INSIGHT

The Issue of Data Protection in EU Trade Commitments: Cross-border Data Transfers in GATS and Bilateral Free Trade Agreements

Federica Velli*

Abstract: The rapid technological developments and the increasing data flows have not yet been addressed through global coordination. The WTO has so far played a minor role, failing to update its treaties to the new reality of digital trade. To reduce the uncertainty as to the economic and privacy-related impacts of cross-border data flows, governments as well as the European Union have started including this topic and data protection concerns in Free Trade Agreements. This *Insight* will first investigate how the General Data Protection Regulation rules on the transfer of personal data might conflict with GATS' main commitments, and then consider how the EU has addressed data protection in the context of Free Trade Agreements.

Keywords: General Data Protection Regulation – General Agreement on Trade in Services – free trade agreements – cross-border personal data transfers – adequacy decisions – fundamental right to data protection.

I. Introduction

In recent years the EU has made data protection and free trade two of its significant spheres of action. The year 2016 represents well this double interest in both areas with the adoption of the General Data Protection Regulation (GDPR), on the one hand, and the signature of the Comprehensive Economic Trade Agreement (CETA),[1] on the other hand. The interdependence of trade and data protection has become more prominent

* Student research assistant, The Hague University of Applied Sciences (THUAS), f.velli@student.hhs.nl. The Author wishes to thank Dr. Luca Pantaleo for his valuable comments and assistance and the two anonymous reviewers for their constructive insights. Any mistakes remain those of the Author.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR); Comprehensive Economic Trade Agreement (CETA) of 30 October 2016 between Canada, of the one part and the European Union and its Member States, www.ec.europa.eu.

ISSN 2499-8249
doi: 10.15166/2499-8249/325

due to the rise of digital services, to the point where processing personal data is an indispensable aspect of providing market competitive services.[2] Let us just think about using our smartphones to purchase items online or receiving tailored advertisement via e-mail. Personal data are continuously collected, processed, and stored.

The GDPR succeeded to Directive 95/46/EC (DPD) and is currently one of the most important developments in EU data protection law.[3] It provides uniform data protection rules for all Member States, focusing on the safeguard of the fundamental rights of privacy and data protection, and codifying more individual rights, such as the right to be forgotten.[4] How does this new paradigm reconcile with the interests of the EU to promote free trade in order to strengthen its position as one of the most influential trading actors in the world? Can the adoption of the GDPR constitute an infringement of EU trade commitments in GATS, and how is this tension addressed in EU free trade agreements (FTAs)?

This *Insight* is an attempt to provide an answer (at least a partial one) to these questions, looking at the different approaches taken by GATS and EU FTAs to balance trade and data protection interests in cross-border data transfers, and reflecting on their implications for upholding the fundamental right to data protection embodied in the GDPR.

II. Cross-border data transfers in the GDPR

Chapter 5 of the GDPR begins with a general prohibition to transfer data to third countries to then outline a hierarchy of exclusions.[5] The main exclusions enabling controllers or processors to transfer data are three, namely: a) through an adequacy decision adopted by the European Commission (Art. 45 GDPR), b) transfers subject to appropriate safeguards (Art. 46 GDPR), or c) derogations for specific situations (Art. 49 GDPR).[6]

Starting with a) above, – which can be considered the most straightforward option – Art. 45 establishes a mechanism according to which the Commission can adopt a decision called “adequacy decision". With such an assessment, the transfer of personal data

[2] GDPR, cit., Recital 101: “flows of personal data to and from countries outside the Union and international organizations are necessary for the expansion of international trade and international cooperation”.

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[4] GDPR, cit., Art. 17; S. Yakovleva, K. Irion, M. Bartl, *Trade and Privacy: Complicated Bedfellows? How to Achieve Data Protection-proof Free Trade Agreements*, Amsterdam: Institute for Information Law (IViR), 2016, p. 5; for more information on the rights of data subjects see P. Voigt, A. Von Dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Cham: Springer, 2017, pp.141-184.

[5] GDPR, cit., Art. 44.

