Chapter 5
Restrictions on Data Transfers and Trade Agreements

In reaction to the stalemate in the multilateral trading system, international governance of digital trade has gradually shifted toward bilateral and regional trade agreements. This allowed countries to start to regulating cross-border flows of personal data outside the WTO framework. The first section of this chapter traces the development of data flow clauses in the trade agreements of the EU, the US, and other countries. It also looks at the negotiations of the big trade agreements in the late 2010s, such as the TTIP, the TiSA, and the TPP (Sect. 5.1). The second section outlines the scope for data flow clauses in the trade agreements of the EU based on different legal requirements stemming from the architecture of EU law, the GDPR, and other regulations. These requirements include the primacy of fundamental rights over international law with regard to the right to continuous protection of personal data in Article 8 CFR, the accommodation of the legal mechanisms for the transfer of personal data in the GDPR, the inclusion of cooperation mechanisms on the basis of Article 50 GDPR, and the ban of data localization requirements beyond data protection and privacy concerns. These legal requirements are necessary to consider when drafting data flow clauses for EU trade agreements (Sect. 5.2). The third section of this chapter offers and analyzes four potential designs for data flow clauses for EU trade agreements (Sect. 5.3). The fourth section is dedicated to the analysis of the EU model data flow clauses that the European Commission introduced as a template for future trade negotiations in 2018 (Sect. 5.4).

5.1 Data Flow Clauses in Trade Agreements

The first section of this chapter is dedicated to the development of data flow clauses in trade agreements over the last two decades.[1] The EU was the first to address cross-border flows of personal data in its trade agreements. Over time, the EU tried

[1] See generally Burri (2021), pp. 26–41.

T. Naef, *Data Protection without Data Protectionism*, EYIEL Monographs - Studies in European and International Economic Law 28,
https://doi.org/10.1007/978-3-031-19893-9_5

different methods to accommodate its data protection regime (Sect. 5.1.1). On the international plane, the development of data flow clauses was significantly influenced by the negotiations of the big trade agreements in the 2010s, such as the TTIP, the TiSA, and the TPP (Sect. 5.1.2). The US started to include comprehensive data flow clauses in trade agreements only after they withdrew their signature from the TPP. Currently, the US aggressively tries to commit its trading partners to the free flow of personal data across borders (Sect. 5.1.3). Four examples of trade agreements from other countries complete the overview (Sect. 5.1.4).

5.1.1 Development in EU Trade Agreements

The EU has been the pioneer in including data flow clauses in its trade agreements.[2] The following trade agreements of the EU represent the most important milestones in the development of data flow clauses: The EU-Algeria Association Agreement from 2002 (Sect. 1.1), the EU-CARIFORUM Economic Partnership Agreement from 2008 (Sect. 1.2), the EU-Canada Comprehensive Economic and Trade Agreement (CETA) from 2016 (Sect. 1.3), and the EU-Japan Economic Partnership Agreement (JEEPA) from 2018 (Sect. 1.4).

5.1.1.1 EU-Algeria Association Agreement

The earliest provision addressing cross-border data flows in a trade agreement can be found in the EU-Algeria Association Agreement (AA) from 2002.[3] The EU-Algeria AA does not contain a chapter on electronic commerce or digital trade. The provision on cross-border data flows is located in the chapter on competition and other economic matters:

> **Article 45**
> The Parties undertake to adopt appropriate measures to ensure the protection of personal data in order to eliminate barriers to the free movement of such data between the Parties.

It is remarkable that the EU and Algeria qualify data protection as a contributing factor to eliminating barriers to cross-border data flows in their AA.[4] Prior, the protection of personal data or privacy was normally included as a legitimate public policy objective that legitimated deviations from other obligations in a trade

[2] Contra Yakovleva (2020), p. 487.

[3] Euro-Mediterranean Agreement establishing an Association between the European Community and its Member States, of the one part, and the People's Democratic Republic of Algeria, of the other part, 22 April 2002 [2005] OJ L 265/1.

[4] Willemyns (2020), p. 237.

agreement.[5] Article 45 EU-Algeria AA reflects EU-style data protection. The provision implies that cross-border flows of personal data are possible under the condition that an adequate level of protection for personal data be preserved.

5.1.1.2 EU-CARIFORUM Economic Partnership Agreement

The EU tried a new approach in the EU-CARIFORUM Economic Partnership Agreement (EPA) from 2008.[6] Article 119 EU-CARIFORUM EPA in the electronic commerce chapter of the trade agreement outlines the objective and the principles of the chapter. In the second paragraph, Article 119 connects electronic commerce with data protection:

> **Article 119 Objective and principles**
> 2. The Parties agree that the development of electronic commerce must be fully compatible with the highest international standards of data protection, in order to ensure the confidence of users of electronic commerce.

The provision does not directly address cross-border flows of personal data, but it mentions electronic commerce that relies on such data flows. The provision implies that cross-border flows of personal data are possible under the condition of the presence of an adequate level of protection for personal data. More specifically, the provision refers to the "highest international standards of data protection." The EU-CARIFORUM EPA also includes a full chapter on data protection to flesh out these standards. Article 197 describes the general objective of the chapter on data protection:

> **Article 197 General Objective**
> 1. The Parties and the Signatory CARIFORUM States, recognising:
> (a) their common interest in protecting fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data;
> (b) the importance of maintaining effective data protection regimes as a means of protecting the interests of consumers, stimulating investor confidence and of facilitating transborder flows of personal data;

[5] For example, Article XIV(c)(ii) GATS. See Sect. 4.2.1.4.2.1.

[6] Economic Partnership Agreement between the CARIFORUM States, of the one part, and the European Community and its Member States, of the other part, 16 December 2017, OJ L 289/I/3 [2008]. Another EPA that entails a separate chapter on data protection is the Interim Agreement with a view to an Economic Partnership Agreement between the European Community and its Member States, of the one part, and the Central Africa Party, of the other part, 17 December 2007 [2009] OJ L 57/1.

(c) that the collection and processing of personal data should be accomplished in a transparent and fair manner, with due respect accorded to the data subject,

agree to establish appropriate legal and regulatory regimes, as well as appropriate administrative capacity to implement them, including independent supervisory authorities, in order to ensure an adequate level of protection of individuals with regard to the processing of personal data, in line with existing high international standards.[7]

2. The Signatory CARIFORUM States shall endeavour to implement the provisions of paragraph 1 as soon as possible and no later than seven years after the entry into force of this Agreement.

In line with Article 8 CFR, Article 197 EU-CARIFORUM EPA underlines the fundamental rights aspect of data protection in paragraph 1(a) and combines it with the facilitation of cross-border data flows in paragraph 1(b).[8] The provision commits the parties to establish a data protection regime, as well as appropriate administrative capacity, including independent supervision, in order to ensure an adequate level of protection within a relatively short period of time. This is the first time that an EU trade agreement specifically refers to an adequate level of protection for individuals regarding the processing of personal data. Even if the provision refers to existing "high international standards," it is evident that the chapter on data protection specifically reflects EU-style data protection regulation. The data protection principles and the conditions for enforcement mechanism that follow in Article 199 EU-CARIFORUM EPA are a start to ensure a high standard of data protection when correctly implemented.[9]

The chapter on data protection is complemented with rules on cooperation in Article 201 EU-CARIFORUM EPA. They underline the importance of cooperation to facilitate the development of an adequate level of protection for personal data:

Article 201 Cooperation

1. The Parties acknowledge the importance of cooperation in order to facilitate the development of appropriate legislative, judicial and institutional frameworks as well as an adequate level of protection of personal data consistent with the objectives and principles contained in this Chapter.

[7] Such standards are those included in the following international instruments:

(i). Guidelines for the regulation of computerised personal data files, modified by the General Assembly of the United Nations on 20 November 1990;

(ii). Recommendation of the Organisation for Economic Cooperation and Development Council concerning guidelines governing the protection of privacy and trans-border flows of personal data of 23 September 1980.

[8] Fontoura Costa (2020), p. 487.

[9] Ibid., 489.

The second paragraph of Article 201 entails a list of areas in which the parties agree to cooperate. For example, the list includes the exchange of information and expertise, assistance in drafting legislation, guidelines and manuals, and assistance with the design and implementation of compliance initiatives aimed at economic operators and consumers. Nevertheless, it would have been useful to also include compliance initiatives aimed at public authorities. Overall, the EU implemented essential parts of its data protection regulation in the EU-CARIFORUM EPA and used the trade agreement to lay the basis for an improvement of the level of protection for personal data in the contracting parties' legislative, judicial, and institutional frameworks.

5.1.1.3 EU-Canada Comprehensive Economic and Trade Agreement

The EU abandoned the approach taken in the EU-CARIFORUM EPA and chose yet another approach in the CETA from 2016.[10] The CETA does not include a general provision on the free flow of personal data across borders. This can be explained by the fact that Canada already had an adequacy decision from the EU. This means that the transfer of personal data from the EU to commercial organizations in Canada was already possible without the need for further safeguards.[11] Yet the CETA does not include substantive rules on data protection either. Article 16.4 CETA on trust and confidence in electronic commerce only entails a very general reference to the regulation of data protection:[12]

> **Article 16.4 Trust and confidence in electronic commerce**
> Each Party should adopt or maintain laws, regulations or administrative measures for the protection of personal information of users engaged in electronic commerce and, when doing so, shall take into due consideration international standards of data protection of relevant international organisations of which both Parties are a member.

The reference to international organizations is limited to the standards of the UN and the OECD as Canada is not a party to Convention 108, and the EU member states are not members of APEC. The OECD Privacy Guidelines pursue economic rather than broader normative goals of protecting personal data.[13] The provision recognizes data protection as a necessary condition for spurring international trade

[10] Comprehensive Economic and Trade Agreement (CETA) between Canada and the European Union and its Member States, 30 October 2016 [2017] OJ L 11/23.

[11] Wolfe (2019), p. 73; Greenleaf (2018), p. 208.

[12] Streinz (2019), p. 335.

[13] Yakovleva (2018), p. 496. Cp. Sect. 3.1.1.2.1.

and does not acknowledge its fundamental rights character as Article 197.1(a) of the EU-CARIFORUM EPA did.[14]

Moreover, the CETA does not restrict national or regional regulations even if they might interfere with the free flow of personal data across borders in fields covered by the agreement.[15] The provision on cross-border flows of personal data concerning financial services in Article 13.15(2) CETA exempts EU data protection law from the scope of the CETA chapter on financial services:[16]

> **Article 13.15 Transfer and processing of information**
> 2. 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 shall be in accordance with the legislation governing the protection of personal information of the territory of the Party where the transfer has originated.

The CETA clearly makes a distinction between domestic data protection regulation and international trade law.[17] The CETA does not contain any data protection obligations and there are no rules for cross-border flows of personal data in the trade agreement. The EU was careful to keep separate the regulation of data protection and trade rules.[18] In addition, the EU started to shield its rules for the transfer of personal data from other obligations in the CETA as is evidenced by the provision on financial services in Article 13.15(2) CETA.

5.1.1.4 EU-Japan Economic Partnership Agreement

In the negotiation of the JEEPA, the EU was faced with Japanese demands—likely inspired by the concurrent negotiations of the TPP—to include a general provision on cross-border flows of personal data.[19] The EU was reluctant to include such provisions and resisted the Japanese demands until the end. Indeed, this disagreement emerged as the last big hurdle to the conclusion of the JEEPA.[20] After five years of negotiations, the two parties achieved agreement at the EU-Japan Summit in 2017. In a joint declaration, Prime Minister Shinzo Abe and Commission President

[14] Cp. Wunsch-Vincent (2008), p. 520.

