, recently invalidated by the CJEU[23]) and all other countries.[24] All adequacy decisions are currently under review by the European Commission.[25] The European Commission is currently conducting adequacy assessments for South Korea and for the UK following Brexit, which could be problematic following the CJEU *Schrems II* decision.[26] First introduced by the 1995 Data Protection Directive, the adequacy mechanism predates the EU Charter. But in the 2015 *Schrems I* ruling, the CJEU retroactively gave it constitutional meaning.[27] In short, personal data can flow as freely as within the EEA to third countries that have been 'cleared' as having an adequate level of protection. Transfers of personal data to other countries are only allowed if the data controller has implemented adequate safeguards, such as the SCCs approved by the European Commission, binding corporate rules (BCRs, for multinational companies or companies conducting joint economic activity), approved industry codes of conduct, or certification.[28] In practice, SCCs were, until recently, the most widely used tool for systematic international transfers of personal data to countries without an adequacy decision.[29] Although in the 2020 *Schrems II* decision the CJEU has concluded that the SCCs are valid in light of the EU Charter, the Court explained that, in practice, the use of the SCCs is only allowed if they yield a standard of protection for transferred personal

22 European Commission, 'European Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows' (23 January 2019) <http://europa.eu/rapid/press-release_IP-19-421_en.htm> accessed 22 May 2020.

23 *Schrems II* (n 4).

24 GDPR (n 2) art 45.

25 Catherine Stupp, 'Commission Conducting Review of All Foreign Data Transfer Deals' (*Euractiv*, 9 November 2017) <www.euractiv.com/section/data-protection/news/commission-conducting-review-of-all-foreign-data-transfer-deals/> accessed 22 May 2020.

26 Samuel Stolton, 'Commission Uncertain on Future UK Data Adequacy Agreement' (*Euractiv*, 24 June 2020) <https://www.euractiv.com/section/data-protection/news/commission-uncertain-on-future-uk-data-adequacy-agreement/> accessed 27 July 2020; Christakis (n 5).

27 *Schrems I* (n 1) para 72. This goal is now explicitly incorporated in GDPR (n 2) art 44.

28 GDPR (n 2) arts 40(2), 42(2), 46.

29 IAPP–EY Annual Governance Report (2019) 110 <https://iapp.org/store/books/a191P000003Qv5xQAC/> accessed 22 May 2020, showing that 88% of personal data transfers from the EU to the United States are based on the SCCs.

data 'essentially equivalent' to that in the EU.[30] If this is not the case, data exporters must put in place 'supplementary measures' to remedy the lack of essential equivalence of personal data protection or stop transferring personal data. If data exporters fail to do so, Data Protection Authorities are obliged to suspend or prohibit personal data transfers. This requirement makes the use of the SCCs problematic for transfers of personal data outside the EEA, especially to non-democratic countries.[31] Most of the adequate safeguards imply that the foreign recipient of European personal data should have an establishment or a business partner in the EEA. Foreign companies that collect personal data of Europeans via the internet and do not have a local establishment or business partner (for example, mobile app providers), may only rely on the codes of conduct and certification, none of which appear to be currently operational.[32]

If it is not reasonably possible for a company to adopt any of the above-mentioned safeguards, a company may rely on the specific derogations contained in Article 49 GDPR, which include explicit consent of a data subject, necessity of transfer for the conclusion or performance of a contract, or necessity for the establishment, exercise or defence of legal claims. These derogations are, however, only suitable for 'occasional' or 'non-repetitive' transfers, and cannot be relied upon for the purposes of regular and systematic transfers.[33] They are the only legal grounds that companies from the so-called 'non-adequate' countries that have no presence or business partner in the EEA

30 *Schrems II* (n 4) paras 96, 99, 100, 133–37, 142; Christopher Kuner, 'The *Schrems II* Judgment of the Court of Justice and the Future of Data Transfer Regulation' (*European Law Blog*, 17 July 2020) <https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/> accessed 27 July 2020.

31 *Schrems II* (n 4). The European Commission is currently working on updating the standard contractual clauses (SCCs); see Henriette Tielemans, 'What to Expect on Revised Standard Contractual Clauses' (IAPP, 29 September 2020) <https://iapp.org/news/a/revised-standard-contractual-clauses-what-to-expect/> accessed 12 November 2020. The new (draft) SCCs are not yet publicly available.

32 The author is not aware of any approved codes of conducts or certification mechanisms serving as appropriate safeguards for international transfers of personal data. The European Data Protection Board (EDPB) (an independent EU body consisting of representatives from EU Member States' data protection authorities) only recently adopted some of the necessary guidance on the certification mechanisms (EDPB, 'Guidelines 1/2018 on Certification and Identifying Certification Criteria in Accordance with Articles 42 and 43 of the Regulation' (4 June 2019) including Annex 2). See also Ryan Chiavetta, 'The Road to GDPR Certifications Won't Be a Short One, It Seems' (IAPP, 30 October 2018) <https://iapp.org/news/a/the-road-to-seeing-gdpr-certifications-wont-be-a-short-one/> accessed 22 May 2020. The EDPB has not yet adopted guidance on the codes of conduct as a tool for transfers of personal data outside the EEA.

33 EDPB, 'Guidelines 2/2018 on Derogations of Article 49 Under Regulation 2016/679' (25 May 2018) 4.

can use for cross-border collection of personal data in the absence of codes of conduct or certification.

2.3 *Compatibility of the EU Regime for Data Transfer with International Trade Law*

Shortly after the EU data protection framework was introduced, several academics flagged the potential inconsistency of the rules for transfers of personal data with the EU's commitments under the GATS, such as most-favoured nation (MFN) treatment, national treatment and market access, and cannot be justified under the Article XIV GATS general exception.[34] The EU is bound by these commitments not only under the GATS;[35] those commitments are present in virtually all the EU's post-GATS bilateral trade agreements.[36] Such warnings have intensified over time[37] under the influence of several factors:

34 Peter Swire and Robert E Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (Brookings Institution Press 1988) 188–96; Joel R Reidenberg, 'E-Commerce and Trans-Atlantic Privacy' (2001) 38 Hous L Rev 717, 736–737; Lucas Bergkamp, 'The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy' (2002) 18(1) CLS Rev 31, 39–40. On the contrary, Shaffer argued that a hypothetical claim of the United States regarding WTO inconsistency of EU's framework for personal data transfers 'would likely not prevail' (cf Gregory Shaffer, 'Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of US Privacy Standards' (2000) 25 Yale J Intl L 1, 46–51). Asinari admits that the EU regime for transfers of personal data may violate the EU's WTO commitments, but concludes that the violation can be justified under the general exception (Maria VP Asinari, 'Is There any Room for Privacy and Data Protection Within the WTO Rules' (2002) 9 ECL Rev 249, 277). It should however be noted that Asinari's article predates the WTO's interpretation of the 'necessity test' in most recent WTO case law as well as CJEU's case law on privacy and data protection as fundamental rights.

35 GATS (n 11) arts II, VI and VII; Annex 1B (n 6).

36 Such obligations are part of most of the EU's international trade agreements, the most recent examples being the Comprehensive Economic and Trade Agreement Between Canada, of the One Part, and the European Union and Its Member States, of the Other Part (14 September 2014) [2017] OJ L11/23 (CETA) arts 9.3, 9.5 and 9.6; the EU–Singapore Free Trade Agreement (not yet ratified by the EU, authentic text as of April 2018) arts 8.5, 8.6; and the Economic Partnership Agreement Between the European Union and Japan (JEFTA), Annex to the Proposal for a Council Decision, COM(2018) 192 final (18 April 2018) arts 8.15–8.17 <http://trade.ec.europa.eu/doclib/docs/2018/august/tradoc_157228.pdf#page=185> accessed 22 May 2020.

37 See eg Carla L Reyes, 'WTO-Compliant Protection of Fundamental Rights: Lessons from the EU Privacy Directive' (2011) 12 Melbourne JIL 1, 24–26; Perry Keller, *European and International Media Law: Liberal Democracy, Trade and New Media* (OUP 2011); Rolf H Weber, 'Regulatory Autonomy and Privacy Standards Under the GATS' (2012) 7 Asian Journal of WTO & International Health Law & Policy 25; Rolf H Weber and Dominic Staiger, *Transatlantic Data Protection in Practice* (Springer 2017) 58–59; Diane A MacDonald and Christine M Streatfeild, 'Personal Data Privacy and the WTO' (2014) 36

the increasing importance of international transfers of personal data for digital trade; the Snowden revelations that led to the invalidation of the EU–US Safe Harbor framework for commercial transfers of personal data to the United States in 2015;[38] the challenge to the validity of the SCCs and the Privacy Shield at the CJEU (which resulted in higher standards for the former and invalidation of the latter);[39] the adoption of the GDPR in 2016 (which introduced a stricter enforcement regime); and recurring pressure to include cross-border data flow provisions in trade agreements. Although the GDPR only marginally changed the framework for personal data transfers compared to the 1995 Data Protection Directive, it significantly raised the stakes of violating these rules by introducing harsh penalties, which include a fine of up to 4% of the total worldwide annual turnover of an undertaking for the preceding financial year.[40] Under certain circumstances, this fine could be based not just on the turnover of a business unit that has violated the rules, but instead on the turnover of a multinational entity as a whole.[41] Higher stakes for violating

---

Hous J Intl L 625; Svetlana Yakovleva and Kristina Irion, 'The Best of Both Worlds? Free Trade in Services and EU Law on Privacy and Data Protection' (2016) 2 EDPL 191; Nivedita Sen, 'Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path?' (2018) 21(2) JIEL 323; Samuel Coldicutt and Nivedita Sen, 'Testing the GDPR's WTO Readiness' (Linklaters) <www.linklaters.com/en/insights/blogs/tradelinks/testing-the-gdprs-wto-readiness> accessed 22 May 2020; Aaditya Mattoo and Joshua P Meltzer, 'International Data Flows and Privacy The Conflict and Its Resolution' (2018) World Bank Group Policy Research Working Paper 8431 <http://documents.worldbank.org/curated/en/751621525705087132/pdf/WPS8431.pdf> accessed 22 May 2020. In contrast, acknowledging that EU adequacy assessment may violate EU's WTO commitments, Chen envisions the possibility of such violation being justified under GATS art XIV(c)(ii) (Yi-Hsuan Chen, 'The EU Data Protection Law Reform: Challenges for Service Trade Liberalization and Possible Approaches for Harmonizing Privacy Standards into the Context of GATS' (2015) Span YB Intl L 211, 218).