[6] For more information see M. Krzysztofek, *GDPR: General Data Protection Regulation EU 2016/679: Post-reform Personal Data Protection in the European Union*, Alphen aan den Rijn: Kluwer Law International, 2018, p. 233 *et seq.*

of individuals from the EU to a specific third country is allowed in a general manner because the country in question has a level of data protection that is essentially equivalent to that guaranteed by the EU.[7]

A second possibility to transfer personal data is provided for by Art. 46 GDPR, which mandates the use of appropriate safeguards, such as legally binding and enforceable instruments between public authorities or bodies, binding corporate rules, the standard data protection clauses approved by the Commission, or an approved code of conduct or certification mechanism.[8] Other safeguards such as contractual clauses drawn up by the parties, or provisions in administrative arrangements can also be considered appropriate safeguards but only after being validated by competent supervisory authorities.[9]

Lastly, derogations for specific situations are listed in Art. 49 GDPR. This provision enables personal data transfers to a third country that does not offer adequate protection nor any of the measures under Art. 46 GDPR under specific circumstances.[10]

Although these three options could already be recognised in Arts 25 and 26 of the DPD, the GDPR has made the greatest changes in Art. 45. It refined adequacy decisions, specifying the factors that the Commission shall take into consideration to make an equivalent protection assessment, such as the rights of data subjects and the obligations for data processors or controllers, the presence of independent supervisory bodies as well as of efficient enforcement mechanisms for data protection rights.[11] In addition, Arts 45, paras 3 and 4, GDPR provide that a periodic review must take place at least every four years, with the Commission having a strong supervisory role in tracking developments occurring in third countries. In spite of these and other updates, adequacy decisions have continued to attract the attention and scrutiny of scholars, in particular in regard to the effects of these decisions on international trade.[12]

[7] Art. 29 Data Protection Working Party, *Adequacy Referential,* WPS 254 rev.01, 2018, p. 3; Court of Justice, judgment of December 2015, case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, para. 73.

[8] GDPR, cit., Art. 46, para 2,let. a)-f).

[9] *Ibid.*, Art. 46, para. 3; See M. KRZYSZTOFEK, *GDPR: General Data Protection Regulation EU 2016/679*, cit., p. 241.

[10] The most notable derogation of Art. 49 is the explicit consent of a data subject to a proposed data transfer after being informed of its possible risks in para. (a)

[11] GDPR, cit., Art. 45, para 2, let. a)-c), and recital 104,

[12] See among others A. MATTOO, J.P. MELTZER, *International Data Flows and Privacy: The Conflict and Its Resolution*, in *Journal of International Economic Law*, 2018, p. 781; G.M. RUOTOLO, *The EU Data Protection Regime and the Multilateral Trading System: Where Dream and Day Unite*, in *Questions of International Law*, 31 May 2018, www.qil-qdi.org, p. 26.

III. The regime under GATS: MFN, NT and market access vs. adequacy decisions

III.1. GATS, MFN, NT and market access obligations

The WTO has failed to update its treaties to the new reality of digital trade and there is currently no global framework to regulate cross-border data flows.[13] WTO Members have not addressed what constitutes a legitimate regulation of cross-border transfers of data and have not categorized what can be trade distorting.[14] Nonetheless, the WTO Dispute Settlement Body concluded that WTO rules apply to digital services.[15] The WTO has several agreements that implicitly relate to digital trade.[16] However, as has been pointed out, these instruments do not take into consideration the different types of data nor encompass the landscape of new services created by the Internet.[17] In the following pages, an analysis of the compatibility of adequacy decisions with GATS' three core commitments will be carried out, starting from the Most-Favoured-Nation Treatment (MFN) obligation. The two options envisaged in the GDPR –namely, when a country is granted an adequacy decision or sectoral scheme – will be explored.

a) Adoption of adequacy decisions.

Determining whether the adoption of adequacy decisions only for some countries could breach the EU's MFN obligation entails proving the likeness of two or more services and service suppliers, and the existence of a less favourable treatment which modifies the conditions of competition in favour of the services of one Member com-

[13] The WTO Working Programme on Electronic Commerce concluded that "the electronic delivery of services falls within the scope of the GATS". See Council for Trade in Services, Work Programme on Electronic commerce: interim report to the General Council S/C/8 of 31 March 1999. Disagreements between Members left classification issues unresolved, reducing the progress of the programme which did not result in any concrete measure aside from the extension of the "e-commerce moratorium". Panels and the Appellate Body have been taking a dynamic interpretative approach, effectively deciding some controversial issues, see WTO DSB, Appellate Body report of 21 December 2009, case no. ds363, *United States v. China, China-Publications and Audiovisual Products*, paras. 363-365; See M. Burri, *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation*, in *UC Davis Law Review*, 2017, p. 93 *et seq.*; A. Porges, A. Enders, *Data Moving Across Borders: The Future of Digital Trade Policy*, in *E15Initiative International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum*, 2016.