[15] Berka (2017), p. 179.

[16] Yakovleva and Irion (2020), p. 14.

[17] Irion and Bartl (2017), p. 5.

[18] But see Burri (2017), p. 107.

[19] Streinz (2019), p. 335. The EU also declined in 2013 to grant India what it called "data secure status" as part of the proposed trade agreement. According to Graham Greenleaf that would have meant the recognition of completely inadequate laws in India as being adequate. See Greenleaf (2014), pp. 432–433.

[20] Mucci et al. (2016).

Jean-Claude Juncker stressed the importance of ensuring "a high level of privacy and security of personal data as a fundamental right and as a central factor of consumer trust in the digital economy, which also further facilitate mutual data flows, leading to the development of digital economy."[21] They indicated that their respective data protection reforms offered new opportunities for simultaneous findings of adequacy. The JEEPA was successfully concluded in July 2018.[22] In the end, the parties settled on a *rendez-vous* clause:

> **Article 8.81 Free flow of data**
> The Parties shall reassess within three years of the date of entry into force of this Agreement the need for inclusion of provisions on the free flow of data into this Agreement.

In 2019, the EU Commission adopted an adequacy decision for Japan.[23] The EU has thus continued to treat data protection and international trade law as two separate tracks with little middle ground. Only after the negotiations with Japan were effectively concluded did the Commission reach an internal compromise on a new template for horizontal provisions for cross-border data flows and data protection.[24]

5.1.2 Development in the Mega-Regional Trade Agreements

On the international plane, the development of data flow clauses was significantly influenced by the negotiations of the big trade agreements in the 2010s. The negotiations of the TTIP between the EU and the US were never completed but they showed how the two parties clashed over the issue of cross-border flows of personal data (Sect. 5.1.2.1). The multilateral negotiations of the TiSA were not completed either. The proposals of the US for a data flow clause triggered a defensive reaction from the EU (Sect. 5.1.2.2). In contrast, the multilateral negotiations for the TPP saw the inclusion of an intricate data flow clause, which was also integrated in the Comprehensive and Progressive Agreement for the Trans-Pacific Partnership (CPTPP) after the US withdrew its signature from the TPP (Sect. 5.1.2.3).

[21] European Commission (2017b).

[22] Agreement between the European Union and Japan for an Economic Partnership, 17 July 2018 [2018] OJ L 330/3.

[23] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, [2019] OJ L 76/1.

[24] Streinz (2019), p. 335. See Sect. 5.4.

5.1.2.1 Transatlantic Trade and Investment Partnership

The TTIP was a proposed trade agreement between the US and the EU. While the idea for such an agreement had been circulating for more than a decade, formal negotiations only started in 2013. Several negotiation rounds took place in the following years and efforts to wrap-up negotiation in late 2016—before the new US administration took office—failed. The negotiations were subsequently halted by US President Donald Trump. After the US left the Paris Agreement on Climate Change, the Council of the EU decided in 2019 that the negotiating directives for the TTIP had become obsolete.[25]

In the beginning of the negotiations, EU Justice Commissioner Viviane Reding stated that data protection issues had been cut out of the TTIP as a result of "a political decision by the US and EU."[26] She also warned against bringing data protection to the trade talks at a conference in Washington D.C., indicating that the US would not be very happy with the exclusion of cross-border flows of personal data under the TTIP. She said that "[t]here are challenges to get [the TTIP] done and there are issues that will easily derail it. One such issue is data and the protection of personal data."[27] Nevertheless, US Trade Representative Michael Froman never publicly said that data protection should be off the agenda.[28]

The leaked draft text of the TTIP from 2016 did *not* include a provision on cross-border flows of personal data.[29] The leaked EU note on the tactical state of play in the TTIP negotiations from March 2016 summarized that "[d]iscussions on e-commerce covered all proposals except for the provisions on data flows and computing facilities." Nevertheless, the note also indicated that "[t]he US signaled that progress on [...] key EU interests might be accelerated if discussions on data flows and computing facilities also advanced faster." It is safe to assume that cross-border flows of personal data were repeatedly a topic on the agenda. This is probably also the reason why the European Parliament asked the Commission to ensure that the EU's *acquis* on data privacy was not compromised through the liberalization of data flows.[30] The Parliament recommended that a comprehensive and unambiguous horizontal self-standing provision based on Article XIV GATS should be incorporated into the TTIP to fully exempt the existing and future EU legal framework on the protection of personal data.[31] Interestingly, the recommendations of the Parlia-

[25] Council of the EU (2019), Article 3.

[26] Fleming (2013). See also European Commission (2013a).

[27] European Commission (2013b).

[28] Fleming (2013).

[29] The negotiation documents were leaked by Wikileaks. The documents are available on their website.

[30] European Parliament (2015), Article 2(b) xii.

[31] Ibid.

ment allowed the negotiation of a data flow clause *if* the full application of data protection rules on both sides of the Atlantic was guaranteed.[32]

The negotiations of the TTIP confirm that the EU once again decided to separate the regulation of data protection from international trade law and to shield its rules for the transfer of personal data from other obligations in trade agreements. It is questionable whether the US would ever have agreed to a trade agreement without rules enabling cross-border flows of personal data. Such rules have become more important for the US when the Privacy Shield was invalidated and the possibility to use the instruments in Article 46 GDPR has become unsure. They will continue to be important because eventually the adequacy decision for the new Transatlantic Data Privacy Framework, which is currently in preparation, will be challenged and its validity will not be evident.[33]

5.1.2.2 Trade in Services Agreement

Due to the lack of progress in the negotiations at the WTO, some WTO members formed a sub-group called the Really Good Friends (RGF) in 2012 to discuss the possibility of a services liberalization agreement. Led by the US and the EU, the RGF consisted of more than 20 countries including Australia, Canada, Japan, the Republic of Korea, Switzerland, Colombia, and Mexico. Negotiations for the TiSA started immediately after the formation of the sub-group. Over 20 full negotiation rounds took place in Geneva in the following years. Just as with the TTIP, efforts to wrap-up the negotiations in late 2016 failed. The negotiations are currently suspended and the future of the TiSA is unclear.

One of the reasons why the TiSA was not successfully concluded were the controversies over rules on cross-border flows of personal data.[34] A leaked US negotiation document from 2014 titled "Proposal of New Provisions Applicable to All Services" suggested the inclusion of a provision on movement of information:[35]

> **Article X.4**
> No Party may prevent a service supplier of another Party from transferring, accessing, processing or storing information, including personal information, within or outside the Party's territory, where such activity is carried out in connection with the conduct of the service supplier's business.

[32] Ibid.

[33] noyb (2022).

[34] Yakovleva (2018), p. 496.

[35] The negotiation documents were leaked by Wikileaks. The documents are available on their website.

This proposal for a data flow clause in the TiSA did not include any exception for the protection of personal data.[36] According to other leaked negotiation documents from 2015 and 2016, the provision was later included as Article 2 in the negotiating text of the TiSA Annex on Electronic Commerce. The annotated negotiation documents show that many countries considered exceptions or conditions for this provision, so as to allow more flexibility for domestic regulation. For instance, Hong Kong proposed that "[t]here should be a balance between free movement of information across border and protection of personal data. Advancing the former cause should be without prejudice to safeguarding the latter right."[37] Switzerland also proposed to include safeguards that "[e]ach party applies its own regulatory regime concerning the transfer of data and personal data by electronic means."

The leaked negotiation documents also indicated that the TiSA Annex on Localization sought to ban "local presence" and other "local performance" requirements. It is unclear whether restrictions on cross-border flows of personal data based on domestic data protection regulation would have been included in this ban. The exceptions do not mention data protection related safeguards.

The European Commission did not comment on the data flow clauses in the negotiation documents because it was waiting for the final agreement on the Privacy Shield with the US before addressing the issue of cross-border flows of personal data in the TiSA negotiations. Nevertheless, the European Parliament took a firm stand on the regulation of cross-border flows of personal data in the TiSA. It recommended that the Commission take a cautious approach to the negotiation of chapters concerning data and privacy protection. It suggested the incorporation of a comprehensive, unambiguous, horizontal, self-standing, and legally binding provision based on Article XIV GATS, which would fully exempt the existing and future EU legal framework for the protection of personal data from the scope of the TiSA.[38] Negotiations have not been resumed since 2017.

5.1.2.3 Comprehensive and Progressive Agreement for Trans-Pacific Partnership

The TPP was a trade agreement between Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, Vietnam, and the US signed in 2016. It was not ratified and could not enter into force because US President Donald Trump withdrew the US signature from the TPP in 2017. The remaining countries negotiated a new trade agreement called the CPTPP that incorporated most of the provisions from the TPP and entered into force in 2018.

[36] Berka (2017), p. 180; Kelsey and Kilic (2014), pp. 15–16.

[37] Burri (2017), p. 124.

[38] European Parliament (2016), Paragraph 1(c)ii., iii. and v.

The US significantly shaped the design of the provision on cross-border flows of personal data during the negotiations of the TPP, which was integrated without changes into the CPTPP:

Article 14.11 Cross-Border Transfer of Information by Electronic Means

1. The Parties recognize that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.
2. Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.
3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:
   (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
   (b) does not impose restrictions on transfers of information greater than are required to achieve the objective.

The first paragraph of the provision introduces the data flow clause by recognizing the differences between regulatory regimes for cross-border flows of personal data. The second paragraph entails the obligation to allow cross-border flows of personal data by electronic means for the conduct of business. This is the first time a provision explicitly formulates a commitment to the free flow of personal data across borders. Nevertheless, the third paragraph allows derogations from this obligation for legitimate public policy objectives under two conditions. It can be assumed that data protection and privacy qualify as legitimate public policy objectives under this provision. The first condition for the derogation demands compliance with the standards that can also be found in the *chapeau* of Article XIV GATS. The second condition refers to restrictions that should not be greater than *required* to achieve the objective pursued by the measure in question. It is not entirely clear what kind of standard the second condition foresees. The use of the word required might imply that the test should be easier than a necessity test. However, only the English and the Spanish version of the CPTPP use language that does not hint at a necessity test. The French version clearly refers to a necessity test.

In addition, the parties recognize in Article 14.8 CPTPP that the economic and social benefits of protecting the personal data of users of electronic commerce as well as the contribution that this makes to enhancing consumer confidence in electronic commerce. However, the parties do not refer to the fundamental rights character of data protection. It must be assumed that the CPTPP, which is the only mega-regional trade agreement in force, is likely to set international standards for data flow clauses in future trade agreements.

5.1.3 Development in US Trade Agreements

Although the US was not the first mover when it came to data flow clauses in trade agreements, they have extensively pursued this option in more recent years. The trade agreement with the Republic of Korea from 2012 was the first attempt by the US to get some form of commitment to the free flow of personal data across borders (Sect. 5.1.3.1). The US intensified their efforts to include strong obligations for cross-border flows of personal data in the negotiations of the TTIP, the TiSA, and the TPP. After the withdrawal of its signature from the TPP, the US started to include stronger obligations on cross-border flows of personal data in trade agreements such as the United States-Mexico-Canada Agreement (USMCA) from 2018 (Sect. 5.1.3.2) and the US-Japan Digital Trade Agreement from 2019 (Sect. 5.1.3.3).

5.1.3.1 US-South Korea Free Trade Agreement

The trade agreement with the Republic of Korea from 2012 (KORUS) was the first US trade agreement to include a provision on the free flow of personal data across borders.[39] The provision on cross-border information flows is located in Article 15.8 of the e-commerce chapter in the KORUS:

> **Article 15.8 Cross-Border Information Flows**
> Recognizing the importance of the free flow of information in facilitating trade, and acknowledging the importance of protecting personal information, the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders.