38 *Schrems I* (n 1).

39 *Schrems II* (n 4), Vincent Manancourt, 'The EU Court Ruling that Could Blow up Digital Trade' (*Politico*, 13 July 2020) <https://www.politico.eu/article/us-china-data-flows-at-risk-in-top-eu-court-ruling/> accessed 27 July 2020.

40 GDPR (n 2) art 83(5).

41 Article 29 Working Party, 'Guidelines on the Application and Setting of Administrative Fines for the Purposes of the Regulation 2016/679, WP253' (3 October 2017) 6; CJEU, Case C-41/90, *Höfner and Elsner v Macrotron*, ECLI:EU:C:1991:161, para 21; CJEU, Case C-217/05, *Confederación Española de Empresarios de Estaciones de Servicio v Compañía Española*, ECLI:EU:C:2006:784, para 40. See also CJEU, Case C-97/08, *Akzo Nobel v Commission*, ECLI:EU:C:2009:536, para 60; CJEU, Case T-299/08, *Elf Aquitaine v Commission*, ECLI:EU:T:2011:217, para 56; CJEU, Case 48–69, *ICI v Commission*, ECLI:EU:C:1972:70, paras 125–46.

the rules on transfers of personal data outside the EEA increase the risks of a collision between international trade law and EU's data protection framework.

Although the GATS does not specifically regulate cross-border flows of (personal) data, such flows may still be captured by GATS' 'mode of supply 1' (cross-border trade) when data transfers enable cross-border provision of services.[42] Some have argued that differences in the treatment by the EU of services and service providers from countries that have and those from countries that do not have an adequacy decision may amount to a violation of the MFN principle.[43] Moreover, restrictive rules for transfers to countries that have not been afforded an adequacy decision have been characterized as discrimination between foreign service providers, especially those who do not have an establishment or business partner in the EEA, and providers from the EEA, and thus constitute another potential violation of the GATS, namely the national treatment obligation.[44] For example, unlike EEA providers, foreign companies cannot use legitimate business interest a as lawful ground for collecting Europeans' personal data: Such collection coincides with a cross-border transfer of personal data, which requires an additional legal basis. However, legitimate business interest is not mentioned among the lawful grounds for cross-border transfers in the GDPR.

The CJEU's *Schrems II* decision may have implications beyond transfers of personal data to the US, the EU–US Privacy Shield and the SCCs directly addressed by the decision. The obligation on data exporters to assess whether foreign legal frameworks provide for an 'essentially equivalent' level of data protection and, if not, put in place 'supplementary measures,' as well as the obligation of Data Protection Authorities to suspend or prohibit transfers if data a exporter fails to put such measures in place, applies not only to the SCCs addressed in the decision but also to other mechanisms for systematic transfers of personal data under Article 46 GDPR, most importantly the BCRs.[45] Depending on how restrictive these 'supplementary measures' – as interpreted by Data Protection Authorities – should be, the EU framework may

42 Susannah Hodson, 'Applying WTO and FTA Disciplines to Data Localization Measures' (2018) 18 World Trade Review 5, 8.

43 See eg Asinari (n 34) 273; Yakovleva and Irion (n 37) 203; Kristina Irion, Svetlana Yakovleva and Marija Bartl, 'Trade and Privacy: Complicated Bedfellows? How to Achieve Data Protection-Proof Free Trade Agreements' (Institute for Information Law (IViR), Amsterdam, 13 July 2016) 28–30; Bergkamp (n 34) 39; Keller (n 37) 353; Reyes (n 37) 14–16; Sen (n 37) 335–338.

44 See eg Coldicutt and Sen (n 37); Yakovleva and Irion (n 37) 204.

45 *Schrems II* (n 4) para 105; European Data Protection Board, 'Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data' (10 November 2020) para 22.

become at risk of violating market access commitments in data processing and database services, where transfers of data are essential for the production and delivery of services.[46]

The data governance model allowing free cross-border flows of (personal) data discussed in the following Section – gaining popularity in recent free trade agreements – is also eventually bound to exercise mounting pressure on the EU's framework for transfers of personal data.

2.4 *Changing Landscape of International Trade Law*

In response to technological change, new international law disciplines for digital trade are emerging through bi- and plurilateral trade venues that by-pass the WTO. The so-called 'new generation' free trade agreements entered into by the EU's most important trading partners, such as Canada, Japan and the United States, tend to include provisions obliging their parties to allow free cross-border flows of information, including personal data. These disciplines have, for example, been included in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP),[47] the US–Mexico–Canada Agreement (USMCA)[48] and the US–Japan Digital Trade Agreement.[49] In all such agreements, a free data flow obligation is counterbalanced by an exception, strongly resembling that of the GATS Article XIV (c) that allows parties to derogate

46 See eg Sen (n 37) 335; Reyes (n 37) 22; Weber (n 37) 33–34; Daniel Crosby, 'Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments' (2016) The E15 Initiative World Economic Forum Policy Brief 5–7 <http://e15initiative.org/wp-content/uploads/2015/09/E15-Policy-Brief-Crosby-Final.pdf> accessed 22 May 2020; Coldicutt and Sen (n 37).

47 Comprehensive and Progressive Agreement for Trans-Pacific Partnership Between Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Vietnam (signed 8 March 2018, effective 30 December 2018) (CTPPP) art 14.11 <www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf> accessed 22 May 2020, which states 'Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person'.

48 Under art 19.11 of the Agreement Between the United States of America, the United Mexican States, and Canada (revision of the 1994 North American Free Trade Agreement, signed 30 November 2018, effective 1 July 2020) (USMCA), '[n]o Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person' (<https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19_Digital_Trade.pdf> accessed 22 May 2020).

49 Agreement Between the United States of America and Japan Concerning Digital Trade (26 December 2019) (US–Japan Digital Trade Agreement) art 11 <https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf> accessed 22 May 2020.

from it to adopt and maintain regulation in public interest.[50] Cross-border data flows are also high on the agenda in the negotiations on e-commerce at the WTO between 76 WTO members.[51]

The possibility of inclusion of such a provision with a GATS Article XIV-type exception for data protection in Trade in Services Agreement (TiSA) and Transatlantic Trade and Investment Partnership (TTIP) – both now stalled – sparked a strong push back from European academics and civil society in 2015–2016.[52] Later on, in order to avoid any risk of undermining the fundamental rights to privacy and the protection of personal data, the EU ultimately refrained from including such a provision in the Economic Partnership Agreement between the European Union and Japan (JEFTA) and the revision of the EU–Mexico Free Trade Agreement.[53] In the case of Japan, the absence of such clause was compensated by the adoption of a mutual adequacy decision under the GDPR shortly before JEFTA took effect.[54]

Unlike the CPTPP, the USMCA and the United States–Japan Digital Trade Agreement, the EU's approach in the above-mentioned 2018 model clauses[55] contains a narrower prohibition on restrictions of cross-border data flows and a broad exception for domestic privacy and data protection rules, including restrictions on transfers of personal data.[56] It is precisely for these reasons

50 CPTPP (n 47) art 14.11(3); USMCA (n 48) art 19.11; US–Japan Digital Trade Agreement (n 49) art 11(2).

51 European Commission, '76 WTO Partners Launch Talks on E-Commerce' (25 January 2019) <http://trade.ec.europa.eu/doclib/press/index.cfm?id=1974&title=76-WTO-members-launch-talks-on-e-commerce> accessed 22 May 2020.

52 See Irion, Yakovleva and Bartl (n 43) 44–45, 59–60; Maryant Fernández Pérez, 'Corporate-Sponsored Privacy Confusion in the EU on Trade and Data Protection' (European Digital Rights, 12 October 2016) <https://edri.org/corporate-sponsored-privacy-confusion-eu-trade-data-protection/> accessed 22 May 2020; Resolution Containing the European Parliament's Recommendations to the European Commission on the Negotiations for the Transatlantic Trade and Investment Partnership (8 July 2015) 2014/2228(INI) (TTIP); Resolution Containing the European Parliament's Recommendations to the Commission on the Negotiations for the Trade in Services Agreement (3 February 2016) 2015/2233 (TiSA).