[14] S.A. Aaronson, P. Leblond, *Another Digital Divide: The Rise of Data Realms and its Implications for the WTO*, in *Journal of International Economic Law*, 2018, p. 246.

[15] *Ibid.*; WTO DSB, Appellate Body report of 7 April 2005, case no. ds285, *Antigua and Barbuda v. United States, US-Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, para.6.370; *United States v. China*, cit., paras 363-365.

[16] Among others see WTO, *Ministerial Declaration on Trade in Information Technology Products* of 13 December 1996.

[17] S.A. Aaronson, P. Leblond, *Another Digital Divide*, cit., p. 251.

pared to any other.[18] As affirmed in *EC- Bananas III*, a violation can include both *de jure* or *de facto* differential treatment.[19] Due to the lack of existing case law on online services, it is yet uncertain how the issue of likeness will be addressed. In this context, Yankovleva, Irion and Bartl refer to the phenomenon of "privacy paradox" in business to consumer transactions as one way of highlighting how higher data protection standards might not necessarily influence consumers' choice.[20] Concerning a less favourable treatment, providers operating under an adequacy decision are in an advantageous position because they can benefit of an automatic and virtually unlimited right to transfer data from and to the EU, unlike services and service suppliers from third countries that do not obtain such a decision. Therefore, even though not facially discriminatory, the mechanism of adequacy decisions may give rise to a *prima facie* preferential treatment for countries which fulfil the requirement of an essentially equivalent level of data protection. Hence, provided the analysis of the WTO adjudicating bodies, adequacy decisions could be found in violation of the EU's MFN commitment.[21]

Next to a finding of adequacy, the DPD provided that if a country was found to lack an adequate level of protection after an assessment of the Commission, Member States had "to prevent any transfer of data of the same type to the third country in question".[22] Therefore, arguably service suppliers from a country with poor data protection standards not yet found inadequate could have continued to process data according to other safeguards, while this was not possible after a finding of "inadequacy".[23] This situation is no longer present in the GDPR, which explicitly states that a decision under Art. 45 is without prejudice to the possibility to transfer data according to Arts 46 to 49 GDPR.[24]

b) Adoption of sectoral schemes.

A differential treatment might also be observed when some countries are able to negotiate a sectoral scheme for personal data flows with the Commission while others

[18] Art. II:1 GATS; WTO DSB, Panel Report of 30 September 2015, case no. ds453, *Panama v. Argentina, Argentina-Measures Relating to Trade in Goods and Services,* paras 7.147-7.149.

[19] WTO DSB, Appellate Body Report of 25 September 1997, case no. ds27, *Ecuador, Guatemala Honduras Mexico United State v. European Communities*, *EC-Regime for the Importation, Sale and Distribution of Bananas*, paras 229-234; See also WTO DSB, Panel Report of 22 May 1997, case no. ds27, *Ecuador, Guatemala Honduras, Mexico and United States v. European Communities*, *EC-Regime for the Importation, Sale and Distribution of Bananas*, paras 7.349, 7.384, 7.396; Both the Panel and the Appellate Body found a violation of Art. II GATS based on the *de facto* asymmetric effect of origin-neural provisions.

[20] S. YAKOVLEVA, K. IRION, M. BARTL, *Trade and Privacy*, cit., p. 29.

[21] Panel Report *Ecuador, Guatemala Honduras, Mexico and United States v. European Communities*, cit., paras 7.349-7.353; Appellate Body Report *Panama v. Argentina*, cit., paras 6.5-6.8.

[22] DPD, cit., Art. 25, para. 4.

[23] *Ibid.*; C.L. REYES, *WTO-Compliant Protection of Fundamental Rights*, cit., p. 156-157.

[24] GDPR,cot., Art. 45, para. 7.

are not.[25] Under Art. 45, para. 3, GDPR the Commission has the power to approve sectoral schemes with a third country considering the same elements of adequacy decisions, in order to regulate the transfer of personal data only in certain sectors of industry. It has been argued that this instrument entails a more "lenient treatment" with respect to third countries which had to undergo a "full" assessment.[26] Furthermore, the Commission might decide to conclude a sectoral agreement with a third country lacking adequate data protection in one or more sectors, but not with equally "inadequate" countries. Once adopted, the agreement can have the same effect of an adequacy decision in that it could lead to the same discriminatory effect, although limited to the specified sectors concerned.