The provision refers to personal data, but the importance of protecting it is put in strong contrast with a call on the parties to endeavor to refrain from imposing or maintaining unnecessary barriers to cross-border flows of personal data. There are no further indications as to what constitutes a "necessary" or "unnecessary" barrier in the KORUS. It is also not clear whether domestic rules on cross-border flows of personal data are considered necessary or not. Because the language used in the provision is not actionable,[40] it is uncertain if one party could use it to challenge another party's restrictions on cross-border flows of personal data.[41]

Article 15.8 of the e-commerce chapter in the KORUS is the first attempt by the US to include some form of commitment to the free flow of personal data across borders. Two other US trade agreements from 2012—one with Colombia and one with Panama—do not contain any similar provisions.

[39] Wu (2017), p. 23; Aaronson (2015), p. 687.
[40] Yakovleva (2020), p. 487; Wu (2017), p. 23; Burri (2019), pp. 95–96; Aaronson (2015), p. 687.
[41] Aaronson and Townes (2012), p. 6.

5.1.3.2 United States-Mexico-Canada Agreement

The US actively participated in the negotiations of the TPP and signed the trade agreement in 2016. One year later, President Donald Trump decided to withdraw the US signature.[42] In consequence, the US used the renegotiation of the North America Free Trade Agreement in 2018 to set new standards for data flow clauses in their trade agreements.[43] The provision on the cross-border transfer of information by electronic means is located in Article 19.11 of the digital trade chapter in the USMCA:

> **Article 19.11 Cross-Border Transfer of Information by Electronic Means**
> 1. No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person.
> 2. This Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 that is necessary to achieve a legitimate public policy objective, provided that the measure:
>   (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
>   (b) does not impose restrictions on transfers of information greater than are necessary to achieve the objective.[44]

Compared with Article 15.8 KORUS, Article 19.11(1) USMCA is an actionable provision that uses strong language to install an obligation on the parties to refrain from prohibiting or restricting the cross-border transfer of information, including personal information, for the conduct of business.[45] The exception in Article 19.11(2) USMCA require the party imposing a prohibition or restriction on cross-border flows of personal data to justify its measures. The exceptions present a significant burden for any regulation of cross-border flows of personal data. A measure inconsistent with Article 19.11(1) USMCA must be necessary for a legitimate public policy objective and not be applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination, or a disguised restriction on trade. These conditions are

[42] Removing the US from the TPP was one of President Donald Trump's first decisions in office. Nevertheless, the administration of President Barack Obama significantly shaped the design of the provision on cross-border data flows during the negotiations of the TPP.

[43] The USTR mentions the establishment of "rules to ensure that NAFTA countries do not impose measures that restrict cross-border data flows and do not require the use or installation of local computing facilities" in the official summary of objectives for the NAFTA renegotiation. See USTR (2017), p. 9.

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

[45] Willemyns (2020), p. 237.

similar to the general exceptions in Article XIV GATS.[46] However, there is an additional condition in Article 19.11(2)(b) USMCA entailing a separate necessity test that is qualified in a footnote. Differential treatment of data flows solely on the basis that they are cross-border in a manner that modifies the conditions of competition cannot satisfy the additional necessity test in Article 19.11(2)(b) USMCA.[47] This qualification in the footnote seems to be difficult to satisfy with domestic data protection rules that entail legal mechanisms for the transfer of personal data with separate requirements.[48]

There are some essential differences between Article 14.11 CPTPP and Article 19.11 USMCA. The CPTPP introduces the provision on cross-border flows of persona data with a recognition of the differences between regulatory regimes. Such an accommodating introductory clause is absent from the USMCA. Furthermore, the *chapeau* of the derogations in the CPTPP does not include a necessity test like the USMCA does. The English version of the CPTPP refers to restrictions that should not be greater than *required* to achieve the objective. The USMCA also entails a second necessity test, which is further qualified in a footnote. It seems that the USMCA is less permissive than the CPTPP of restrictions on cross-border flows of personal data for data protection or privacy. The data flow clause in the USMCA is in line with the US digital trade agenda. It is an expression of the US view that data protection is an impediment to digital trade and therefore in need of justification.[49]

In addition, the provision on cross-border data flows in Article 19.11(1) USMCA takes precedence over a long and detailed provision on personal information protection in Article 19.8 USMCA:

Article 19.8: Personal Information Protection

1. The Parties recognize the economic and social benefits of protecting the personal information of users of digital trade and the contribution that this makes to enhancing consumer confidence in digital trade.
2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade. In the development of this legal framework, each Party should take into account principles and guidelines of relevant international bodies,[50] such as the *APEC*

[46] See Sect. 4.2.1.4.2.

[47] Svetlana Yakovleva has noted that despite the differences between US- and EU-led trade agreements, they have one trait in common: "they are not formulated as non-discrimination provisions." This is not entirely correct when looking at the qualification in the footnote in Article 19.11(2)(b) USMCA, which entails such a non-discrimination obligation. See Yakovleva (2020), p. 497.

[48] See also Streinz (2019), p. 332.

[49] Ibid., 334.

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

Privacy Framework and the *OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013).*

3. The Parties recognize that pursuant to paragraph 2, key principles include: limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability. The Parties also recognize the importance of ensuring compliance with measures to protect personal information and ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented.
4. Each Party shall endeavor to adopt non-discriminatory practices in protecting users of digital trade from personal information protection violations occurring within its jurisdiction.
5. Each Party shall publish information on the personal information protections it provides to users of digital trade, including how:
   (a) a natural person can pursue a remedy; and
   (b) an enterprise can comply with legal requirements.
6. Recognizing that the Parties may take different legal approaches to protecting personal information, each Party should encourage the development of mechanisms to promote compatibility between these different regimes. The Parties shall endeavor to exchange information on the mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them. The Parties recognize that the *APEC Cross-Border Privacy Rules* system is a valid mechanism to facilitate cross-border information transfers while protecting personal information.

The provision on personal information protection uses weak language for the substantive protection for personal data.[51] While Article 19.8(1) USMCA recognizes the contribution of data protection to enhancing consumer confidence in digital trade, it does not mention data protection as a fundamental right. According to Article 19.8(2) USMCA, the parties should adopt a legal framework that provides for the protection of personal data. However, a footnote clarifies that sector-specific laws or laws that provide for the enforcement of voluntary undertakings by enterprises are enough to comply with this obligation.[52] This approach is tailored to the US patchwork regulation concerning data privacy.[53] It is evident that such a legal framework for the protection of personal data does not have to include the public sector and extend to internet surveillance practices. Even though Article 19.8(3) USMCA entails important data protection principles and highlights the importance of ensuring compliance with measures to protect personal data, it also underlines that any restrictions on cross-border flows of personal information must be necessary and

[51] Streinz (2019), p. 334.
[52] Geist (2018).
[53] Wolfe (2019), p. 74.

proportionate to the risks presented. This is a reference to the obligations on cross-border data flows in Article 19.11 USMCA, which accordingly takes precedence over the protection of personal data. Finally, Article 19.8(6) USMCA encourages the parties to promote compatibility between different legal approaches to data protection and explicitly recognizes that the APEC Cross-Border Privacy Rules system based on the accountability principle is a valid mechanism for cross-border data flows.

5.1.3.3 US-Japan Digital Trade Agreement

The US-Japan Digital Trade Agreement was signed in 2019, along with the US-Japan Trade Agreement. The provisions on digital trade from the USMCA have been included, almost *verbatim*, in the digital trade agreement with Japan. It seems that these provisions have become the model for data flow clauses in future US-led trade agreements.[54] Article 11 of the US-Japan Digital Trade Agreement even entails the same restrictive qualification in the footnote of the exception to the prohibition of restrictions on cross-border data flows.

5.1.4 Development in Non-EU/US Trade Agreements

Trade agreements without the EU or the US as a party also include data flows clauses. Four recent examples show the development of data flow clauses outside the EU and the US: the Costa Rica-Colombia trade agreement from 2013 (Sect. 5.1.4.1), the Mexico-Panama trade agreement from 2014 (Sect. 5.1.4.2), the China-Republic of Korea trade agreement from 2015 (Sect. 5.1.4.3), and the Sri Lanka-Singapore trade agreement from 2018 (Sect. 5.1.4.4).

5.1.4.1 Costa Rica-Colombia Trade Agreement

The Costa Rica-Colombia trade agreement was signed in 2013. It is one of many trade agreements that uses regulatory cooperation to facilitate cross-border flows of personal data:[55]

[54] Yakovleva and Irion (2020), p. 13. These provisions are also included in the US proposal for the electronic commerce negotiations at the WTO. See Sect. 4.2.4.4.

[55] Willemyns (2020), p. 237; Wu (2017), p. 23.

Artículo 16.7 Cooperación

1. Reconociendo la naturaleza global del comercio electrónico, las Partes afirman la importancia de
   b) compartir información y experiencias sobre leyes, regulaciones, y programas en el ámbito del comercio electrónico, incluyendo aquellos relaci-onados con privacidad de datos, confianza del consumidor, seguridad en las comuni-caciones electrónicas, autenticación, de-rechos de propiedad intelectual, y gobierno electrónico;
   c) trabajar para mantener los flujos transfronterizos de información como un elemento esencial en el fomento de un entorno dinámico para el comercio electrónico;

The trade agreement between Costa Rica and Colombia does not go beyond a declaration of intent on cooperation. Very often such provisions on cooperation are "just the equivalent of trade negotiators throwing in the towel on an issue where no perceivable consensus is apparent, or inserting verbiage to provide some filler to a given treaty text."[56] This is also apparent in the provision on the protection of personal data:

Artículo 16.7 Protección de la Información Personal

1. Las Partes procurarán adoptar o mantener leyes, regulaciones o medidas administrativas para la protección de la información personal de los usuarios que participen en el comercio electrónico. Las Partes podrán tener en cuenta las normas internacionales y los criterios de las organizaciones internacionales pertinentes sobre la materia.
2. Las Partes harán sus mejores esfuerzos para intercambiar información y experiencias en cuanto a sus regímenes domésticos de protección de la información personal.

In this case, the parties advise each other to endeavor to adopt data protection laws and only commit to do their best to exchange information about them. Nevertheless, the two countries acknowledge the importance of data protection for the users of electronic commerce.

5.1.4.2 Mexico-Panama Trade Agreement

The Mexico-Panama trade agreement was signed in 2014. It stands out as a trade agreement between two developing economies with a binding commitment on cross-border flows of personal data:

[56] Lacey (2020), p. 202.

> **Artículo 14.10 Flujo Transfronterizo de Información**
> Cada Parte permitirá que sus personas y las personas de la otra Parte transmitan información electrónica, desde y hacia su territorio, cuando sea requerido por dicha persona, de conformidad con la legislación aplicable en materia de protección de datos personales y tomando en consideración las prácticas internacionales.

In this case, the two parties agreed to allow transmissions of electronic information to and from their territory in accordance with data protection legislation and following international practices.[57] The reference to data protection legislation and international practices is open to different interpretations. It could indicate that the commitment to cross-border flows of personal data in the trade agreement is subject to domestic legislation that regulates such data flows for the protection of personal data. It could also mean that domestic legislation should accommodate the obligation on cross-border flows of personal data under consideration of international practices. The provision on data protection in the Mexico-Panama trade agreement does not resolve the ambiguity of the interpretation:

> **Artículo 14.8 Protección de Datos Personales**
> Las Partes fomentarán la adopción o mantenimiento de leyes y regulaciones para la protección de los datos personales de los usuarios del comercio electrónico. Las Partes tomarán en consideración las prácticas internacionales que existen en esta materia.