53 Both agreements include a commitment to reconsider the issue within three years after the agreement enters into force. See JEFTA (n 36) art 8.81; EU Proposal for a Chapter on Digital Trade of the Modernised EU–Mexico Free Trade Agreement (21 April 2018) art XX <http://trade.ec.europa.eu/doclib/docs/2018/april/tradoc_156811.pdf> accessed 22 May 2020. See also Fortnam (n 8).

54 See supra n 23.

55 Horizontal Provisions (n 8).

56 Model article A prohibits an exhaustive list of restrictions on cross-border data flows: the requirement to use local computing facilities or network elements (both as such and as a precondition for data transfers), data localization requirements, and prohibition on

that it may be difficult for the EU to convince its trading partners to accept these clauses: while outlawing some data localization rules of its trading partners, such as Indonesia,[57] the proposed clauses are unlikely to affect the EU's own restrictions inconvenient for those trading partners. Conversely, the EU is unlikely to agree to the cross-border data flow provisions advanced by the United States just mentioned above, for this would mean a clear derogation from Charter-based fundamental rights. Nevertheless, adherence to this model by countries that maintain a free flow of personal data from the EU based on adequacy decisions, in particular, Canada, Japan and New Zealand, puts pressure on the EU's restrictions on transfers of personal data.

3 Applying the Two Necessities: A Catch-22 for the EU

3.1 *Framing the Issue*

This Section illuminates the clash between EU law and international trade law regulating trade in services, when it comes to the regulatory framework that both legal systems require for cross-border transfers of personal data.

In trade agreements, one of the primary mechanisms to accommodate the EU's autonomy to adopt and maintain regulation inconsistent with its international trade commitments are the so-called general exceptions. The part of the general exception of GATS Article XIV(c)(ii) that is specifically relevant for privacy and data protection reads as follows:

> Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures …

storing or processing information abroad. Model article B contains a national security-type exception for domestic privacy and data protection regime – sufficiently broader than the GATS Article XIV(c)(ii) exception, which allows each party to take any measures 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'.

57 Herbert Smith Freehills LLP, 'Indonesia Proposes Amendments to Its Data Localisation Requirement' (*Lexology*, 11 December 2018) <www.lexology.com/library/detail.aspx?g=a116020b-cee3-433f-b62b-a5e988477d8e> accessed 22 May 2020.

> (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to …
>
> (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts …

Section 3.2 argues that the trade 'necessity test' – the core of the general exception – could be too narrow to accommodate EU's autonomy to maintain the GDPR framework for transfers of personal data. As a result, the EU may be required by the WTO (or dispute settlement body under another trade agreement) to adjust the rules on cross-border transfers of personal data and, potentially, to abandon the adequacy approach.

From an EU law perspective, entering into a new international trade agreement or complying with an existing one that limits any of the fundamental rights under EU Charter is a derogation from the EU Charter and thus is subject to its Article 52(1). According to this provision,

> [a]ny limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

As the CJEU has explained, the derogation clause applies equally to both internal and external legislative acts of the EU, such as international agreements.[58] Affirming the supremacy of the EU Charter over the EU's international agreements, the CJEU confirmed that the EU may neither conclude nor implement through an EU legislative act any international agreement (or decision of an international adjudicating body based on this agreement) if the conditions laid out in this derogation clause, namely the proportionality and 'necessity' tests (that is, the 'EU Charter "necessity test"') are not fulfilled.[59] Then, Article 218(11) TFEU[60] provides for a mechanism to ensure that an international trade

58 Opinion 1/15 (n 1) para 146.

59 Arianna Vedaschi, 'Privacy and Data Protection Versus National Security in Transnational Flights: The EU – Canada PNR Agreement' (2018) 8(2) IDPL 124, 138.

60 Treaty on the Functioning of the European Union (consolidated version, 26 October 2012) OJ C 326, 47–390.

agreement is compatible with the EU's constitutional framework before it is concluded by the EU. It allows an EU Member State, the European Parliament, the Council or the European Commission to request an opinion from the CJEU regarding the compatibility of a proposed international agreement with the EU Treaties, including the EU Charter. If the CJEU decides that such agreement is incompatible with the Treaties, the international agreement cannot take effect until and unless it is brought in compliance with the Treaties. This provision was used at the request of the European Parliament concerning the EU–Canada agreement on the transfer and processing of Passenger Name Record data (the *Opinion on EU–Canada PNR Agreement*),[61] which, among other things, mandated transfers of Europeans' personal data to Canada. In this landmark ruling, having tested these provisions against the requirements of the derogation clause, including the EU Charter 'necessity test', the CJEU held that agreement could not be concluded unless revised.[62]

It is now settled law at the CJEU that international agreements entered into by the EU must be 'entirely compatible with the Treaties and with the constitutional principles stemming therefrom.'[63] In particular, such agreements must be compatible with the right to privacy and the right to the protection of personal data.[64] This is crucial to the analysis because, if the EU framework for personal data transfers were deemed inconsistent with a trade agreement – for example, for failing to meet the requirements of the trade 'necessity' test contained in the general exception – and the EU was required to bring its laws into conformity with the trade agreement, compliance with the decision of a trade adjudicating body establishing such inconsistency would be a derogation from the fundamental rights codified by Articles 7 and 8 of the EU Charter. It follows from the CJEU's jurisprudence, however, that before such decision of an international trade adjudicating body could be implemented, compliance would have to be tested under the requirements of Article 52(1) of the EU Charter. Yet, as Section 3.3 argues in detail, trade law's 'necessity test' viewed as a derogation from the EU's fundamental right to privacy and the protection of personal data is unlikely to meet the EU Charter 'necessity' test. Put differently, the trade 'necessity test' obligates the EU to derogate from fundamental rights more than the EU is legally allowed to do under Article 52(1) of the EU Charter.

61 Opinion 1/15 (n 1).
62 ibid paras 232(2)–(3).
63 ibid paras 67, 70.
64 ibid paras 70, 119.

To sum up, not only could the EU framework for personal data transfers be found in violation of the EU's international trade commitments, but in addition international trade commitments requiring (unrestricted) transfers of personal data outside the EEA may be found inconsistent with the EU Charter. Simultaneous application of the two 'necessity tests' (trade law and Article 52 of the Charter), could thus potentially put the EU in a catch-22 situation discussed in Section 3.4.

An important doctrinal point should be clarified before moving on. Although international trade agreements are binding on the EU and constitute an 'integral part' of its legal system,[65] in the hierarchy of EU legal order EU primary law (including the EU Charter) prevails over the EU's international trade commitments.[66] Moreover, neither international trade agreements nor the decisions of international trade adjudicating bodies have direct effect in the EU.[67] This, nevertheless, does not make the EU's obligations under international trade law less binding from an international law perspective. Under international law, the EU must perform its obligations in good faith.[68] The EU may face liability and retaliation under international trade law if it fails to comply with its trade commitments or a decision of a trade-adjudicating body, even if such compliance is not possible due to constraints contained in EU primary law.[69] This is why constitutional restrictions on compliance with such obligations or decisions are a potentally serious problem.

3.2 *Necessity Under International Trade Law and Its Application to the EU Framework on Personal Data Transfers*

To be justified under the general exception contained in GATS Article XIV, a GATS-inconsistent measure has to meet one of the material requirements of

65 See eg CJEU, Case 181–73, *R & V Haegeman v Belgian State*, EU:C:1974:41, para 5; CJEU, Opinion 2/13 – Accession of the EU to the European Convention for the Protection of Human Rights and Fundamental Freedoms, ECLI:EU:C:2014:2454, para 180.

66 CJEU, Joined Cases C-402/05 P and C-415/05 P, *Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities*, ECLI:EU:C:2008:461, paras 282, 307, 308, 316.

67 Aliki Semertzi, 'The Preclusion of Direct Effect in the Recently Concluded EU Free Trade Agreements' (2014) 51 CML Rev 1125, 1132–35; see also Szilard Gáspár-Szilágyi, 'The "Primacy" and "Direct Effect" of EU International Agreements' (2015) 21(2) EPL 343; Paul Craig and Grainne De Búrca, *EU Law: Text, Cases, and Materials* (6th edn, OUP 2015), 362–63; Francesca Martines, 'Direct Effect of International Agreements of the European Union' (2014) 25(1) EJIL 129. For an elaborate discussion of these issues in the present context, see Yakovleva and Irion (n 37) 200–02.

68 Vienna Convention on the Law of Treaties (1969) 1155 UNTS 331 (VCLT) art 31.1.

69 ibid art 27.

the general exception set forth in Article XIV (a) to (e) and the introductory clause (or *chapeau*) of this Article.[70] The wording of the general exception is remarkably consistent in most US- and EU-led FTAs, in that they closely follow GATS Article XIV.[71] This is why the interpretation of trade 'necessity test' at the WTO may be relevant also in the context of other trade agreements.