The piecemeal approach to the adoption of adequacy decisions and sectoral schemes might also have negative implications in regards to Art. VI GATS on domestic regulation focused on the reasonable, objective, and impartial administration of measures of general application.[27]

As regards National Treatment (NT), Art. XVII:1 GATS prohibits less favourable treatment to services and service suppliers of any other Member in respect to that accorded to national like services and service suppliers.[28] In line with the GDPR, third countries can be grouped in two main categories, those with and those without an adequacy decision. In the first case, once the essential equivalence with the EU data protection regime is established, a third country is provided with the authorization to transfer, process and control data collected in the EU. Yet, while EU suppliers are inherently adequate as they comply with the entirety of the GDPR, only 13 third countries were granted an adequacy decision or a sectoral agreement, leaving the vast majority of non-EU countries outside of this scheme.[29] Even though this reinforces the case for an unfavourable treatment among third countries under the MFN provision, it also underlines that the system of essential equivalence creates a wide opportunity gap between EU and third country suppliers, which has been argued to modify "the conditions of competition in favour of services based in EU/EEA".[30] Without an adequacy decision, third country suppliers will need to further their data protection standards introducing appropriate safeguards according to Art. 46, para. 2, which could be subject to prior authorisation from national authorities.[31] Here too, the analysis of the WTO dispute set-

[25] See among others C.L. REYES, *WTO-Compliant Protection of Fundamental Rights*, cit., p. 155; A. MATTOO, J.P. MELTZER, *International Data Flows and Privacy*, cit., p. 781.

[26] S. YAKOVLEVA, K. IRION, *The Best of Both Worlds? Free Trade in Services, and EU Law on Privacy and Data Protection*, in *European Data Protection Law Review*, 2016, p. 20.

[27] Art. VI GATS; C.L. REYES, *WTO-Compliant Protection of Fundamental Rights*, cit., p. 160 *et seq*.

[28] Art. XVII GATS.

[29] European Commission, *Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection*, ec.europa.eu.

[30] S. YAKOVLEVA, K. IRION, M. BARTL, *Trade and Privacy*, cit., pp. 32-33.

[31] GDPR, cit., Art. 46, para. 3; G.M. RUOTOLO, *The EU Data Protection Regime*, cit., p. 27.

tlement body will determine on a case-by-case basis whether services or service suppliers are "like" in the first place, and whether a *de facto* differential treatment affects negatively the conditions of competition for non-EU suppliers.

With respect to market access, each WTO Member is committed to providing services and service suppliers of any other Member treatment no less favourable than that specified in the conditions in its Schedule of Commitments for each mode of supply.[32] In the case *US-Gambling*, the WTO adjudicating bodies interpreted the ban on the remote supply of online gambling services as a breach of market access as it amounted to a zero quota.[33] It has been argued that in the application of the GDPR there is no risk of an analogous finding because the regulation provides for other possibilities for authorized data transfers to countries which do not meet the adequacy criterion.[34] However, following this reasoning, the only situation that could result in such an automatic market restriction would be if there were a full suspension of the rules on the transfer of personal data to a third country. This has never happened in practice so far, not even after the annulment of Safe Harbour,[35] but an interruption of data transfers might amount to a market access restriction contrary to Art. XVI:1 GATS and to a zero quota under Art. XVI:2, let. a) and c), GATS.[36]

III.2. Justifications

When a measure is found to violate one or several of the GATS commitments, it can still be saved based on a number of justifications. In the case of the GDPR, Arts V and XIV GATS represent two possible defences.

Art. V GATS allows WTO Members to enter in preferential trade agreements, which further liberalise trade and afford deeper economic integration in comparison to other WTO Members. This Art. can be used to justify entering into an agreement otherwise GATS-inconsistent if this fulfils "internal" and "external" conditions.[37] The first refer to the extent that an agreement liberalises trade in services in terms of sectoral coverage and removal of discrimination.[38] The second condition, instead, is concerned with the WTO Members not parties to the arrangement, and requires that they will not suffer a higher "overall level of barriers to trade in services" as a result of it.[39]

[32] Art. XVI:1, GATS.

[33] *Antigua and Barbuda v. United States*, cit., paras 238, 251-252

[34] S. Yakovleva, K. Irion, *The Best of Both Worlds?*, cit., p. 22.