The provision encourages the parties to adopt or maintain data protection legislation and requires them to consider international practices when doing so. In any case, the provision is subject to general exceptions like those in Article XIV GATS, which were included in Article 19.2(2) Mexico-Panama trade agreement *mutatis mutandis*.[58]

5.1.4.3 China-Republic of Korea Trade Agreement

The China-Republic of Korea trade agreement was signed in 2015. The two parties address data protection with a rather weak provision:

> **Article 13.5 Protection of Personal Information in Electronic Commerce**
> Recognizing the importance of protecting personal information in electronic commerce, each Party shall adopt or maintain measures which ensure the protection of the personal information of the users of electronic commerce and share

[57] Wu (2017), p. 23.
[58] Monteiro and Teh (2017), p. 50.

information and experience on the protection of personal information in electronic commerce.

In this case, the two parties recognize the importance of protecting the personal data of users of electronic commerce.[59] It is interesting that China included a provision on data protection, a value it does not seem to implement domestically.[60] It is also notable that the provision includes an obligation to share information and experiences on the protection of personal information in electronic commerce. This seems like a cooperation commitment in order to address any obstacles that may arise in the cross-border flow of personal data between the two countries.

5.1.4.4 Sri Lanka-Singapore Trade Agreement

The Sri Lanka-Singapore trade agreement was signed in 2018. The influence of the CPTPP on the data flow clause in the Sri Lanka-Singapore trade agreement cannot be overlooked—even if Sri Lanka is not a member of the CPTPP.[61] The provision on cross-border flows of personal data in the electronic commerce chapter of the Sri Lanka-Singapore trade agreement is essentially the same:

Article 9.9 Cross-Border Transfer of Information by Electronic Means

1. The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.
2. Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.
3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 of this Article to achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade.

However, an important difference between the data flow clauses in the Sri Lanka-Singapore trade agreement and the CPTPP can be found in the exception. The condition in the CPTPP that a measure may not impose restrictions on transfers of information greater than required to achieve its legitimate objective is not replicated in Article 9.9(3) of the Sri Lanka-Singapore trade agreement. The Sri Lanka-Singapore trade agreement is more permissive of restrictions on cross-border flows of personal data. Restrictions must be adopted to achieve a legitimate public policy objective such

[59] Ibid., 51–52.

[60] Willemyns (2020), p. 238; Weber et al. (2020), p. 569.

[61] Cp. Burri (2017), p. 128.

as the protection of personal data and they have to satisfy the conditions that can also be found in the *chapeau* of the general exceptions in Article XIV GATS.

5.1.5 Summary

The first data flow clauses in EU and US trade agreements illustrate their respective positions on data protection-based restrictions for cross-border flows of personal data perfectly. The EU sees data protection as a precondition for trade whereas the US perceives it as a potential trade barrier akin to data protectionism. In line with its digital trade agenda, the US pushed for a binding commitment on cross-border flows of personal data in the negotiations of the mega-regional trade agreements in the 2010s. After the US withdrew its signature from the TPP, it used the USMCA to set new standards for data flow clauses. The USMCA is currently the trade agreement with the strongest obligation on cross-border flows of personal data.[62] It prohibits the parties from restricting the free flow of personal data and imposes strict conditions for exceptions, including the standards from the *chapeau* of Article XIV GATS and two necessity tests, one of which is further qualified in a footnote. This provision has become the model for US-led trade agreements. At the same time, the provision in the CPTPP has become the model for new trade agreements of its members, as the Sri Lanka-Singapore trade agreement from 2018 shows.

The EU tried different approaches in its trade agreements. It used the EU-CARIFORUM EPA from 2008 to underline the fundamental rights character of data protection. This agreement committed the parties to establish a data protection regime, as well as appropriate administrative capacity, including independent supervision, in order to ensure an adequate level of protection and facilitate cross-border flows of personal data. In contrast, the CETA from 2016 only contains a very general reference to data protection. The CETA clearly makes a distinction between domestic data protection regulation and international trade law.[63] The CETA does not contain any data protection obligations anymore, and it includes no rules for cross-border flows of personal data. The EU separated the regulation of data protection from trade rules.[64] In addition, the EU started to shield its rules for the transfer of personal data from other obligations in the CETA as the provision on cross-border flows of personal data concerning financial services in Article 13.15(2) CETA shows.

[62] Willemyns (2020), p. 237.
[63] Irion and Bartl (2017), p. 5.
[64] But see Burri (2017), p. 107.

5.2 Legal Requirements for Data Flow Clauses in EU Trade Agreements

The second section of this chapter is dedicated to the legal requirements for data flow clauses in EU trade agreements. The architecture of EU law, the right to continuous protection of personal data in Article 8 CFR, the GDPR, and other regulations impose requirements upon the EU for the inclusion of data flow clauses in trade agreements. The most important requirement is the primacy of fundamental rights over international law (Sect. 5.2.1). In addition, data flow clauses in EU trade agreements should accommodate legal mechanisms for the transfer of personal data in the GDPR (Sect. 5.2.2). The GDPR also encourages the EU to develop means for cooperating with third countries in the field of data protection (Sect. 5.2.3). Finally, the GDPR and Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the EU entail requirements for a ban on data localization obligations of third countries that are not motivated by data protection or privacy (Sect. 5.2.4).

5.2.1 Respecting the Primacy of Fundamental Rights Over International Law

The first legal requirement for data flow clauses in EU trade agreements is the primacy of fundamental rights over international law. This requires a brief explanation of the relationship between primary EU law and international law (Sect. 5.2.1.1) before it is possible to discuss the implications for data flow clauses in EU trade agreements (Sect. 5.2.1.2).

5.2.1.1 The Relationship of Primary Union Law and International Law

Primary Union law is above international law in the hierarchy of the legal order in the EU (Sect. 5.2.1.1.1). The ECJ has two important competences with regard to this subordination of international law: The Court can *a priori* examine the lawfulness of a proposed international agreement according to the opinion procedure in Article 218(11) TFEU (Sect. 5.2.1.1.2) and the Court can *a posteriori* review the lawfulness of an international agreement with regard to the EU Treaties in an annulment procedure according to Article 263 TFEU or in a preliminary ruling procedure according to Article 267(b) TFEU (Sect. 5.2.1.1.3).

5.2.1.1.1 Hierarchy in the Legal Order

Primary Union law is derived from the EU Treaties, the Charter based on Article 6(1) TEU since the adoption of the Lisbon Treaty in 2009, and the general principles of law established by the ECJ.[65] The EU Treaties do not regulate *expresis verbis* the hierarchical position of international agreements within the legal order of the EU.[66] Article 216 TFEU only states that international agreements concluded by the EU are binding upon the institutions of the Union and on its member states. The ECJ endorsed early on that international agreements concluded by the EU form an integral part of Union law from the moment of their entry into force.[67]

5.2.1.1.2 A Priori Examination of International Agreements by the European Court of Justice

An important competence of the ECJ with regard to the subordination of international law is that the Court can *a priori* examine the lawfulness of a proposed international agreement according to the opinion procedure in Article 218(11) TFEU: any member state, the European Parliament, the Council or the Commission may seek the opinion of the ECJ on the compatibility of a proposed international agreement with the EU Treaties.[68] This examination also extends to the Charter and the general principles of law established by the ECJ.[69] Should the ECJ find an incompatibility, the proposed agreement may only enter into force if it is amended.

5.2.1.1.3 A Posteriori Review of International Agreements by the European Court of Justice

Another important competence of the ECJ with regard to the subordination of international law is that the Court can *a posteriori* review the lawfulness of an international agreement with regard to the EU Treaties in an annulment procedure according to Article 263 TFEU or via a preliminary ruling procedure according to Article 267(b) TFEU.[70] This review power also extends to the Charter and the general principles of law established by the ECJ.

---

[65] Craig and de Búrca (2017), p. 111; Lenaerts and Van Nuffel (2011), p. 753.

[66] Mohay (2017), p. 157; van Rossem (2009), p. 194; Van Vooren and Wessel (2014), p. 211, 221; Lenaerts and Van Nuffel (2011), p. 817.

[67] ECJ, *R. & V. Haegeman v Belgian State*, para. 5; Van Vooren and Wessel (2014), p. 211; Eeckhout (2011), p. 327.

[68] Cp. ECJ, Opinion 2/15, para. 305 and ECJ, Opinion 1/15, para. 232; Mohay (2017), p. 153; see generally Craig and de Búrca (2017), pp. 369–371; Eeckhout (2011), pp. 268–274.

[69] Cp. ECJ, Opinion 1/17, para. 237 and ECJ, Opinion 1/15, para. 119; Cremona (2020), p. 3, 10.

[70] Cp. ECJ, *Western Sahara Campaign UK*, paras 36–37; ECJ, *Parliament v. Council and Commission,* paras 67–70 and ECJ, *Germany v. Council*, para. 72. Importantly, the annulment by the

The ECJ has previously annulled decisions of the Council approving an international agreement because of a breach of the general principles of Community law. In *Germany v. Council*, the ECJ annulled the first indent of Article 1(1) of Council Decision 94/800/EC of 22 December 1994 approving the Framework Agreement on Bananas concluded by the EC and certain third countries, because it violated the general principle of non-discrimination.[71] Article 264 TFEU holds that if an action is well-founded, the ECJ should declare the act concerned to be void and, if the Court considers this necessary, state which of the effects of the act that has been declared void should be considered as definitive. The power to determine the date at which the annulment of the act becomes effective and to what extent is important to prevent the annulment from resulting in a legal vacuum.[72]

An annulment by the ECJ merely invalidates the internal act of conclusion of an international agreement with the consequence that the agreement is inapplicable within the EU but remains valid on the international plane.[73] When the ECJ annulled Council Decision 2004/496/EC of 17 May 2004 approving the PNR agreement with the US and the underlying adequacy decision, the Court recognized that the EC cannot rely on its own law as a justification for not fulfilling the agreement, which remains applicable for a period of 90 days from termination thereof, and preserved the effect of the decision on adequacy until the end of that period.[74]

5.2.1.2 Implication for the Design of Data Flow Clauses

Any EU international trade commitment must respect the provisions of the EU Treaties and the Charter.[75] This includes the right to data protection in Article 8 CFR. In order to ensure the lawfulness of a data flow clause, the European Commission must respect Article 8 CFR when negotiating trade agreements. This also concerns the right to continuous protection of personal data that is transferred from the EU to a third country, which is an unwritten constituent part of Article 8 CFR. It is therefore important to recognize and state in a trade agreement that the protection of personal data is a fundamental right, and that the protection of personal data must continue when it is transferred across borders.

There are two options for the EU to deal with the primacy of fundamental rights over international law when negotiating data flow clauses in trade agreements. The

ECJ merely invalidates the internal act of conclusion of an international agreement with the consequence that the agreement is inapplicable within the EU but remains valid on the international plane. Peters (1997), p. 76; see generally Eeckhout (2011), pp. 292–298.

[71] ECJ, *Germany v. Council*, para. 72.

[72] Cp. ECJ, *Parliament v. Council*, para. 88 and ECJ, *Commission v. Council*, para. 57; Barents (2004), p. 259.

[73] Peters (1997), p. 76.

[74] ECJ, *Parliament v. Council and Commission,* paras 68–74.