Article XIV(c)(ii) has never been applied by a WTO panel. However, privacy and data protection is not the first public policy interest in tension with trade liberalisation. The interpretation of the 'necessity test' in WTO cases touching upon other public policy interests listed in GATS Article XIV(c) and Article XX of the General Agreement on Tariffs and Trade (GATT)[72] can inform the interpretation of paragraph (c)(ii). The method used to interpret 'necessity' applied by WTO adjudicating bodies is fairly consistent irrespective of the specific public interest invoked to justify the measure, be it the protection of public morals, public health or securing compliance with a WTO-consistent law.[73] Existing WTO case law has established a high threshold for meeting the 'necessity test', which in some cases has been almost impossible to meet.[74]

70 WTO, *Argentina – Measures Relating to Trade in Goods and Services*, Report of the Appellate Body (9 May 2016) WT/DS453/AB/R (*Argentina – Financial Services*) para 6.161; WTO, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, Report of the Appellate Body Report (20 April 2005) WT/DS285/AB/R (*US – Gambling*) para 292.

71 The most recent examples of EU trade agreements where the GATS (n 11) art XIV was closely reproduced include CETA art 28.3(2)(c)(ii), EU–Singapore FTA art 8.62(e)(ii), and JEFTA art 8.3 (each in supra n 36).

72 Marrakesh Agreement (n 6) Annex 1A.

73 The WTO adjudicating bodies apply the same interpretation of 'necessity' as pronounced in WTO, *Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef*, Report of the Appellate Body (10 January 2001) WT/DS161/AB/R, WT/DS169/AB/R (*Korea – Various Measures on Beef*) paras 160–64 irrespective of the specific paragraph of GATS art XIV or GATT art XX. See eg in relation to GATT art XX(b), WTO, *European Communities – Measures Affecting Asbestos and Asbestos-Containing Products*, Report of the Appellate Body (5 April 2001) WT/DS135/AB/R (*ES – Asbestos*) para 171–75; in relation to GATS art XIV(a), WTO, *US – Gambling* (n 70) paras 291, 305–08; in relation to GATS art XIV(c), WTO, *Argentina – Financial Services* (n 70) paras 6.202–205, 6.227 et seq. See also Panagiotis Delimatsis, 'Protecting Public Morals in a Digital Age: Revisiting the WTO Rulings on *US – Gambling* and *China – Publications and Audiovisual Products*' (2011) 14(2) JIEL 257, 262.

74 ibid 266; Ingo Venzke, 'Making General Exceptions: The Spell of Precedents in Developing Article XX GATT into Standards for Domestic Regulatory Policy' (2011) 12(05) German Law Journal 1111, 1118–19.

The assessment of the 'necessity' of a GATS-inconsistent measure applied by the WTO adjudicating bodies – first expounded in *Korea – Various Measures on Beef*[75] – requires 'weighing and balancing' of the following factors:[76]

1. The relative importance of the protected public interest(s) pursued by such inconsistent measure,
2. The contested measure's contribution to the achievement of objective pursued,
3. The trade restrictiveness of the measure,[77] and
4. A determination of whether, in the light of importance of the interests at issue, a less trade restrictive alternative is 'reasonably available'.

As the WTO Appellate Body stated in *US – Gambling*, the process of assessing 'necessity' 'begins with an assessment of the 'relative importance' of the interests or values furthered by the challenged measure.'[78] The more important the interest, the heavier it weighs in the assessment, and the heavier it weighs in the justification of a relatively more restrictive measure. First and foremost, the mere fact that the relative importance of a domestic interest can be assessed by trade adjudicators based on their own value structures creates the risk of putting liberalization of international trade ahead of societal interests. Second, how WTO adjudicating bodies assign importance to a particular public policy interest is unclear. In prior cases, they have assigned – without a line of reasoning – different degrees of importance to the various public policy objectives mentioned in the general exceptions of GATS Article XIV and GATT Article XX,[79] but no objective has yet been characterized as 'unimportant.' Some case law suggests that the level of international

75 *Korea – Various Measure on Beef* (n 73) para 164.

76 WTO, *Argentina – Financial Services*, Report of the Panel (9 May 2016) WT/DS453/R, Add.1, para 7.661, *US – Gambling* (n 70) paras 304–07, WTO, *European Communities – Measures Prohibiting the Importation and Marketing of Seal Products*, Report of the Appellate Body (18 June 2014) WT/DS400/AB/R and WT/DS401/AB/R (*EC–Seal Products*) paras 5.169, 5.214.

77 Assessment of this factor was left out in Appellate Body Report *EC – Asbestos* (n 73).

78 *US – Gambling* (n 70) para 306; *Korea – Various Measures on Beef* (n 73) para 164; WTO, *Brazil – Measures Affecting Imports of Retreaded Tyres*, Report of the Appellate Body (17 December 2007) WT/DS332/AB/R (*Brazil – Retreaded Tyres*) para 143.

79 See eg *EC – Asbestos* (n 73) para 172; *Brazil – Retreaded Tyres* (n 78) para 179; *Argentina – Financial Services* (n 76) para 7.671.

support of the interest at stake[80] or the actual (as opposed to aspired) contribution of the measure to achieve a claimed level of protection of public policy interest[81] could weigh in this assessment.

Assessment of factors 2 and 3 in the list above comprises a weighing and balancing of the contribution of the measure to the protected interest with the trade restrictiveness of the measure in light of the relative importance of the protected interest or the underlying values of the objective pursued.[82] On a continuum between 'indispensable' and 'making a contribution to,' 'necessity' is understood as being closer to 'indispensable' rather than 'making a contribution to.'[83] Thus, the greater the contribution of the contested measure, and the less restrictive it is, the more likely it is to satisfy the 'necessity test.'[84]

If the defending party has succeeded in making a *prima facie* case of 'necessity,' the complaining party may rebut it by showing that a less trade-restrictive measure was 'reasonably available' to the defending party. This triggers the assessment of the factor 4 in the list above, which includes a 'comparison between the challenged measure and possible alternatives … and the results of such comparison should be considered in the light of the importance of the interests at issue.'[85] 'Reasonably available' is interpreted as allowing a WTO member to achieve the same level of protection of the public interest or objective pursued without prohibitive cost or substantial technical difficulties.[86] Based on this interpretation, the comparison of alternative measures does not typically involve a fully-fledged proportionality assessment, which is arguably the case in the assessment of the first three factors in the list above.[87] Rather,

80 *Argentina – Financial Services* (n 76) paras 7.671, 7.715.

81 *EC – Seal Products* (n 76) para 5.502; Ming Du, 'The Necessity Test in World Trade Law: What Now?' (2016) 15 Chinese JIL 817, 826–27.

82 *Brazil – Retreaded Tyres* (n 78) para 210; *EC – Seal Products* (n 76) para 5.210; *US – Gambling* (n 70) para 306; *Argentina – Financial Services* (n 76) para 7.684.

83 *Korea – Various Measures on Beef* (n 73) paras 160–61; *US – Gambling* (n 69) para 310; WTO Note by Secretariat, '"Necessity Tests" in the WTO' (2 December 2003) S/WPDR/W/27, 8–9.

84 *Argentina – Financial Services* (n 76) paras 7.685, 7.727 referring to WTO, *Korea – Various Measures on Beef* (n 73) para 163.

85 *US – Gambling* (n 70) para 307.

86 ibid para 308; WTO, *Korea – Various Measures on Beef* (n 73) paras 176, 178.

87 Mads Andenas and Stefan Zleptnig, 'Proportionality: WTO Law in Comparative Perspective' (2007) 42 Tex Intl L J 371, 414; Meinhard Hilf and Sebastian Puth, 'The Principle of Proportionality on Its Way into WTO/GATT Law' in Armin von Bogdandy, Petros C Mavroidis and Yves Mény (eds), *European Integration and International Co-Ordination* (Wolters Kluwer 2002) 199; Gabrielle Marceau and Joel P Trachtman, 'The Technical Barriers to Trade Agreement, the Sanitary and Phytosanitary Measures Agreement, and

this comparison involves the balancing of the administrative and enforcement costs of alternative measures granting the same level of protection to a public interest at issue against the trade costs of such measures.[88]

It is generally agreed that the balancing of the first three factors and that of the fourth factor contain a logical contradiction and are incompatible: the first assessment leaves WTO members much less regulatory autonomy than the other.[89] The WTO adjudicating bodies, most of the time, base their decision on the assessment of the fourth factor – a more lenient approach compared with the proportionality assessment – which, arguably, allows WTO members to choose the level of protection of the public interest at issue.[90] However, the risk that those bodies will conduct a full-fledged cost-benefit balancing always remains. Furthermore, in practice, the WTO members' autonomy to choose and maintain their own level of protection could be much narrower than it may seem at first glance, notably because it can be narrowed depending on how the adjudicating bodies interpret the term 'same level' of protection.

Does the 'same' level of protection mean a desired level of protection (subjectively determined by the State and not (yet) necessarily achieved) or the actual level of protection achieved by the disputed measures? The WTO adjudicating bodies have not been consistent in their answer to this question. For example, in *Korea – Various Measures on Beef*, based on the actual application of the contested measure, judging by the design of the contested measure the Appellate Body 'assumed' that 'Korea intended to reduce considerably the number of cases of fraud occurring with respect to the origin of beef sold by retailers' rather than to 'totally eliminate fraud.'[91] From this perspective, alternative measures (compared to the contested measure) should not be required

---

the General Agreement on Tariffs and Trade: A Map of the World Trade Organization Law of Domestic Regulation of Goods' (2002) 36(5) JWT 811, 826–28, 851–53; Gabrielle Marceau and Joel P Trachtman, 'A Map of the World Trade Organization Law of Domestic Regulation of Goods: The Technical Barriers to Trade Agreement, the Sanitary and Phytosanitary Measures Agreement, and the General Agreement on Tariffs and Trade' (2014) 48(2) JWT 351, 368–69; Weber (n 37) 43.