[35] More information on Safe Harbour and Privacy Shied F. Terpan, *EU-US Data Transfer from Safe Harbour to Privacy Shield: Back to Square One?,* in *European Papers,* 2018, Vol. 3, No 3 www.europeanpapers.eu, p. 1 *et seq.*

[36] S. Yakovleva, K. Irion, M. Bartl, *Trade and Privacy*, cit., p. 32.

[37] Arts V:1 and V:4 GATS.

[38] *Ibid.*, Art. V:1, let. a) and b).

[39] *Ibid.* Art. V:4.

The GDPR is a directly applicable regulation which unifies Member States' laws and allows for the free flow of personal data within the internal market, answering to the internal features provided in Art. V:1 GATS. In addition, a case can be made advocating for the dependency on chapter 5 GDPR to preserve compliance with the regulatory regime for the flow of data within the internal market, as well as for maintaining analogous high data protection standards when data from the EU are transferred and processed in third countries.[40] Looking at the external condition of Art. V GATS, the GDPR does not aim to restrict cross-border data transfers with third states, but complying with its rules creates additional obligations for non-EU providers. Therefore, Art. V GATS could be deemed a first justification in case of a breach of the MFN obligation, but it yet lacks an essential interpretation of its clauses including V:4 to make a definitive assessment.[41] Indeed, the term "trade barriers" and the extent of the economic disadvantage of non-members will be crucial determinations to uphold or reject a justification on Art. V GATS.

Concerning Art. XIV GATS, this provides for a general exception clause which enables parties to deviate from their commitments under GATS to comply with national laws and regulations, including those aimed at the protection of individuals' privacy.[42] The literature expresses an overall unpredictability when WTO adjudicating bodies apply Art. XIV GATS and similarly Art. XX GATT, due to the difficulty for a respondent to meet their requirements.[43] To be justified, a measure must comply with a two-tier test consisting of first, whether it falls within the scope of one of the exceptions outlined in the Art.; and second, whether it meets the requirements of the chapeau.[44] The Appellate Body established that for a measure to be found provisionally justified under Art. XIV, let. c), it should have been designed to ensure compliance with national laws and regulations which are not inconsistent with GATS, and that it is necessary to achieve a

[40] S. YAKOVLEVA, K. IRION, M. BARTL, *Trade and Privacy*, cit., p. 33-34.

[41] The Panel and Appellate Body have yet to address whether a similar reading to GATT XXIV:5, let. a), would be applied to GATS V:4 or if the Article will be interpreted independently. For the application of Art. XXIV GATT see WTO DSB, Report of the Appellate Body of 22 October 1999, case no. ds34, *India v. Turkey*, *Turkey - Restrictions on Imports of Textile and Clothing Products*, para. 48 *et seq.*

[42] Art. XIV, let. c)(ii), GATS.

[43] S. YAKOVLEVA, K. IRION, M. BARTL, *Trade and Privacy*, cit., p. 34, cites the 2015 research of the organisation Public Citizen stating that the general exceptions in GATT art. XX and GATS XIV were satisfied only in one of 40 cases www.citizen.org, p. 2, referring to WTO DSB, Appellate Body report of 12 March 2001, case no. ds135, *Canada v. European Communities, EC- Asbestos*, paras 174-175,192, let. f). The Appellate Body also reversed the Panel's and upheld a justification based on GATT XX, let. g), in WTO DSB, Appellate Body report of 22 October 2001, case no. ds58, *Recourse to Art. 21.5 DSU by Malaysia* in *India, Malaysia, Pakistan and Thailand v. United States, US-Shrimp*. See among others M. BURRI, *The Governance of Data and Data Flows*, cit., p. 91; G. GREENLEAF, *Free Trade Agreements and Data Privacy: Future Perils of Faustian Bargains?* in D.J.B. SVANTESSON, D. KLOZA (eds.), *Transatlantic Data Privacy Relationships as a Challenge for Democracy*, Cambridge: Intersentia Ltd, 2017, p. 185 *et seq*.

[44] *Antigua and Barbuda v. United States*, cit., para. 292.

certain level of enforcement compared to alternative measures.[45] At first scrutiny, Arts 45, 46 and 49 GDPR seem to be within the scope of Art. XIV, let. c), given that they aim at securing compliance with EU data protection standards and are not *per se* inconsistent with GATS. A deeper analysis needs to be done in regards to the last part of the test, namely the necessity of the provisions to comply with the EU data protection regime including their trade restrictiveness. For example, the GDPR might face an argument about existing alternatives focused on the principle of accountability employed in Canada and in the Asia-Pacific Economic Community.[46]

Furthermore, according to the chapeau of this Art. a measure should not be inconsistent or qualify as arbitrary or unjustifiable discrimination between countries.[47] A case could be made concerning the very need of adopting adequacy decisions, their potentially arbitrary nature, as well as the sectoral agreements. For instance, the choice to stipulate agreements such as Privacy Shield with some countries instead of others might not pass the test and be seen as an unjustifiable discrimination.[48] Thus, in a hypothetical dispute, WTO adjudicating bodies will have to undertake an extensive and important balancing exercise between the policy considerations at the basis of the protection of individual rights, and those for unrestrained international trade.