[75] Van Waeyenberge and Pecho (2014), p. 752; Gstöhl and Hanf (2014), p. 745 fn. 61.

first option does not include a commitment to the free flow of personal data across borders and focuses on carving-out data protection from an agreement. The second option includes a commitment to the free flow of personal data across borders and focuses on aligning this commitment with the right to continuous protection of personal data. Should a commitment to the free flow of personal data be integrated into a trade agreement of the EU, it must guarantee that the transfer of personal data can be restricted should the level of protection for personal data not be essentially equivalent to that guaranteed within the EU in cases in which personal data is transferred to a contracting party or parties. This is especially important in cases in which foreign internet surveillance practices capture personal data that is transferred from the EU to the surveilling third country.

5.2.2 Accommodating the Legal Mechanisms for Data Transfers

The accommodation of the legal mechanisms for the transfer of personal data in the GDPR is the second legal requirement for data flow clauses in EU trade agreements. This requires a brief explanation of the relationship between secondary Union law and international law (Sect. 5.2.2.1) before it is possible to discuss the implications for data flow clauses in FTAs of the EU (Sect. 5.2.2.2).

5.2.2.1 The Relationship of Secondary Union Law and International Law

International law is above secondary Union law in the hierarchy of the legal order in the EU (Sect. 5.2.2.1.1). The ECJ may review secondary Union law in light of an EU international agreement in an annulment procedure according to Article 263 TFEU or in a preliminary ruling procedure according to Article 267(b) TFEU. However, the ECJ has not always acknowledged international agreements concluded by the EU as a standard for the review of secondary Union law. The question of review has been linked to the issue of the direct effect of international agreements (Sect. 5.2.2.1.2).

5.2.2.1.1 Hierarchy in the Legal Order

Subject to the EU Treaties, institutions of the Union and its member states are bound by international agreements through Article 216 TFEU. International law holds a

superior position in the hierarchy of the EU legal order than secondary Union law.[76] Given the primacy of international law over secondary Union law, the courts of the EU and its member states must ensure that secondary Union law and national legislation is interpreted as far as possible in conformity with the obligations contained in international agreements concluded by the EU.[77] However, a conforming interpretation is not possible in circumstances in which secondary Union law or national legislation clashes with an international agreement, and in which conformity would lead to an interpretation *contra legem*. [78]

5.2.2.1.2 Review of Secondary Law in Light of International Agreements by the European Court of Justice

It follows from the hierarchy of the EU legal order that the lawfulness of secondary Union law, which is contrary to an EU international agreement, may be reviewed by the ECJ in an annulment procedure according to Article 263 TFEU or in a preliminary ruling procedure according to Article 267(b) TFEU.[79] However, the ECJ has not always acknowledged international agreements concluded by the EU as a standard for the judicial review of secondary Union law. The question of review has been linked to the issue of direct effect of international agreements.[80]

Direct effect exists when the contracting parties so indicate in the terms of an agreement.[81] Until recently, it was rare that the EU and the other contracting party or parties addressed the issue of direct effect in a trade agreement.[82] Given the lack of presumption of direct effect in international agreements that are binding on the EU, it is often left to the ECJ to decide whether a provision has direct effect or not. The ECJ has repeatedly pointed out that the interpretative liberty to determine direct effect in international agreements is based on the fact that agreements contain no explicit provisions on the issue. The ECJ stressed that in conformity with the principles of international law, "Community institutions which have the power to negotiate and conclude an agreement [...] are free to agree with that country what effect the provisions of the agreement are to have in the internal legal order of the contracting

[76] Cp. ECJ, *IATA and ELFAA*, para. 35 and ECJ, *Commission v. Germany*, C-61/94, para. 52; Lenaerts (2010), p. 519; see generally Barnard and Peers (2017), p. 196; Van Vooren and Wessel (2014), p. 211; Lenaerts and Van Nuffel (2011), pp. 862–863.

[77] Van Waeyenberge and Pecho (2014), p. 752; see generally Van Vooren and Wessel (2014), pp. 238–240; Eeckhout (2011), pp. 355–357.

[78] ECJ, AG Opinion, *Rízení Letového Provozu*, para. 58; Lenaerts (2010), p. 519.

[79] Mohay (2017), p. 159; Craig and de Búrca (2017), pp. 371–372; Lenaerts and Van Nuffel (2011), pp. 871–873.

[80] Van Waeyenberge and Pecho (2014), p. 753; Craig and de Búrca (2017), pp. 368–369; Eeckhout (2011), p. 297.

[81] ECJ, *Portugal v. Council*, para. 34.

[82] Cp. Van Waeyenberge and Pecho (2014), p. 753.

parties."[83] In the absence of an agreement between the contracting parties on the effect of the provisions of the agreement in the internal legal orders, the ECJ considers whether the nature or broad logic of an agreement precludes direct effect, and, whether the provision in question is, as regards its content, unconditional and sufficiently precise.[84]

The EU started to depart from its conventional approach in 2010 by breaking the silence with regard to the direct effect of trade agreements in the internal legal order.[85] The Council Decision approving the trade agreement with the Republic of Korea explicitly stated that the agreement shall not be construed as conferring rights or imposing obligations which can be directly invoked before Union or member state courts.[86] Subsequently concluded trade agreements have usually included a general clause with similar effect.[87] For example, Article 30.6(1) CETA provides that nothing in the agreement should be construed as conferring rights or imposing obligations on persons other than those created between the parties under public international law, nor as permitting the agreement to be directly invoked in the domestic legal systems of the parties. Such a provision prevents a trade agreement from being directly invoked before Union and member states courts. It also blocks the possibility of using a trade agreement as a standard for the judicial review of secondary Union law.

5.2.2.2 Implications for the Design of Data Flow Clauses

The possibility to review the legal mechanisms for the transfer of personal data in the GDPR for compatibility with a data flow clause in a trade agreement depends on the direct effect of the provision and the trade agreement in question. As long as a Council decision approving the trade agreement, or the agreement itself, entails a provision that excludes direct effect of the agreement, then the legal mechanisms for data transfers in the GDPR cannot be reviewed for their compatibility with the trade agreement in question. The inclusion of such a provision is important to safeguard the EU regulation of data transfers from potential challenges.

Recital (102) GDPR explicitly allows the conclusion of international agreements which involve the transfer of personal data to third countries, insofar as such

[83] ECJ, *Air Transport Association of America*, para. 49; ECJ, *Kupferberg*, para. 17.

[84] ECJ, *FIAMM*, para. 110; ECJ, *Intertanko*, para. 45; ECJ, *IATA and ELFAA*, para. 39; ECJ, *International Fruit Company*, paras 19–20; see generally Lenaerts and Van Nuffel (2011), p. 865; Van Vooren and Wessel (2014), pp. 227–233.

[85] Semertzi (2014), p. 1127.

[86] Article 8 Council Decision 2011/265/EU 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 [2011] OJ L 117/1.

[87] Semertzi (2014), p. 1131.

agreements do not affect the GDPR and include an appropriate level of protection for the fundamental rights of the data subjects:

> This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects.

Data flow clauses of the EU should be designed in a way that accommodates the legal mechanisms for the transfer of personal data in the GDPR as an implementation of the trade agreement. Data flow clauses should not replace the legal mechanisms for the transfer of personal data in the GDPR because these mechanisms provide the necessary details for safe, cross-border flows of personal data. I have already argued that a commitment to the free flow of personal data across borders in an EU trade agreement must guarantee that such data flows can be restricted in case the level of protection for personal data is not essentially equivalent to that guaranteed within the EU when personal data is transferred to the contracting party or parties. This is important to safeguard decisions of supervisory authorities to ban or suspend data transfers according to Article 58(2)(f) and (j) GDPR, especially on the basis of instruments providing appropriate safeguards in Article 46 GDPR.

5.2.3 Including Cooperation for the Protection of Personal Data

The inclusion of a provision on cooperation for the protection of personal data is the third legal requirement for data flow clauses in EU trade agreements. A provision in Chapter V of the GDPR on transfers of personal data is specifically dedicated to international cooperation for the protection of personal data:

> **Article 50 International cooperation for the protection of personal data**
> In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:
>
> (a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;
> (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;
> (c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

Article 50 GDPR clearly encourages the EU to develop the means for cooperating with third countries in the field of data protection. The proliferation of data protection laws around the world, as well as the extraterritorial dimension of EU data protection law, make it necessary for the EU to interact with other data protection systems, both politically and legally.[88] The provision entails that the Commission has the broadest powers to engage in tasks relating to international outreach and cooperation in the field of data protection.[89] The Commission has already announced that it "will continue to engage actively in dialogue with its international partners, at both bilateral and multilateral level, to foster convergence by developing high and interoperable personal data protection standards globally."[90]

Article 50(a) and (b) GDPR focus on cross-border enforcement of legislation for the protection of personal data. Article 50(c) GDPR stresses that relevant stakeholders should be engaged in these discussions. Article 50(d) GDPR refers more generally to the promotion of exchange on data protection legislation. Recital (116) GDPR underlines that the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in accordance with the GDPR. With regard to the transfer of personal data, the powers of the Commission include among other things the adoption of adequacy decisions, and the powers of the supervisory authorities include among other things corrective actions in the form of a suspension or a ban on data transfers using instruments providing appropriate safeguards such as standard data protection clauses. The two examples require assessments of the level of protection for personal data that is transferred to a third country. These assessments must be independent. However, cooperative instruments in a trade agreement could facilitate a dialogue to improve the level of data protection in a third country in which the existing protection is not considered to be adequate.[91] In addition, the Commission and the supervisory authorities are also responsible for approving the new data transfer instruments and providing appropriate safeguards in the GDPR, such as codes of conduct and certifications. It could be useful to establish cooperative instruments in a trade agreement to exchange information on how these mechanisms work.

The EU has already included provisions on cooperation for the protection of personal data in Article 201(1) of the EU-CARIFORUM EPA from 2008.[92]

[88] Kuner (2020), pp. 858–859.

[89] Ibid., 860.

[90] European Commission (2017a), p. 11.

[91] Cp. Mancini (2020), p. 205; But see Robert Wolfe arguing that "a trade agreement might not be the best vehicle for regulatory cooperation [. . .], if the objective is some form of equivalence." Wolfe (2019), pp. 65–66.

[92] See Sect. 5.1.2.2.

> The Parties acknowledge the importance of cooperation in order to facilitate the development of appropriate legislative, judicial and institutional frameworks as well as an adequate level of protection of personal data consistent with the objectives and principles contained in this Chapter.

However, the EU also changed its approach to cooperation for the protection of personal data in later trade agreements. Although the CETA is an innovation when it comes to regulatory cooperation, data protection is not considered at all. The Cooperation Forum established by the CETA creates a formal mechanism to facilitate dialogue between Canadian and EU regulatory authorities. Chapter 21 of the CETA on regulatory cooperation encourages regulators to exchange experiences and information and identify areas in which cooperation could occur. All cooperation is voluntary and regulators in the EU and Canada retain their power to adopt legislation according to Article 21.2(4) and (6) CETA. Nevertheless, the chapter on regulatory cooperation in the CETA does not apply to electronic commerce.[93]

It can be observed that interest in regulatory cooperation with the EU in the field of data protection is high. Notably, the UK's proposal on a future partnership in the exchange and protection of personal data with the EU from 2018 advocated a partnership that includes "ongoing regulatory cooperation between the EU and the UK on current and future data protection issues, building on the positive opportunity of a partnership between global leaders on data protection."[94]

It is important to distinguish between two types of regulatory cooperation. Aaditya Mattoo describes regulatory cooperation that could be far-reaching and lead to harmonization or mutual recognition on the one hand, and regulatory cooperation that only involves greater mutual understanding of how regulatory discretion in each jurisdiction will be exercised on the other hand.[95] The latter form of cooperation is less intense, but it is equally valuable because it lends predictability to trade relations.