88 Donald H Regan, 'The Meaning of "Necessary" in GATT Article XX and GATS Article XIV: The Myth of Cost-Benefit Balancing' (2007) 6(3) World Trade Review 347; Benn McGrady, 'Necessity Exceptions in WTO Law: Retreaded Tyres, Regulatory Purpose and Cumulative Regulatory Measures' (2009) 12(1) JIEL 153; Andrew TF Lang, 'Reflecting on Linkage: Cognitive and Institutional Change in the International Trading System' (2007) 70(4) MLR 523.

89 Venzke (n 74) 1133; Regan (n 88) 348.

90 Regan (n 88) 350; Venzke (n 74) 1138.

91 *Korea – Various Measures on Beef* (n 73) para 178, fn omitted.

to achieve a higher level of protection than that actually achieved by the contested measure. The level of protection desired by the defending WTO member is thus irrelevant. Remarkably, in that case the alternative measure that, according to Appellate Body, was reasonably available to Korea involved significantly higher administrative and enforcement costs.[92] This, however, did not prevent the Appellate Body from concluding that the contested measure did not pass the assessment under the fourth factor. Conversely, in *US – Gambling*, where the alternative measure proposed by a claiming party was dismissed as 'not an appropriate alternative' the Appellate Body explained that a 'reasonably available' alternative measure should preserve the responding Member's 'right to achieve its desired level of protection.'[93] Although the Appellate Body did not elaborate on the degree of deference to the WTO members in the assessment of the 'desired level', it could still be argued that the choice of this word requires a subjective assessment, namely what the WTO member aimed for, rather than an objective assessment of what the contested measure actually achieves. Clearly, the risk that trade adjudicating bodies will not respect the level of protection asserted by a defending party persists.

More generally, even if the adjudicating bodies were to afford sufficient deference to the level of protection desired by the State, the analytical exercise of ensuring that an alternative measure would achieve exactly the same level of protection would be nothing more than educated second-guessing. Especially when public policy goals pursued by contested measures are non-economic values, in practice it may be difficult to accurately define the level of their protection serving as benchmark for comparison of alternative measures. It is equally difficult to determine *ex ante* whether alternative measures would secure the same level of protection.

Recall that, while the assessment of reasonably available alternative measures is conducted in the light the importance of the public interest at issue, existing WTO case law does not shed much light on the weight of this factor in the assessment. There is, therefore, a related risk that the importance of the public interest, as determined by the adjudicating bodies, may influence the assessment of whether a less trade restrictive alternative measure is reasonably available. One could argue that the importance of the interest influences the deference to the level of protection chosen by the country. Thus, in *Korea – Various Measures on Beef*, where the Appellate Body did not make any statement as to the importance of the public interest pursued by the contested

92 ibid para 175.

93 *US – Gambling* (n 70) paras 308, 317, fn omitted.

measure, the level of deference to the chosen level of protection was lower as compared to *US – Gambling*, where the Appellate Body agreed that the contested measure protected 'very important societal interests.'[94]

From the above, one may conclude that the application of trade law's 'necessity test' to the EU framework for transfers of personal data to third countries may not result in the recognition of the 'necessity' of this framework by the WTO adjudicators for at least two reasons. First, it could be argued that the link between the EU framework for data transfers and the purpose to ensure a high level of protection of personal data, especially from the access of foreign governments to this data, is closer to 'making a contribution to' rather than 'indispensable.' In theory, an adequacy decision certifies that a particular third country ensures a level of personal data protection 'essentially equivalent' to that in the EU,[95] where the 'level of data protection' means not only the quality of the data protection rules, but multiple other factors, including the respect for the rule of law and human rights, access of public authorities to personal data, existence and effective functioning of independent supervisory authorities, etc.[96] However, at least four weaknesses in the design of the adequacy mechanism prevent it from delivering on this promise in practice. First, an adequacy decision embodies an assessment of a third country's legal framework at a particular point in time and does not provide for effective dynamic mechanisms of ensuring that the third country will maintain the same level of personal data protection throughout the life of the adequacy decision (the 'snapshot' problem). Periodic reviews of adequacy decisions, required under the GDPR Article 45(3) at least every four years, are simply not frequent enough in the fast-paced environment of the digital age. Second, if a foreign data controller violates the third country's data protection rules when processing a European's personal data, enforcement of such rights abroad is burdensome (the 'heavy burden' problem). Third, adequacy decisions, at best, guarantee that personal data transferred from the EEA is equally protected in the first country of destination – the one granted an adequacy decision – but most of the time fail to provide for the level of protection in relation to onward transfers of such data to other countries (the 'onward transfer' problem). Last but not least, adequacy assessments are not always 'objective and logical' but are prone to political

94 *US – Gambling* (n 70) para 232, referring to WTO, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, Report of the Panel (20 April 2005) WT/DS285/R, paras 6.492, 6.533.

95 *Schrems I* (n 1) para 73; GDPR (n 2) recital 104.

96 GDPR (n 2) art 45.

pressures from EU trading partners and the EU's own external digital trade policy (the 'political pressure' problem).[97]

Second, one can argue that the EU framework is not the 'least trade restrictive,' especially in relation to businesses not having an establishment or business partner in the EU. Other less restrictive options, such as the APEC Cross-Border Privacy Rules may be considered as 'reasonably available' to the EU.[98] Since the EU's rules for transfers of personal data are more restrictive than in the rest of the world, 'it may be difficult to prove that privacy cannot be otherwise protected.'[99] One could assert, as a counter-argument, that the level of protection of the fundamental right to personal data protection chosen by the EU – 'effective and complete' protection[100] – makes other less restrictive alternatives unavailable to the EU. In particular, in contrast to the EU Charter, existing international standards on personal data protection, such as the OECD 2013 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the 2015 APEC Privacy Framework[101] take an instrumental approach to the protection of personal data and therefore warrant a lower level of personal data protection (their primary purpose is to keep restrictions on personal data transfers to a minimum).[102] However, as explained above, it is entirely possible that trade adjudicators would give little deference to the EU's aspired level of protection, and would focus instead on the actual level of protection achieved. In the absence of precise statistics on this matter, the adjudicators may buy into empirical arguments, such as those offered by Bamberger and Mulligan that compared the EU data protection regime to the more liberal approach of the United States, and found that, although the latter was not as comprehensive 'on the books,' it operated much

97 See Christopher Kuner, 'Developing an Adequate Legal Framework for International Data Transfers' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Science+Business Media BV 2009) 8–9 <https://ssrn.com/abstract=1464323>; Graham Greenleaf, 'Japan: EU Adequacy Discounted' (2018) UNSW Law Research Paper No 19–5 <https://ssrn.com/abstract=3276016> both accessed 19 August 2020.

98 For a discussion see Svetlana Yakovleva, 'Should Fundamental Rights to Privacy and Data Protection Be a Part of EU's International Trade "Deals"?' (2018) 17(3) World Trade Review 477, 498–99.

99 Mira Burri, 'The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation' (2017) 51(65) UC Davis L Rev 65, 95–96.

100 CJEU, Case C-131/12, *Google Spain v Agencia Española de Protección de Datos*, ECLI:EU:C:2014:317, para 34; CJEU, Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, ECLI:EU:C:2018:388, para 28.

101 Asia-Pacific Economic Cooperation (APEC), 'Updates to the APEC Privacy Framework' (14–15 November 2016) <http://mddb.apec.org/Documents/2016/SOM/CSOM/16_csom_012app17.pdf> accessed 22 May 2020.

102 Yakovleva (n 98) 8–9.

more effectively 'on the ground'.[103] The dual fact that the EU framework for data transfers provides for the same restrictive approach in relation to any information that qualifies as personal data (which include a broad range of data under EU law)[104] and does not calibrate restrictiveness in relation to the severity of the risk of interference in individuals' fundamental rights could also be used as an indication that other – more granular and overall less trade restrictive – frameworks are 'reasonably available' to the EU. Consequently, the importance of the right to the protection of personal data would be given relatively less weight in a trade dispute. While in EU law it is recognized as a fundamental right – and hence one of the highest values in the EU, on par with other fundamental rights – trade adjudicating bodies may lean towards an economic approach to privacy and data protection that underlies existing international standards on data protection mentioned above.[105]

3.3 *Necessity Under EU Law*

The Lisbon treaty[106] not only transformed the right to the protection of personal data into a *sui generis* binding fundamental right; it also granted the EU competence to legislate on the protection of personal data as a fundamental right,[107] which underlies the adoption of the GDPR.[108] In contrast, the Data Protection Directive was based on the EU competence to regulate the internal market.[109] The constitutionalization of the fundamental rights to privacy and the protection of personal data eventually not only shifted the core normative rationale of protecting these rights within the EU from predominantly economic goal of ensuring free flow of personal data in the EU to the protection of individual rights, it also altered the balance between economic and non-economic values in the EU's external economic policy.[110] Entrusted with the

103 Deirdre K Bamberger and Keneth A Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (*Information Policy*) (MIT Press 2015). Bert-Jaap Koops also underscores 'an enormous disconnect' between European data protection law and reality (see Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4(4) IDPL 250, 256).