To summarise, neither Art. V nor Art. XIV GATS seem to provide steady justifications for the GDPR's rules on cross-border data transfers, and their suitability to justify a departure from GATS' main obligations largely relies on the interpretation of the WTO adjudicating bodies. The following section elaborates on data protection in the context of FTAs, increasingly used to negotiate trade relations and where parties see the opportunity to regulate cross-border data flows.

IV. How do bilateral FTAs address trade and privacy interests?

FTAs have been gaining ground on the international trade scene at the expenses of the multilateral trading system. At the time of writing, the EU is engaged with over 20 countries either in pending bilateral negotiations or awaiting the adoption of FTAs.[49] Among

[45] *Panama v. Argentina*, cit., para. 6.202, referring to WTO DSB, Appellate Body Report of 11 December 2000, case no. ds161, *United States v. Republic of Korea*, *Korea- Various Measures on Beef*, para. 157; P. Van Den Bossche, D. Prevost, *Essentials of WTO Law*, Cambridge: Cambridge University Press, 2016, p. 108 *et seq.*

[46] S. Yakovleva, K. Irion, *The Best of Both Worlds?*, cit., p. 25; A. Mattoo, J.P. Meltzer, *International Data Flows and Privacy*, cit., pp. 784-785.

[47] P. Van Den Bossche, D. Prevost, *Essentials of WTO Law*, cit., p. 110.

[48] WTO Panel Report of 10 November 2004, case no. ds285, *Antigua and Barbuda v. United States*, *US-Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, para. 6.584 stating that the absence of consistency may lead to a conclusion of arbitrary and unjustifiable discrimination; S. Yakovleva, K. Irion, *The Best of Both Worlds?*, cit., p. 25.

[49] European Commission, *Overview of FTA and other Trade Negotiations. Update May 2019,* trade.ec.europa.eu.

others, its most recent agreements include an FTA with Japan and the conclusion of an agreement with the four founding members of Mercosur.[50]

FTAs make several separate references to data protection in areas such as financial services, telecommunications, and electronic commerce, as the cross-border transfer of data is liked to a multitude of services. Taking a bird's eye view, the EU moved beyond a more classic "negative" approach in GATS, rooted on exceptions, and leans towards a "positive" approach, calling on the parties to maintain adequate data protection measures. The following paragraphs will provide three examples which illustrate how this has been done in practice in bilateral FTAs, and later give some thoughts on a standalone data protection clause proposed by the Commission for future trade and investment agreements. The examples below do not offer a comprehensive analysis of all data protection references in EU FTAs but strive to sketch some of the main recent developments.

IV.1. Examples from EUKOR, CETA and EU-Japan FTA

The free trade agreement with South Korea signed in 2010 states the following concerning the protection of personal data in financial services: "Each Party, reaffirming its commitment to protect fundamental rights and freedom of individuals, shall adopt adequate safeguards to the protection of privacy, in particular with regard to the transfer of personal data".[51]

Paragraph (b) lays down an obligation to protect personal data without this being an exception to the previous paragraph. As Bendiek and Schmieg note, this gives new force to develop adequate safeguards in the first place, stressing their need rather than being a policy interest subordinate to other provisions as in GATS.[52] One pitfall of this formulation is however that each party is responsible for the protection of personal data, which can result in a hardly monitorable and enforceable data protection safeguard.[53]

Six years later, CETA builds upon the previous formulation for protecting personal data with this Art.: "Each Party shall maintain adequate safeguards to protect privacy, in particular with regard to the transfer of personal information. If the transfer of financial information involves personal information, such transfers should be in accordance with

[50] Decision (EU) 2018/1907 of the Council of 20 December 2018 on the conclusion of the Agreement between the European Union and Japan for an Economic Partnership; Commission, *New EU-Mercosur trade agreement – The agreement in principle* of 1 July 2019, trade.ec.europa.eu.