Regulatory cooperation for the protection of personal data in the EU must respect and guarantee the right to continuous protection for personal data in Article 8 CFR and accommodate the legal mechanisms for data transfers in the GDPR. Within these limits, regulatory cooperation may be used to improve the continuous protection for personal data that is transferred to third countries. The GDPR acknowledges in Recital (101) that flows of personal data to and from countries outside the EU are necessary for the expansion of international trade. Cooperation for the protection of personal data in trade agreements should not be seen as a red line, even if data protection is a fundamental right in the EU and its content is not negotiable. The Commission recently wrote in its communication on a European strategy for data

[93] However, regulatory cooperation for the protection of personal data could indirectly take place by means of regulatory cooperation on cross-border trade in services which is subject to regulatory cooperation according to Article 21.1 CETA. Cross-border flows of personal data are closely related to trade in services. Accordingly, cooperation on regulatory matters pertaining to data protection might not be totally excluded. Mancini (2020), p. 199.

[94] HM Government (2017), para. 22.

[95] Mattoo (2015), p. 7.

from 2020 that it is convinced that international cooperation must be based on an approach that promotes the EU's fundamental values, including protection of privacy.[96] It is of paramount importance that regulatory cooperation for the protection of personal data is led by data protection experts and not conducted by trade officials.[97] The EU should advance its own data protection rules as the baseline and conceive regulatory cooperation as a tool to reach greater convergence on data protection standards.[98]

5.2.4 Banning Other Data Localization Obligations

Some data localization obligations in third countries are not motivated by data protection or privacy. The European Commission observed in its communication on a European strategy for data from 2020 that "European companies operating in some third countries are increasingly faced with unjustified barriers and digital restrictions."[99] These restrictions may concern personal data but also non-personal data. The requirement to ban data localization obligations that are not motivated by data protection or privacy can be found in the GDPR and in Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union.[100]

With regard to personal data, Article 1(3) GDPR states that the free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. If an EU member state imposes localization requirements on personal data that are not motivated by data protection or privacy, then they will have to be assessed against the provisions on the fundamental freedoms and the permitted ground to derogate from those freedoms in the TFEU.[101] For example, the exceptions in Article 52(1) TFEU enable EU member states to retain restrictions on the free movement of services in respect of public policy, public security, and public health. Recital (101) GDPR acknowledges that flows of personal data to and from countries outside the Union are necessary for the expansion of international trade. It implies that restrictions on cross-border flows of personal data that are not motivated by data protection or privacy should also be banned on the international level wherever possible. Such a ban, however, must be accompanied with exceptions

[96] European Commission (2020), p. 23.

[97] Mancini (2020), p. 200; Irion and Bartl (2017), p. 10.

[98] Mancini (2020), p. 205.

[99] European Commission (2020), pp. 23–24; see also Mancini (2020), p. 205; Hodson (2019), p. 581; Peng and Liu (2017), pp. 187–192.

[100] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L 303/59.

[101] European Commission (2019), p. 13; see for example ECJ, *Commission v Grand Duchy of Luxemburg*, paras 90–91.

similar to those in EU law. The Commission observed in its Communication for a European strategy for data from 2020 that, without prejudice to the EU's framework for the protection of personal data, the "free and safe flow of data should be ensured with third countries, subject to exceptions and restrictions for public security, public order and other legitimate public policy objectives of the European Union."[102] Such a solution can be applied to trade agreements.

The restriction of cross-border flows of non-personal data is a subject that has not been addressed in this research so far. There should be data protection in trade agreements without data protectionism in the form of restrictions on cross-border flows of non-personal data. In 2018, the EU adopted Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the EU. The regulation aims to ensure the free flow of non-personal data within the Union by establishing rules relating to data localization requirements. Recital (18) Regulation (EU) 2018/1807 states that data localization requirements in the EU represent a clear barrier to the free provision of data processing services across the Union.[103] This is why, according to Article 4(1) Regulation (EU) 2018/1807, data localization requirements in the EU are prohibited—unless they are justified on grounds of public security in compliance with the principle of proportionality. The prohibition of data localization requirements in the EU are far-reaching. Recital (13) Regulation (EU) 2018/1807 explicitly states that, given the large amounts of data which public authorities handle, it is of the utmost importance that public authorities lead by example and refrain from imposing data localization requirements when they use data processing services.

The prohibition of data localization requirements for non-personal data in the EU should be replicated in trade agreements. However, the exceptions should not be limited to public security. Recital (18) Regulation (EU) 2018/1807 clarifies the intention of the regulation to limit the justification for data localization requirements in the EU to public security in Article 4(1) Regulation (EU) 2018/1807:[104]

> In order to give effect to the principle of free flow of non-personal data across borders, to ensure the swift removal of existing data localisation requirements and to enable, for operational reasons, the processing of data in multiple locations across the Union, [...] Member States should only be able to invoke public security as a justification for data localisation requirements.

Panos Koutrakos argues that public security is most closely associated with what is traditionally understood as the core of national sovereignty, that is, the sphere of

[102] European Commission (2020), pp. 23–24.

[103] Article 3(5) Regulation (EU) 2018/1807 defines data localization as any obligation, prohibition, condition, limit or other requirement provided for in the laws, regulations or administrative provisions, which imposes the processing of data in the territory of a specific Member State or hinders the processing of data in any other Member State.

[104] Somaini (2020), p. 88.

activity within which the state has primary responsibility to protect its territory and citizens.[105] The Council summarized that public security

> presupposes the existence of a genuine and sufficiently serious threat affecting one of the fundamental interests of society, such as a threat to the functioning of institutions and essential public services and the survival of the population, as well as by the risk of a serious disturbance to foreign relations or the peaceful coexistence of nations, or a risk to military interests.[106]

Kristina Irion argues that the public security exception is too narrow because it precludes EU member states from taking measures that can be justified on grounds of public policy or the protection of health of humans, animals or plants.[107] This should be considered in the exceptions to the data flow clauses in EU trade agreements.

5.2.5 Summary

The scope for data flow clauses in EU trade agreements is determined by several legal requirements stemming from the architecture of Union law, the GDPR, and other regulations. The most important requirement is the primacy of fundamental rights over international law. Any data flow clause in an EU trade agreement must respect the right to continuous protection of personal data found in Article 8 CFR. The ECJ has two important competences with regard to the subordination of international law: The Court can *a priori* examine the lawfulness of a proposed international agreement according to the opinion procedure and the Court can *a posteriori* review the lawfulness of an international agreement in an annulment procedure or in a preliminary ruling procedure. Furthermore, data flow clauses in EU trade agreement should be designed in a way that can accommodate the legal mechanisms for the transfer of personal data in the GDPR. The data flow clauses should *not* replace the legal mechanisms for the transfer of personal data in the GDPR because these mechanisms provide the necessary details for safe data transfers. In addition, the Council decision approving a trade agreement, or the trade agreement itself, should include a provision that precludes the direct effect of the agreement to formally exclude the review of the legal mechanisms for the transfer of personal data in the GDPR for their compatibility with the trade agreement in question. The data flow clauses should also include a provision on cooperation for the protection of personal data in line with the objectives of Article 50 GDPR. Lastly, Recital (101) GDPR acknowledges that flows of personal data to and from countries outside the Union are necessary for the expansion of international trade. This implies that restrictions on cross-border flows of personal data that are not

[105] Koutrakos (2016), p. 192.
[106] Council of the EU (2017), Recital (12a).
[107] Irion (2018), p. 9.

motivated by data protection or privacy should be banned. Such a ban must be accompanied with exceptions similar to those in place in EU law.

5.3 Designs for Data Flow Clauses in EU Trade Agreements

The third section of this chapter is dedicated to the design of data flow clauses in EU trade agreements. There are two options to deal with the primacy of fundamental rights over international law in cases in which the EU negotiates data flow clauses for a trade agreement.[108] The first option does not include a commitment to the free flow of personal data across borders and focuses on carving-out data protection from an agreement. The second option includes a commitment to the free flow of personal data across borders and focuses on aligning this commitment with the right to continuous protection of personal data in Article 8 CFR. The following suggestions for the design of data flow clauses in EU trade agreements all include a commitment to the free flow of personal data across borders. Such a commitment by the EU must guarantee that data transfers can be restricted if the level of protection for personal data is not essentially equivalent to that guaranteed within the EU when personal data is transferred to the contracting party or parties. This section introduces four suggestions for the design of data flow clauses in EU trade agreements and describes their advantages and shortcomings with regard to the legal requirements described above.[109] The four suggestions are: a data flow obligation with a privacy exception (Sect. 5.3.1), a data flow obligation with an adequacy exception (Sect. 5.3.2), a data flow obligation with an adequacy condition (Sect. 5.3.3), and a data flow obligation with data protection obligations (Sect. 5.3.4).

5.3.1 Data Flow Obligation with a Data Protection Exception

The first suggestion for an EU data flow clause consists of a data flow obligation and a data protection exception. The combination of a data flow obligation and a data protection (or privacy) exception is also used in the CPTPP, the Sri Lanka-Singapore trade agreement, the USMCA, and the US-Japan Digital Trade Agreement. Nevertheless, there are certain crucial differences between these trade agreements. For example, the data flow obligations in Article 14.11(2) CPTPP and in Article 9.9(2) Sri Lanka-Singapore trade agreement are worded positively (each party shall allow the cross-border transfer of personal data), whereas the data flow obligations in Article 19.11(1) USMCA and in Article 11(1) US-Japan Digital Trade Agreement

[108] See Sect. 5.2.1.2.

[109] The designs do not address cooperation for the protection of personal data and the banning of other data localization requirements in detail.

are worded negatively (no party shall prohibit or restrict the cross-border transfer of personal data). For a data flow obligation in a EU trade agreement, it would be advisable to follow the CPTPP model and provide a positively worded obligation that focuses on allowing cross-border flows of personal data and to refrain from an explicit prohibition to restrict such data flows. The positive obligation leaves more room to accommodate the legal mechanisms for the transfer of personal data in the GDPR.

Two paragraphs should precede the data flow obligation in the design of the clause. The first paragraph should recognize and state that the protection of personal data is a fundamental right, and that the protection of personal data must continue when it is transferred across borders. The second paragraph should recognize and state that the parties may have their own regulatory requirements concerning the transfer of personal data. The data flow obligation must be read and interpreted in light of these two paragraphs. With regard to the EU regulation of data transfers, these two paragraphs and the data flow obligation could accommodate the legal mechanisms for the transfer of personal data. This includes—in the absence of an adequacy decision according to Article 45 GDPR—the instruments providing appropriate safeguards according to Article 46 GDPR and the derogations in Article 49 GDPR.

The data protection exception must cover restrictions on cross-border flows of personal data that are imposed because of the level of protection for personal data existing in the third country contracting party for the transferred data. Such an exception should be applicable when the European Commission revokes or the ECJ invalidates an adequacy decision for a contracting party, and when a supervisory authority in an EU member state uses its corrective powers in Article 58(2)(f) and (j) GDPR to suspend or ban transfers of personal data to a contracting party.

There are important differences in the formulation of such an exception among the existing data flow clauses in trade agreements. These differences are decisive for the justification of restrictions on cross-border data flows for data protection or privacy. The least permissive exceptions can be found in Article 19.11(2) USMCA and Article 11(2) US-Japan Digital Trade Agreement. According to these exceptions, measures that are inconsistent with the data flow obligation must be necessary to achieve a legitimate public policy objective, they may not constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade, and they may not impose restrictions that are greater than necessary to achieve the objective. The last condition constitutes a second necessity test and is further qualified in a footnote. Measures do not meet the second necessity test if they accord different treatment to cross-border flows of personal data solely on the basis that they are cross-border in a manner that modifies the conditions of competition to the detriment of a covered person. This qualification makes it difficult to accommodate legal mechanisms for the transfer of personal data that require additional safeguards for cross-border flows of personal data. It is not certain if the EU regulation of data transfers could be justified under the exceptions in Article 19.11(2) USMCA and Article 11(2) US-Japan Digital Trade Agreement because of the second necessity test.