104 See Nadezhda Purtova, 'The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10(1) Innovation and Technology 40.

105 Yakovleva (n 98) 482–85, 489, 496.

106 Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community (signed at Lisbon, 13 December 2007) OJ C 306 (Lisbon Treaty).

107 Treaty on the Functioning of the European Union (n 60) art 16(1).

108 GDPR (n 2) recitals 1 and 12.

109 Data Protection Directive (n 16) recitals 3, 5 and 8.

110 Under the Lisbon Treaty, negotiation and conclusion of international trade agreements must be guided by the universality and indivisibility of human rights and fundamental freedoms, respect for human dignity and principles of the United Nations and international law (Treaty on European Union (n 60) arts 2(5) and 2, 13–390).

power to interpret the Charter, the CJEU has taken up a role of a guarantor of EU fundamental rights and played an important role in building up jurisprudence on Articles 7 and 8 of the Charter as well as in the interpretation of the derogation clause of Article 52(1) in relation to these rights. In the abovementioned *Opinion on EU – Canada PNR Agreement*, the CJEU has used data protection 'as a vehicle to assert EU fundamental rights in an international context.'[111]

From the CJEU case law, it follows that any legislative act of the EU that involves personal data processing, such as use or transfer or personal data, constitutes 'in itself' a limitation of the fundamental right to the protection of personal data, regardless of whether it can be justified.[112] Such limitation first triggers the assessment under the requirements of Article 8(2) of the EU Charter. Then, any limitation on this right is only lawful if it meets the requirements of Article 52(1) of the EU Charter,[113] which provides for a mechanism of balancing different fundamental rights and freedoms with each other, as well as with other competing policy objectives.[114]

It is the prerogative of the CJEU to conduct a fact-based assessment of whether a derogation is 'necessary' in each particular case.[115] Since 2009, the CJEU has been rather proactive in applying the EU Charter 'necessity test'(Article 52(1)) when balancing the fundamental rights to privacy and the protection of personal data with other competing rights and interests. In a line of cases, most notably *Volker und Markus Schecke*, *Digital Rights Ireland*, *Tele 2*, *Schrems I*, and *Opinion on EU – Canada PNR Agreement*, the CJEU elevated the EU Charter necessity test to the level of 'strict necessity' when a derogation from the fundamental rights to privacy and the protection of personal data is

111 Christopher Kuner, 'International Agreements, Data Protection, and EU Fundamental Rights on the International Stage: Opinion 1/15, EU – Canada PNR' (2018) 55 CML Rev, 857, 858.

112 CJEU, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources*, ECLI:EU:C:2014:238, paras 34–36; CJEU, Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke and Eifert v Land Hessen*, ECLI:EU:C:2010:662, para 58. See also European Data Protection Supervisor (EDPS), 'Assessing the Necessity of Measures that Limit the Fundamental Right to the Protection of Personal Data: A Toolkit' (11 April 2017) 7 <https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf> accessed 22 May 2020.

113 Existing CJEU case law suggests that the conditions of lawfulness of personal data processing contained in art 8(2) and art 52(1) of the EU Charter should be analysed cumulatively. See eg Opinion 1/15 (n 1) paras 137–38, 142 et seq.

114 Unlike international trade law, the text of art 52(1) explicitly mentions that the assessment of 'necessity' should include a fully-fledged proportionality balancing.

115 EDPS (n 112) 8.

at stake.[116] This approach was later taken up by the European Data Protection Authorities[117] and the European Data Protection Supervisor (EDPS).[118] It is now settled CJEU case law that the 'strict necessity' standard should apply horizontally in all contexts, both commercial and national security, as long as limitation of the fundamental rights to privacy and data protection is at stake.[119]

By setting a higher threshold for derogation from the fundamental rights protecting personal data when balanced against the freedom of expression and information (Article 11) and the freedom to conduct a business (Article 16), the CJEU arguably tilted the balance between different fundamental rights in favour of those concerning privacy and data protection. Although Lenaerts, the President of the CJEU, contended that 'there is no hierarchy of qualified rights under the Charter',[120] in practice, the CJEU *de facto* tends to rank fundamental rights to privacy and data protection at a higher level, as the article explains further below.

Just as with the trade 'necessity test', 'strict necessity' under Article 52(1) of the EU Charter in relation to privacy and data protection is hard to satisfy. In assessing 'strict necessity' the CJEU determines whether 'it is possible to envisage measures which affect less adversely that fundamental right of natural persons and which still contribute effectively to the objectives … in question.'[121] This approach resembles the least-restrictive-means principle of trade law. While trade law requires that measures aimed at protecting the right to protection of personal data should be least restrictive on trade, conversely, the EU Charter demands that trade rules should be least restrictive of fundamental rights.

Both the *Schrems I* and *Opinion on EU – Canada PNR Agreement* judgements came in the wake of the Snowden revelations, which exposed the risks of US mass surveillance for Europans' privacy. This awareness has put the rules concerning foreign governments' access to Europeans data for national

116 Joined Cases C-92/09 and C-93/09 (n 112) paras 77 and 86; Joined Cases C-293/12 and C-594/12 (n 112) paras 51 and 52; CJEU, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige v Tom Watson*, ECLI:EU:C:2016:970, paras 96 and 103; *Schrems I* (n 1) para 92; CJEU Opinion 1/15 (n 1) para 140.

117 See eg Article 29 Working Party, 'Working Document 01/2016 on the Justification of Interferences with the Fundamental Rights to Privacy and Data Protection Through Surveillance Measures when Transferring Personal Data (European Essential Guarantees), WP 237' (13 April 2016) 5.

118 EDPS (n 112) 2.

119 See ibid 7, referring to a line of the CJEU jurisprudence.

120 Koen Lenaerts, 'Exploring the Limits of the EU Charter of Fundamental Rights' (2012) 8(3) European Constitutional Law Review 375, 392–393.

121 Joined Cases C-92/09 &C-93/09 (n 112) para 86.

security or law enforcement purposes and the rights of individuals to effective remedy against such foreign states in the spotlight of 'adequacy' assessment of a foreign country's data protection framework. The same issues lie at the core of the recent CJEU *Schrems II* decision, which invalidated the EU–US Privacy Shield. These developments suggest that foreign government surveillance will (at least in the near future) remain the main obstacle for the validity of mechanisms of personal data transfers outside the EEA.

According to the CJEU, international agreements can only pass the 'strict necessity' if they:[122]

1. Lay down clear and precise rules governing the scope and application of the measure in question (e.g. the extent to which public authorities of a foreign country can access personal data); and
2. Impose minimum safeguards for transferred personal data, so that the persons whose data has been transferred have sufficient guarantees to protect their personal data against the risk of abuse effectively. This requirement harks back to Article 8(3) of the EU Charter, according to which the establishment of an independent authority supervising the compliance with the fundamental right to the protection of personal data is an essential component of the fundamental right to the protection of personal data.[123]

Conversely, as the CJEU explained in *Schrems I*

> Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use … Likewise, legislation not providing for any possibility for an individual to pursue legal remedies … does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter … The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law.[124]

122 *Schrems I* (n 1) paras 93, 95; Opinion 1/15 (n 1) paras 141, 154, *Schrems II* (n 5) para 176.

123 EU Charter (n 1) art 8(3) as interpreted by the CJEU in Opinion 1/15 (n 1) para 229; *Schrems I* (n 1) para 41.

124 *Schrems I* (n 1) paras 93, 95.

The CJEU factored two other general considerations in its analysis: First, the seriousness of the interference that a particular measure limiting the fundamental rights to privacy and the protection of personal data entails[125] and, second, the importance of the interest pursued by the measure. Concerning the latter factor, recall that the relative importance of competing interests also takes part in the assessment of trade 'necessity.' According to the CJEU, the objective of public security can justify even serious interferences with privacy and data protection, if such measures meet the 'strict necessity test.'[126] (emphasis added) The economic interests of a private party, however, seem to be at the other end of the importance continuum. As the CJEU noted in *Google Spain*, '[i]n the light of the potential seriousness of that interference, it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing.'[127] In the *Satamedia* judgement,[128] that predates the EU Charter by one year, the court took an approach to balancing the right to the protection of personal data against the right to freedom of expression that 'demonstrates that the protection of personal data weighs heavily relative to that part of freedom of expression which falls under 'journalistic purposes'. In other words, the CJEU place[d] greater weight on the protection of personal data than on freedom of expression in this context.'[129] The relatively higher importance of the fundamental right to the protection of personal data, as compared to other fundamental rights, also reveals itself through the aspired level of protection of this right – 'effective and complete,'[130] as pronounced by the CJEU. The requirement of 'complete' protection could make the balancing of this right with other competing fundamental rights challenging and leave suboptimal room for respecting those other rights.[131] To sum up, although, as discussed above, data protection may not be considered of highest importance in international trade law, cross-border

125 EDPS (n 112), 7.

126 Opinion 1/15 (n 1) paras 149, 154.

127 Case C-131/12 (n 100) para 81. Remarkably, in this case the CJEU did not consider the fundamental right to freedom of expression enshrined in art 11 of the EU Charter, but rather limited the balancing assessment to the fundamental rights to privacy and personal data protection on the one hand and the right to conduct business on the other.