[51] Decision 2011/265/EU of the Council of 16 September 2010 on the signing, on behalf of the European Union, and provisional application of the Free Trade Agreement between the European Union and its Member States, of the one part, and the Republic of Korea, of the other part, Ch. 7 Sub-section E Art. 7.43, let. b).

[52] A. Bendiek, E. Schmeig, *European Union Data Protection and External Trade. Having the Best of Both Worlds?*, in *German Institute for International and Security Affairs SPW Comments*, no. 11, 2016, p. 3.

[53] A. Wessels, *Broken Data Protection in EU trade agreements* in FFII Blog, 22 September 2016, blog.ffii.org, p. 5.

the legislation governing the protection of personal information of the territory of the Party where the transfer has originated".[54]

Following an obligation to maintain adequate privacy standards, this clause presents an additional element, namely that transfers of personal data should be governed by the law of the party where the transfer originated. This strives to secure the data protection standards of the country of origin, although it does not confer a right on the parties to take unilateral action to protect personal data. Rather than being a carve-out provision, the second sentence could possibly offer interpretational guidance on the words "adequate safeguards" from the sentence above.[55] While with an adequacy decision a transfer of personal data would take place on an even level between parties with essentially equivalent data protection measures, under Arts 46 and 49 further requirements will need to be fulfilled by the third country processor or controller. As a consequence, even though adequacy decisions are not dependent on the free trade agreement, they can be essential for liberalising data transfers by shortening requirements, time, and costs.

A different outlook was taken in the EU-Japan FTA with the following Art.: "Nothing in paragraph 1 restricts the right of a Party to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as that right is not used to circumvent Sections B to D and this Sub-Section".[56]

Although the negative approach recalls Art. XIV GATS, the main focus is here shifted on the right to the protection of personal data, rather than on an undue restriction to trade that can be justified by other regulatory goals. Departing from the previous two examples, Art. 8.36 EU-Japan FTA gives a unilateral right to adopt data protection measures to both parties conditional to not circumventing some sections of the agreement.[57] What still remains uncertain is whether the scope of this Art. is sufficiently broad to encompass all facets of the GDPR's implementation without being considered an attempt to circumvent the agreement.

Aiming to address the shortcomings of data protection clauses such as the ones described, European Commission has presented an alternative for future FTAs which will be described next.

[54] CETA, cit., Ch. 13, Art. 13.15, para. 2.

[55] A.WESSELS, *Broken Data Protection in EU Trade Agreements*, cit., p. 8.

[56] Council Decision (EU) 2018/1907 of 20 December 2018 on the conclusion of the Agreement between the European Union and Japan for an Economic Partnership, Ch. 8, sub-section 5, Art. 8.63.

[57] Investment liberalisation, Cross-border trade in services, Entry and temporary stay of natural persons, and the sub-section on Financial services.

IV.2. Provisions on Cross-border Data Flows and the Protection of Personal Data and Privacy (2018)

A completely new and audacious approach to cross-border data transfers has recently been negotiated in EU FTAs. This innovative formulation has already been introduced in the negotiations with Indonesia and has also been proposed in the negotiations with Australia, with some modifications.[58]

The provisions on the topic of data transfers address cross-border data flows, data protection, and regulatory cooperation and, unlike EURKOR or CETA, are horizontal in nature covering all economic sectors.[59] Art. 2 on data protection states the following:

> "1. Each Party recognises that the protection of personal data and privacy is a fundamental right [...]
> 2. *Each Party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data. Nothing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards*.
> 3. [...]
> 4. For the purposes of this agreement, "personal data" means any information relating to an identified or identifiable natural person.
> 5. For greater certainty, the Investment Court System does not apply to the provisions in Articles 1 and 2." (emphasis added)

This Article fills some of the gaps left open by the previous attempts. Significantly, it rests on the parties' common understanding of data protection as a fundamental right and defines personal data broadly, in order to encompass potential differences between the parties and include a vast range of circumstances. In addition, both parties are empowered with the right to unilaterally take action to maintain and establish data protection safeguards in para. 2. From an EU point of view, this could also include the choice of adopting or revoking an adequacy decision. Lastly in paragraph 5, mention is made to the investment court system (ICS) which will exclude from its scope the fundamental right to privacy and the parties' possibility to adopt data protection measures.[60]

[58] European Commission, *Explanatory note*, 5th Round of Trade Negotiations between the European Union and Indonesia trade.ec.europa.eu. The proposal on the protection of personal data in the EU- Australia FTA does not refer to ICS. European Commission, *EU-Australia proposal on digital trade*, trade.ec.europa.eu.