The most permissive exception can be found in Article 9.9(3) Sri Lanka-Singapore trade agreement. Any restriction on the cross-border flow of personal data to achieve a legitimate public policy objective must not be applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination, or a disguised restriction on trade. This version of an exception is suitable for the EU. The exception does not entail a necessity test. A necessity test could potentially put pressure on the legal mechanisms for data transfers in the GDPR. The absence of a necessity test allows the parties to have their own regulatory systems for cross-border flows of personal data. The standards of arbitrary and unjustifiable discrimination and disguised restrictions on trade should be easy to satisfy for the EU in a bilateral trade agreement, as long as the EU regulation of data transfers is applied in good faith and respects due process. In a multilateral trade agreement, it is important for the Commission and the supervisory authorities to apply the EU regulation of data transfers equally in comparable situations to all contracting parties. As long as this is the case, these standards should not be a problem in a multilateral trade agreement either. Against this background, the first design for a data flow clause with a data flow obligation and a data protection exception could look like this:

Data Flow Clause Design One

1. The Parties recognize that data protection is a fundamental right and that the protection of personal data must continue when it is transferred across borders.
2. It is recognized that each Party may have its own regulatory requirements concerning the transfer of personal data.
3. The Parties allow the cross-border transfer of personal data when this activity is for the conduct of the business of a covered person.
4. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 3 of this Article to protect the privacy or the personal data of individuals, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade.

The advantages of any trade agreement that includes a commitment to the free flow of personal data is the reciprocity of the commitment. The GDPR only regulates the transfer of personal data from the EU to third countries. Inbound flows of personal data are not guaranteed but can be addressed in a trade agreement. The disadvantage of this design for a data flow clause is that the justification for a restriction on cross-border flows of personal data lies with the defendant. Should a contracting party challenge an EU restriction on cross-border flows of personal data, the EU would have to prove that the restriction is for the protection of personal data. However, the proof seems to be easy on the basis of a reflected decision by the Commission or a supervisory authority.

5.3.2 *Data Flow Obligation with an Adequacy Exception*

The second suggestion for the design of a data flow clause in EU trade agreements consists of a data flow obligation and an adequacy exception. There is no model for such a data flow clause in any current trade agreement. It is a design for a data flow clause that is tailored to EU-style data protection, but should also be acceptable to the contracting parties. Just as the previous design, the first paragraph should recognize and state that the protection of personal data is a fundamental right and that the protection of personal data must continue when it is transferred across borders. The second paragraph should recognize and state that the parties may have their own regulatory requirements concerning the transfer of personal data. The third paragraph should entail the data flow obligation and the fourth paragraph should entail the adequacy exception. The second design for a data flow clause with a data flow obligation and an adequacy exception could look like this:

Data Flow Clause Design Two

1. The Parties recognize that data protection is a fundamental right and that the protection of personal data must continue when it is transferred across borders.
2. It is recognized that each Party may have its own regulatory requirements concerning the transfer of personal data.
3. The Parties allow the cross-border transfer of personal data when this activity is for the conduct of the business of a covered person.
4. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 3 of this Article to guarantee that transfers of personal data only take place subject to an adequate level of protection.

The language used in the adequacy exception would accommodate restrictions on data transfers in cases in which the protection for personal data that is transferred to a contracting party is not adequate to EU standards. The ECJ defined in *Schrems* that an adequate level of protection for personal data is a level of protection that is essentially equivalent to that guaranteed within the EU.[110] The adequacy exception is a strong expression of the right to continuous protection of personal data in Article 8 CFR and accommodates the legal mechanisms for the transfer of personal data in the GDPR. However, international agreements must be interpreted according to the rules in Articles 31-33 VCLT. It is possible that an interpretation of the term "adequate level of protection" on the basis of the VCLT leads to different results than the interpretation in EU law, which could undermine the right to continuous protection of personal data in Article 8 CFR.[111] The situation is even more complicated

[110] ECJ, *Schrems*, para. 73.

[111] Svetlana Yakovleva argues that given the fragmentation of standards on privacy and data protection and the absence of a single reference point, the interpretation of terms such as "adequate" or "appropriate" have no precise obligational content. Yakovleva (2018), p. 195.

because the level of protection guaranteed within the EU is subject to developments in Union law.

This disadvantage of the second design could be resolved with a reference in a footnote that the definition of an adequate level of protection is up to each party. This does not have to weaken the commitment to the free flow of personal data as long as the contracting parties maintain a rule-based system to determine when transfers of personal data may or may not take place based on the level of protection for personal data, and as long as such determinations are open to judicial review. For example, in the EU the independent supervisory authorities have the power to suspend or ban data transfers in cases in which the protection for personal data is not essentially equivalent to that guaranteed within the EU. However, the use of this power is subject to judicial review. It is suggested that the second design is a valid option when the contracting parties have a similar system in place. Without a similar system, the data flow obligation could easily be circumvented with political decisions by a contracting party with a protectionist agenda.

Another disadvantage of this design is—similar to the first design—that the justification for a restriction of data flows lies with the defendant. Should a contracting party challenge an EU restriction on cross-border flows of personal data, the EU would have to prove that the level of protection for personal data that is transferred to the contracting party is not adequate. While this proof is more difficult than the one required in the first design, the respective decisions by the Commission or a supervisory authority provide a good basis to satisfy the burden of proof.

5.3.3 Data Flow Obligation with an Adequacy Condition

The third suggestion for the design of a data flow clause in EU trade agreements combines a data flow obligation with an adequacy condition. It is similar to the second design but instead of integrating the adequacy criterion in the exception, it is formulated as a condition for the commitment to the free flow of personal data in paragraph 3. The third design could look like this:

Data Flow Clause Design Three

1. The Parties recognize that data protection is a fundamental right and that the protection of personal data must continue when it is transferred across borders.
2. It is recognized that each Party may have its own regulatory requirements concerning the transfer of personal data.
3. The Parties allow the cross-border transfer of personal data when this activity is for the conduct of the business of a covered person and the level of protection for the personal data that is transferred is adequate.

The advantage of this design over the second design is that the defendant does not bear the burden of proof because the criterion for an adequate level of protection is

not integrated as an exception. Should a contracting party challenge an EU restriction on cross-border flows of personal data, it must also prove that the level of protection for personal data that is transferred from the EU to its territory is adequate. However, there is a similar disadvantage as in the second design concerning the interpretation of an "adequate" level of data protection according to the rules of the VCLT. A solution could be a provision on cooperation that establishes a dialogue on adequate protection for personal data. The documentation of that dialogue could be used as a supplementary means of interpretation according to Article 32 VCLT.

5.3.4 Data Flow Obligation with Data Protection Obligations

The fourth suggestion for the design of a data flow clause in EU trade agreements entails different obligations: a data flow obligation and several data protection obligations. The design of the data flow clause is the same as the third design with an adequacy obligation and an adequacy condition, but in addition to the data flow clause, the trade agreement in this fourth design would have a separate chapter on data protection. This chapter should entail several data protection obligations that are the basis for an adequate level of protection for personal data.

The fourth design builds upon the approach taken by the EU in the EU-CARIFORUM EPA and the EU-Central Africa EPA.[112] These trade agreements each have a separate chapter on data protection. The chapters define important terms such as "personal data" and the "processing of personal data" as well as "data controller." It is especially important that the term data controller also includes public authorities to incorporate internet surveillance practices within the scope of the agreement. The chapters also include an agreement between the contracting parties that the legal and regulatory regimes should include content principles such as purpose limitation, data quality and proportionality, transparency, security, rights of access, rectification and opposition as well as rules on onward transfers of personal data and sensitive data. The agreement between the contracting parties also extends to the establishment of enforcement mechanisms to ensure a good level of compliance, to provide support and help to individual data subjects in the exercise of their rights, and to provide appropriate redress to injured parties. In spite of these first attempts by the EU to formulate the conditions for an adequate level of protection for personal data in trade agreements, the EU seems skeptical to go further with substantive data protection obligations in trade agreements. During a meeting of the WTO Council for Trade in Services in 2015, a representative of the EU recalled the Union's position that "trade agreements should not go beyond affirming those general principles and should not set substantive standards on personal data protection."[113]

[112] See Sect. 5.1.1.2.

[113] WTO (2015), para. 4.30.

Svetlana Yakovleva argues that the EU Treaties require that the negotiation and conclusion of trade agreements be guided by the universality and indivisibility of human rights and fundamental freedoms, respect for human dignity and principles of the UN and international law, and—in order to remain faithful to these requirements—that the EU maintain its autonomy to protect personal data as a fundamental right, and not just as an instrument to generate consumers' trust.[114] While this position can be agreed with, it does not eliminate the possibility of including data protection obligations in a trade agreement. The European Commission stated that "[i]n particular, an adequacy finding is a unilateral implementing decision by the Commission in accordance with EU data protection law, based on the criteria therein."[115] However, the EU does not explain why the inclusion of data protection obligations in trade agreements is a red line. An explanation could be the loss of authority over the interpretation of such obligations and standards. I would argue, however, that as long as the data flow clause accommodates the legal mechanisms for the transfer of personal data in the GDPR, including the ability of the Commission to take and revoke adequacy decisions and the power of supervisory authorities to suspend or ban the transfer of personal data, then the inclusion of data protection obligations in trade agreements would not undermine the fundamental right to continuous protection of personal data.

The advantage of the fourth design over the third design is that the trade agreement itself provides the basis for the expectations of an adequate level of protection for personal data with the data protection obligations in a specific chapter of the trade agreement. A provision on cooperation should be added that establishes a dialogue on adequate protection for personal data. The documentation of that dialogue could be used as supplementary means of interpretation according to Article 32 VCLT.

5.3.5 Summary

There are different possibilities for designing data flow clauses, should a commitment to the free flow of personal data across borders be integrated into an EU trade agreement. Any design for a data flow clause in a trade agreement of the EU must respect the legal requirements for data flow clauses discussed in the previous section. The four suggestions that were presented in this section all respect the primacy of fundamental rights over international law, which includes the primacy of the right to continuous protection for personal data in Article 8 CFR, and accommodate the legal mechanisms for the transfer of personal data in the GDPR. The first design combines a data flow obligation with a general data protection exception. The second design uses a more specific adequacy exception. The disadvantage of these designs is that

[114] Yakovleva (2018), p. 480.

[115] European Commission (2017a), p. 9, fn. 42.

the justification for a restriction on cross-border flows of personal data lies with the defendant. The EU would have to prove that a measure is taken for the protection of personal data that is transferred to the contracting party (in case of the first design) or that the level of protection for personal data in the territory of the contracting party is not adequate (in case of the second design).

The third design combines a data flow obligation with an adequacy condition. In this design, the parties allow the cross-border transfer of personal data when the level of protection for the personal data that is transferred is adequate. The advantage of this design is that the EU would not bear the burden of proof because the criterion of an adequate level of protection is not integrated as an exception. The term "adequate level of protection," however, might have a different meaning in trade agreements than in EU law based on interpretations according to the VCLT. This could provoke problems with the right to continuous protection of personal data in Article 8 CFR. A footnote referring to an autonomous definition of the term could prevent such problems. Another solution could be a provision for cooperation that establishes a dialogue on adequate protection for personal data. The documentation of that dialogue could be used as a supplementary means of interpretation according to Article 32 VCLT. The fourth design for a data flow clause is the same as the third design with an adequacy obligation and an adequacy condition, but in addition a separate chapter on data protection. The advantage of the fourth design over the third design is that the trade agreement itself provides the basis for the expectations of an adequate level of protection for personal data with the data protection obligations in a specific chapter of the trade agreement.