128 CJEU, Case C-73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*, ECLI:EU:C:2008:727, para 56.

129 Charlotte B Tranberg, 'Proportionality and Data Protection in the Case Law of the European Court of Justice' (2011) 1(4) IDPL 239, 239–48.

130 See supra n 99.

131 Joris VJ van Hoboken, 'Case Note CJEU 13 May 2014, C-131/12 (*Google Spain*)' (14 September 2014) <https://ssrn.com/abstract=2495580> accessed 22 May 2020.

digital trade is unlikely to weigh heavily against data protection in the EU's fundamental rights calculus. While that is a source of potentially serious and irremediable tension, Section 4 of the article suggests a way out.

3.4 *The Incompatibility of Two 'Necessities'*

Now that both tests have been explicated, one can see that the risk of the tension lies in the fact that neither the EU's trade liberalization commitments in trade in services nor a potential decision of an international trade adjudicating body requiring the EU to reduce the restrictions on cross-border transfers of personal data to comply with such commitments are likely to survive the EU Charter's 'strict necessity' assessment. As a factual matter, totally unrestricted transfers of personal data outside the EEA for purposes of facilitating digital trade do not meet any of the prongs of the EU Charter 'strict necessity test'. Put simply, an adequate degree of restriction on cross-border transfers of personal data is necessary.

To show the polar opposition between the two tests, one could say that, because transfers of personal data outside the EEA amount to a limitation of the fundamental rights to privacy and the protection of personal data, the CJEU's assessment of liberalization of data transfers starts from a question 'whether transfers should be allowed and under what conditions.' In trade law the question is the opposite, namely 'whether transfers should be limited.' Implementing a decision of an international trade adjudicating body requiring the EU to abandon restrictions on transfers of personal data or to lower the standard of 'essential equivalence,' which all the mechanisms for systematic personal data transfers should meet based on the CJEU jurisprudence,[132] would run afoul of the core of the conditions under which the CJEU considers transfers of personal data outside the EEA compliant with the EU Charter. It follows from the CJEU *Schrems II* judgment that, in the context of transfers of personal data outside the EEA, the 'strict necessity test' of article 52(1) of the EU Charter is, in a way, applied to countries of destination outside the EEA in the sense that the level of interference with the fundamental rights to privacy and the protection of personal data in a foreign country must be essentially equivalent to a level of interference inside the EEA that would meet the 'strict necessity test' under the EU Charter.[133] This makes 'essential equivalence' a

132 *Schrems I* (n 1) para 73; Opinion 1/15 (n 1) paras 93, 134; *Schrems II* (n 5) paras 96, 104–05.

133 *Schrems II* (n 5) paras 184–85.

constitutional comparison threshold under the EU Charter, a matter of primary rather than secondary EU law.[134]

Two other core conditions for compliance of a data transfer mechanism with the EU Charter are the existence and effective functioning of an independent supervisory authority and effective administrative and judicial remedies for individuals. All the mechanisms allowing for systematic transfers of personal data outside the EEA meet, to some extent, this condition.[135] The absence of an effective redress mechanisms for individuals was one of the reasons for the invalidation of the EU–US Safe Harbour[136] and the EU–US Privacy Shield[137] by the CJEU. This component of the fundamental right to the protection of personal data alone renders infeasible, under the EU Charter, any approach to data transfers that does not allow for a preliminary assessment of the legal regime in the country of destination or does not require a commitment of a personal data recipient in a foreign country to grant EU individuals certain safeguards. Even if other mechanisms for data transfers are theoretically possible, those mechanisms, if applied horizontally to all types of personal data, would not be less trade restrictive as compared to the ones already envisaged in the GDPR. One way or the other, the personal data importer has to explicitly commit to the essential elements of EU's framework for data protection provided for in Article 8 of the EU Charter.

Before moving to the proposed way forward, let us consider the possibility that the WTO adjudicators would take the CJEU's interpretation of the EU Charter into account when considering whether the EU restrictions on transfers of personal data are 'necessary' and least trade restrictive. In such a case, because, as interpreted by the CJEU, transfers of personal data with restrictions already in place are in compliance with the EU Charter, the EU's framework would be considered least trade restrictive. However, this is unlikely to occur if only because international trade adjudicators are bound neither by EU law nor by CJEU jurisprudence. Their competence is limited to the interpretation and application of international trade agreement by which they are established.[138]

134 As explained in supra Section 3.1, in the hierarchy of EU law, the EU Charter is above the EU's international trade commitments. See supra n 66.

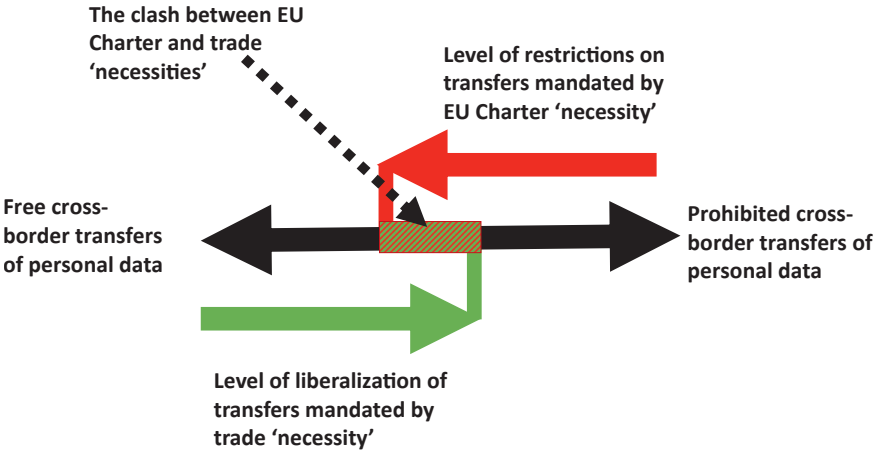
135 eg GDPR (n 2) art 45(2)(b) on adequacy assessment, arts 47(2)(e), 40(4) and 40(2)(k); SCCs (Set I) clause 5(c) and 7(1)(b) for controller to controller transfers (Commission Decision 2001/497/EC); clause V(c) and para 7 of Preamble to Commission Decision 2004/915/EC approving SCCs (Set II) for controller to controller transfers; SCCs clause 5(e) and 7(1)(b) for controller to processor transfers (Commission Decision 2010/87/EU).

136 *Schrems I* (n 1) paras 90, 95.

137 *Schrems II* (n 4) paras 187–89, 197.

138 For a discussion see Yakovleva (n 98) 499–502.

FIGURE 1 Overlap Between the EU Charter and Trade 'Necessities'



SOURCE: Diagram compiled by author.

4 Ways Forward

The discussion in this article has shown that in prior cases concerning the trade-off between the WTO members' autonomy to protect public interests like environment or public health, on the one hand, and trade liberalisation commitments on the other, the trade 'necessity test' has been interpreted restrictively. Too restrictively to accommodate the EU's current approach to cross-border transfers of personal data. At the same time, under the 'strict necessity test' contained in the EU Charter (as interpreted by the CJEU), the regulatory autonomy under EU law to derogate from the protection of the fundamental right to the protection of personal data may be insufficient to comply with the EU's international trade obligations when it comes to cross-border flows of personal data. The sequential application of the two 'necessities' creates an overlap (see Figure 1) where there is a risk that the two 'necessities' may clash putting the EU in a compliance dead-lock between the violation of trade law or unjustifiable derogation from the fundamental right to the protection of personal data, as construed by the CJEU.

From a normative perspective, this state of affairs is not sustainable. The EU should be able to comply with the Charter and its international trade obligations simultaneously. The path forward suggested by this article is guided by three principal considerations. First, from a practical perspective, it is risky to wait until the EU restrictions are struck down by – or even challenged at – an international trade adjudicating body and force the EU's hand. A more

proactive approach seems preferable. Second, and relatedly, ongoing uncertainty surrounding the lawfulness of transfers of personal data outside the EEA, on the one hand, and the compliance with the restrictions on such transfers with EU's international trade commitments, on the other hand, may have a chilling effect on cross-border trade to the detriment of EU businesses. Third, although the approach to cross-border transfers of personal data that would make the most solid contribution to the 'effective and complete' protection of the fundamental right to the protection of personal data is a total ban on such transfers, this rather extreme approach would undermine the very existence of digital cross-border trade with the EU and is thus unwarranted.

From an EU perspective, one way out of the quandary is to negotiate a broader general exception for the protection of personal data in future trade agreements, one that would embrace the EU's restrictions on transfers of personal data. In contrast, the current EU approach of negotiating a more lenient exception for privacy and data protection in a digital trade chapter without aligning it with the general exception may well be, as this article has demonstrated, insufficient to avoid the clash between the two tests and their respective 'necessities.' A single horizontal exception for privacy and data protection, which would apply to all chapters of a trade agreement is a much better option. Instead of a 'necessity test,' such a horizontal exception should have a lower threshold for domestic privacy and data protection framework.