[59] EU Proposal for Provisions on Cross-border data Flows and Protection of Personal Data and Privacy, trade.ec.europa.eu, Arts 1, 2, X.

[60] ICS is a permanent tribunal for investor dispute settlement replacing and addressing some of the deficiencies of investor-to-state dispute settlement (ISDS). The CJEU has recently confirmed the compatibility of ICS with EU law, in Court of Justice, opinion 1/17 of 30 April 2019. See on ICS L. Pantaleo, *The Participation of the EU in International Dispute Settlement. Lessons from EU Investment Agreements*, Den Haag: T.M.C. Asser Press, 2019, p. 70 *et seq.*

The Art. above brings to life the EU's principle according to which "the protection of personal data is non-negotiable".[61] The rationale behind this idea is clear: providing solid guarantees for the fundamental rights to privacy and data protection will bring more trust in the digital economy, which in turn will promote cross-border data flows and make the EU more competitive. This standpoint is also consistent with the fundamental right status of the right to data protection under Art. 8 of the Charter of Fundamental Rights of the European Union and Art. 16 TFEU, which the GDPR strives to uphold.[62]

However, there can be some doubts concerning the effects of this provision and whether it will bring the envisaged outcomes. Art. 2 leaves both parties broad room for manoeuvre to protect their desired privacy standards without any limitation. This might create a situation where parties would be able to unilaterally impose restrictive regulations on cross-border data flows in light of their data protection law. As a consequence, this could result in uncertainty and potentially a lack of transparency for digital service providers inside and outside Europe. Furthermore, the exclusion of data protection from the scope of ICS removes potential concerns on the parties' right to regulate but might render more cumbersome addressing alleged violations. It is yet unclear whether this would also entail the exclusion of other means of investor-state dispute settlement, leaving possible violations to be resolved only between the parties.

Last but not least, the paragraph on regulatory cooperation exempts the topics of privacy and data protection from its scope.[63] While this prevents influences or negotiations to lower data protection standards, it can be seen as a missed chance to promote the EU's standpoint on data protection whilst discussing new developments in digital trade.[64]

V. Conclusions

This *Insight* focused on some of the core issues in the relationship between EU rules on cross-border data transfers and trade commitments. The most recent horizontal provision on data protection shows the willingness of the EU to move away from the GATS' model in order to preserve the fundamental right to data protection of EU citizens and to take the lead in framing new global rules concerning the governance of digital trade based on data protection. However, the analysis carried out in the previous pages has pointed out that both approaches appear to be problematic and to give rise to contro-

[61] See Communication COM(2017)7 of 10 January 2017 from the Commission, *Exchanging and Protecting Personal Data in a Globalised World*, p. 6, citing President Juncker's political guidelines: A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change (2014).

[62] Art. 8 Charter of Fundamental Rights of the European Union; Art. 16 TFEU; *Maximillian Schrems v. Data Protection Commissioner*, paras 38-39 referring to the DPD; recitals 1-2, GDPR.

[63] EU Proposal for Provisions on Cross-border Data Flows and Protection of Personal Data and Privacy trade.ec.europa.eu, Art. X.

[64] See analogous arguments by N. Clehane on behalf of European Services Forum (ESF), *Letter to Mr. Yurukov Chair of TPC Services and Investments*, 12 June 2018, www.esf.be

versies. On the one hand, the GATS framework prioritises trade interests without providing solid guarantees on upholding EU data protection law. On the other hand, the EU proposed Arts for trade and investment agreements strongly favour data protection but might result in negative repercussions on trade interests.

Needless to say, the most suitable solution would be to reach a political compromise at the international level, so that a multilateral solution – as opposed to a web of bilateral arrangements - is achieved with a view to maintaining a chosen level of data protection while promoting data flows.[65] As argued by Mattoo and Meltzer, WTO adjudicating bodies are in fact unlikely to address this crucial issue, and it can be foreseen that many different free trade agreements with varying emphases on data protection will take the lion's share in shaping cross-border data flows and data protection concerns.[66] Even if bilateral agreements might facilitate an understanding between states with divergent positions on data protection matters, it is doubtful whether they represent an adequate solution to an inherently global challenge.

[65] A. MATTOO, J.P. MELTZER, *International Data Flows and Privacy*, cit., p. 788-789.
[66] *Ibid.*