There are precedents for this proposed approach. First, it could be based on more lenient – when compared to 'necessity' – trade law standard, such as 'reasonableness' or the requirement of non-avoidance or non-circumvention of international trade commitments already employed by trade agreements in other contexts, such as the exceptions for data protection and prudential regulation in financial services chapters.[139] Alternatively, it could just use the text of the current, specific exception proposed by the EU but make it truly horizontal. Although the problem lies mostly in the way the trade 'necessity test' is interpreted, WTO members or parties to other trade agreements have little influence over such interpretation. This is why changing the test itself is necessary. Taking into consideration the provisions in post-WTO trade agreements regarding the protection of other non-economic interests (such as the protection of environment, labour rights or sustainable development), the autonomy safeguarded by a broader exception could be reinforced

139 GATS (n 11) art 2(a) of the Annex on Financial Services; WTO Understanding on Commitments in Financial Services (1994) art B.8.

by additional provisions putting the protection of privacy and personal data above or at least on par with digital trade liberalisation.[140]

Another solution would be to make both the EU's rules on transfers of personal data and the general exception for protection of personal data in trade agreements more granular and more compatible with each other. On the EU side, in contrast to the current one-size-fits-all approach to personal data transfers that apply to any personal data, the EU could consider creating different rules for different contexts and categories or groups of personal data. These categories or groups could be differentiated depending on the level of interference with individuals' fundamental rights. The CJEU has already used this benchmarking approach in its assessment of the EU Charter 'necessity' test. Such benchmarking was also suggested by the European Commission in its Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters of 17 April 2018. The Proposal distinguishes between four types of personal data – subscriber information, access data, transactional data, and content data for of transfers of personal data between EU Member States or from outside the EU to an EU Member State in criminal matters. The safeguards that should apply to the transfer of each type of data would thus vary depending on the level of interference with the fundamental rights.[141] A note of caution is in order, however: the transfers envisaged under the above-mentioned proposed regulation are limited to particular criminal investigations and thus, do not include systematic transfers.

To apply this benchmarking approach, one could use the typology suggested by Sen, who proposed a different level of restriction on international transfers of personal data for three categories: company data, business data, and social data.[142] A preliminary analysis, however, suggests that differentiating the level of restrictions on cross-border transfers of data based on this typology may not be consistent with the EU Charter's 'strict necessity' test. Reliance on the type of data alone is not sufficient as a proxy of the level of interference with the fundamental rights to data protection (in other words, the risk to the fundamental rights) associated with the processing of such data.[143] For instance,

140 For examples of such provisions and discussion, see Yakovleva (n 98) 505–07.

141 Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters (17 April 2018) recitals 21, 23, arts 5(3) and 5(4).

142 Sen (n 36) 343–46.

143 Article 29 Working Party, 'Guidelines on Personal Data Breach Notification Under Regulation 2016/679, WP250' (3 October 2017) 21; Article 29 Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679, WP248' (4 April 2017) 7–9.

while the content of a person's email box may not include any sensitive data in a strict sense, overall it may provide a clear idea of the owner's private life thus requiring more protection than data of the same type in general. Therefore, other factors, such as geographical coverage and volume of data, types of individuals concerned (e.g. vulnerable individuals or children), and data protection safeguards, such as pseudonymization, should also play a role in the assessment.

The most optimal, in this article's view, way to introduce granularity into the EU's framework for transfers of personal data outside the EEA is a risk-based approach, as it would fit organically into the logic of the GDPR and the EU Charter. Such a risk-based approach has already been implemented[144] in the GDPR in relation to some data protection elements explicitly or implicitly envisaged in Article 8 of the Charter, such as legitimate interest as a legal ground for processing of personal data,[145] stricter rules for processing special categories of personal data,[146] the principle of accountability,[147] records of processing activities,[148] data breach notification requirement,[149] security of processing,[150] prior consultation with a data protection authority,[151] and data protection impact assessment.[152] This strongly suggests that a risk-based approach to data transfers is feasible. For example, safeguards required for transfers of personal data could be differentiated depending on the remoteness of link between personal data and individuals to which it relates. Along

144 It is, however, worth keeping in mind that the implementation of the risk-based approach in the GDPR is incomplete and is, arguably, in tension with the rights of the data subject envisaged in GDPR (n 2) ch 3 (see Claudia Quelle, 'The "Risk Revolution" in EU Data Protection Law: We Can't Have Our Cake and Eat It, Too' (2017) Tilburg Law School Legal Studies Research Paper Series No 17/2017 1, 20–21).

145 In its pre-GDPR but post EU Charter Opinion 06/2014, Article 29 Working Party explicitly suggests to use the terminology and methodology of traditional risk assessment as a helpful tool to assess the impact of data processing on the individual (see Article 29 Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC, WP 217' (9 April 2014) 37–38). Similarly, in its GDPR guidance on the application of legitimate interest, the UK Information Commissioner's Office (ICO) equates the legitimate interest assessment with a light-touch risk assessment based on the specific context and circumstances (ICO, 'Legitimate Interests' <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests-1-0.pdf> accessed 22 May 2020).

146 GDPR (n 2) art 9, recital 51.

147 ibid art 24, recitals 74–77.

148 ibid art 30(5), recital 82.

149 ibid arts 33–34, recitals 85–88.

150 ibid art 32, recital 83.

151 ibid art 36, recitals 94–96.

152 ibid art 35, recitals 84, 89, 90–93, 95.

those lines, more lenient transfer rules could be designed for data that has only a remote link with individuals, such as pseudonymized data, when such data is transferred without additional information necessary to link the data to particular individuals. By definition, pseudonymized data cannot be attributed to a specific individual without the use of additional information, if such information is kept separately and adequately protected.[153] Recital 28 of the preamble to the GDPR explicitly states that the 'application of pseudonymisation to personal data can reduce the risks to the data subjects concerned.'

As noted by both experts in the field and European Data Protection authorities, the GDPR already provides for more lenient rules for pseudonymized data when it comes to the rights of individuals, data breach notification requirement, and possibilities of using the data for purposes other than that for which it was originally collected.[154] Relaxation of these data protection principles, two of which are explicitly mentioned in Article 8 of the EU Charter, in relation to pseudonymized data suggests that a lighter touch regulatory approach to transfers of such data outside the EEA could be EU Charter and GDPR compliant. Another way to differentiate between different strings of data transfers is by sector. For example, as one of the measures to increase availability of data for businesses, the European Commission has recently proposed to develop sectoral data spaces within the EU in strategic areas, such as manufacturing, agriculture, health and mobility.[155] This line of thinking could also be explored for transfers of personal data outside the EEA.

On the international trade law side, a more nuanced approach to transfers of personal data could be translated into different balancing tests incorporated into international trade agreements. Each of the balancing tests would reflect different degrees of a regulatory autonomy to protect personal data according to the level of interference into fundamental rights that the processing

153 ibid art 4(5).

154 ibid recitals 29, 50 and 156; ibid arts 6(4), 11(1), 12(2), 14(5)(b); Article 29 Working Party, 'Guidelines on Transparency Under Regulation 2016/679, WP260 rev.1' (11 April 2018) 31; Article 29 Working Party, 'Personal Data Breach Notification' (n 143) 15–16, 21; Axel Arnbak, 'Pseudonymisation: Big Data Opportunities in the GDPR' (De Brauw Blackstone Westbroek, 23 October 2018) <www.debrauw.com/newsletter/pseudonymisation-big-data-opportunities-in-the-gdpr/>; Niall McCreanor, 'Pseudonymisation Is the GDPR's "Escape Hatch"' (*IT Governance blog*, 14 May 2018) <www.itgovernance.eu/blog/en/pseudonymisation-is-the-gdprs-escape-hatch>; Gabe Maldoff, 'Top 10 Operational Impacts of the GDPR: Part 8 – Pseudonymization' (IAPP, 12 February 2016) <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/> all accessed 22 May 2020.

155 European Commission, 'A European Strategy for Data' (19 February 2020) COM(2020) 66 final, 6 <https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf> accessed 22 May 2020.

of different categories or groups of personal data entails. The strictness of the trade law threshold for domestic data protection would be proportionate to the magnitude of the risk of interference with fundamental rights to privacy and the protection of personal data. In short, a more lenient test would cover situations where the risk is lower, a more stringent test – when the risk is higher, thus mirroring the granular framework for data transfers in EU law proposed in the previous paragraph. This approach would be aligned with the existing body of international trade law: WTO law already provides for several balancing mechanisms allowing for different degrees of national autonomy to regulate depending on the policy interest at stake and the type of trade agreement. For example, in addition to 'necessity,' WTO trade agreements already contain more lenient balancing mechanisms, such as the requirement mentioned above of reasonableness, non-avoidance or non-circumvention of international trade commitments or the subjective 'it considers necessary' test in the national security exceptions.[156]

5 Conclusion

The pivotal role of personal and other data in the global digital economy intensifies the tension between trade liberalisation commitments and the individual rights to privacy and personal data protection. In the EU, where these rights are binding fundamental rights – this tension could result in a catch-22 situation where the EU would have to choose between adhering to its own constitutional framework and fulfilling its trade obligations. This risk of a compliance deadlock is due to the incompatibility of the exceptions – and, more specifically, the 'necessity tests' lying at their core – that the EU law and international trade agreements have designed to prevent the clash between each others' bodies of rules. The article has argued that to prevent this risk from materialising, a reform of the international trade exception for privacy and data protection and/or the EU's framework for transfers of personal data is necessary and should reflrect a risk-based approach.

156 eg GATT art XXI; GATS art XIV*bis*.