5.4 The Model Data Flow Clauses for EU Trade Agreements

The fourth section of this chapter is dedicated to the model data flow clauses for EU trade agreements. In January 2018, the European Commission endorsed horizontal provisions for cross-border data flows and personal data protection as a model for the future negotiation of trade agreements. A team led by the First Vice-President of the European Commission, Frans Timmermans, has looked into how best to advance the EU's data protection interests in trade negotiations.[116] The result of these efforts are analyzed in this section.[117] The EU opted for an approach that does not include a

[116] The EU has already included these clauses in its proposals for currently negotiated trade agreements with New Zealand, Australia, Chile, Mexico, Indonesia, and Tunisia, as well as in its proposal for the recent WTO negotiations on electronic commerce. See European Commission (2018).

[117] Apart from the document containing the text of the horizontal provisions for cross-border data flows and personal data protection, there are no other official documents from the European Commission on the development, background or interpretation of the model data flow clauses for EU trade agreements.

commitment to the free flow of personal data across borders.[118] The EU model data flow clauses address data protection as a fundamental right (Sect. 5.4.1), introduce a ban on data localization requirements not motivated by data protection or privacy (Sect. 5.4.2), carve-out space for the regulation of data protection from the scope of trade agreements (Sect. 5.4.3), and reject regulatory cooperation in the field of data protection (Sect. 5.4.4).

5.4.1 Addressing Data Protection as a Fundamental Right

Article B of the EU model data flow clauses is dedicated to the protection of personal data and privacy. The first paragraph of Article B addresses data protection and privacy as fundamental rights:

> **Article B Protection of personal data and privacy**
> 1. Each Party recognises that the protection of personal data and privacy is a fundamental right and that high standards in this regard contribute to trust in the digital economy and to the development of trade.

The first paragraph of Article B creates a common understanding among the contracting parties of data protection as a fundamental right.[119] The paragraph does not include the different written constituent parts of the right to data protection in Article 8 CFR, which would have been helpful to clarify the scope of the right to data protection. The paragraph also does not specifically refer to the importance of guaranteeing the protection of personal data in cases in which it is transferred across borders. Moreover, the right to continuous protection for personal data is not mentioned. The first paragraph simply constitutes an acknowledgment of the fundamental rights status of the protection of personal data and privacy. This acknowledgment is also connected to the fostering of trust in the digital economy and to the development of trade.[120] A similar rationale was used in Article 45 EU-Algeria AA from 2002, which was the earliest provision addressing cross-border flows of personal data in an EU trade agreement.[121] This paragraph in the EU model data flow clauses continues the EU's narrative according to which high standards of data protection are a precondition, and not a barrier, to international trade.

The only definition in Article B of the EU model data flow clauses concerns personal data:

---

[118] See Sect. 5.2.1.2. Cp. Mancini (2020), p. 195.
[119] Streinz (2019), p. 336.
[120] Velli (2019), p. 893.
[121] See Sect. 5.1.2.1.

Article B Protection of personal data and privacy
3. For the purposes of this agreement, 'personal data' means any information relating to an identified or identifiable natural person.

It was not considered necessary to include other definitions because the EU model data flow clauses do not entail obligations nor recommendations for domestic regulatory regimes to include data protection principles or enforcement mechanisms like the EU-CARIFORUM EPA from 2008 did. The EU removed all substantive reference to data protection principles from its model data flow clauses and did not include any data protection obligations. This might be a missed opportunity to create a deeper understanding of and commitment to the "high standards of data protection" that are referenced in the first paragraph of Article B. In addition, the EU could have used the term "adequate level of data protection" instead of "high standards of data protection" to be in line with the EU regulation of data transfers.

5.4.2 Banning Data Localization Requirements

Article A of the EU model data flow clauses addresses cross-border data flows without a distinction between personal and non-personal data:

Article A Cross-border data flows
1. The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted between the Parties by:
   (a) requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of a Party;
   (b) requiring the localization of data in the Party's territory for storage or processing;
   (c) prohibiting storage or processing in the territory of the other Party;
   (d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Parties' territory or upon localisation requirements in the Parties' territory.
2. The Parties shall keep the implementation of this provision under review and assess its functioning in 3 years following the entry into force of this Agreement. A Party may at any time propose to the other Party to review the list of restrictions listed in the preceding paragraph. Such request shall be accorded sympathetic consideration.

Article A of the EU model data flow clauses entails a commitment to the free flow of data across borders. In addition, it specifically bans data localization requirements

such as the use of domestic computing facilities for the processing and storage of data. However, an explicit carve-out in paragraph 2 of Article B of the EU model data flow clauses—which is addressed more below—ensures that the anti-localization provision cannot be directed against data protection and privacy rules.[122]

Article A of the model clauses is a manifestation of the EU's opposition to digital protectionism. The European Commission highlighted in a communication from 2017 on exchanging and protecting personal data in a globalized world that "European companies operating in some third countries are increasingly faced with protectionist restrictions that cannot be justified with legitimate privacy considerations."[123]

Data localization requirements in third countries are often motivated by privacy or security considerations.[124] While privacy-based data localization is allowed according to Article B of the EU model data flow clauses, it must be assumed that security-based data localization will be subject to general and security exceptions that are usually part of trade agreements. For example, the general exception in Article 28.3(2)(a) CETA applies to the electronic commerce chapter of the CETA and provides that nothing in the agreement shall be construed to prevent the adoption or enforcement by a party of measures necessary to protect public security or public morals or to maintain public order.[125] This exception for public security, public morals, and public order is further qualified in footnote 33 of the CETA and may only be invoked in cases in which a genuine and sufficiently serious threat is posed to one of the fundamental interests of society. It is suggested that such an exception could not be used to justify data localization that is presented as a protection of public security, but that is applied with a protectionist agenda. Similarly, a national security exception such as entailed in Article 28.6(b)(ii) CETA—echoing the language of Article XIV *bis* GATS—could not be used to generally justify security-based localization requirements. It is only applicable for the protection of essential security interests in time of war or other emergencies in international relations.[126] The ban on data localization in Article A of the EU model data flow clauses could therefore successfully prohibit security-based localization requirements for personal and non-personal data pursued by a contracting party with a protectionist agenda.

In addition, the application of general exceptions to the ban of data localization practices in Article A of the EU model data flow clauses allows derogations for measures adopted for the protection of human, animal or plant life and health. The absence of such an exception in Regulation (EU) 2018/1807 on a framework for the

[122] Streinz (2019), p. 336; Yakovleva (2020), p. 495.

[123] European Commission (2017a), p. 3.

[124] Sargsyan (2016), p. 2222; Chander and Le (2015), pp. 718–721; Castro (2013), p. 1.

[125] Subject to the requirement that the measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the parties where like conditions prevail, or a disguised restriction on trade in services.

[126] See Sect. 4.4.2.

free flow of non-personal data in the EU for non-personal data has been criticized.[127] Considerations for the protection of human, animal or plant life and health would therefore be covered in a trade agreement.

5.4.3 *Carving-Out Space for the Regulation of Data Protection*

The second paragraph of Article B of the EU model data flow clauses is the most important one for the restriction of cross-border flows of personal data:

> **Article B Protection of personal data and privacy**
> 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.

The second paragraph of Article B allows the parties to adopt and maintain regulations for the protection of personal data and privacy, including rules for cross-border flows of personal data. It emphasizes that rules for cross-border flows of personal data are an integral part of the safeguards for the protection of personal data and privacy. The first sentence of paragraph 2 incorporates a subjective appropriateness test similar to that employed in national security exceptions.[128] Under this sentence, the parties enjoy wide discretion in determining what they deem appropriate to ensure the protection of personal data and privacy. This is opposed to the objective necessity test that can be found in Article 19.11(2) USMCA. In addition, the second sentence of paragraph 2 entails a complete carve-out for data protection and privacy safeguards. This means that nothing in the trade agreement may affect the safeguards for the protection of personal data and privacy adopted and maintained by the parties. Article B of the EU model data flow clauses is formulated in a way that makes restrictions on cross-border flows of personal data on the basis of the EU regulation of data transfers *a priori* not subject to the prohibition in Article A on restricting cross-border data flows.[129] Article B is a water-tight provision for any domestic data protection rule affecting cross-border flows of personal data. With this provision, the European Commission may keep its promise that EU data protection rules are not subject to trade negotiations.[130]

[127] Irion (2018), p. 9; see Sect. 5.2.4.
[128] Yakovleva (2020), p. 496.
[129] Ibid., 495.
[130] European Commission (2017a), p. 9.

At the same time, the carve-out for data protection and privacy safeguards may also be problematic. Jacqueline Yin stresses that the carve-out allows the parties to introduce data protectionism under the guise of data protection.[131] Similarly, Federica Velli argues that the carve-out could result in uncertainty for digital service suppliers inside and outside of the EU.[132] The EU model data flow clauses have no solution for data protection rules motivated by a protectionist agenda. For example, a requirement that a copy of all personal data must be stored in the jurisdiction in which it was collected before its transfer abroad is possible under the EU model data flow clauses in cases in which a contracting party declares that the requirement is necessary to safeguard data protection and/or privacy. The same is true for a requirement that the processing of personal data must take place in the jurisdiction in which it was collected before it is transferred abroad.

The EU model data flow clauses show that the EU treats data protection and international trade law as two separate tracks with little or no middle ground.[133] The EU uses international trade law to immunize its own regulation of data protection in the second paragraph of Article B. At the same time, the EU encourages contracting parties to adopt high data protection standards in the first paragraph of Article B. It does not use international trade law to establish obligations to substantiate high data protection standards. It uses EU law—in particular, the right to continuous protection for personal data in Article 8 CFR and the legal mechanisms for the transfer of personal data in the GDPR—to push third countries indirectly into adopting high data protection standards.

5.4.4 Rejecting Regulatory Cooperation for Data Protection

Article X of the EU model data flow clauses addresses cooperation on regulatory issues with regard to digital trade. The third paragraph of Article X rejects regulatory cooperation in the field of data protection:

Article X Cooperation on regulatory issues with regard to digital trade

1. The parties shall maintain a dialogue on regulatory issues raised by digital trade, which shall inter alia address the following issues:
   - the recognition and facilitation of interoperable cross-border electronic trust and authentication services;
   - the treatment of direct marketing communications;
   - the protection of consumers in the ambit of electronic commerce; and
   - any other issue relevant for the development of digital trade.

[131] Yin (2018).

[132] Velli (2019), p. 893.

[133] See Sect. 5.1.2.

2. Such cooperation shall focus on exchange of information on the Parties' respective legislation on these issues as well as on the implementation of such legislation.
3. For greater certainty, this provision shall not apply to a Party's rules and safeguards for the protection of personal data and privacy, including on cross-border data transfers of personal data.

Article X does not simply leave data protection out of the list of issues for cooperation and dialogue. The third paragraph of Article X explicitly mentions that the protection of personal data and privacy, including rules for cross-border flows of personal data, is excluded from cooperation.[134] Scholars and interest groups have underlined that this is a shortcoming. For example, the European Services Forum (ESF) bemoans the EU model data flow clauses for establishing that regulatory cooperation does not cover cross-border flows of personal data.[135] The ESF considers that this is a missed opportunity for the EU to better explain the GDPR. The EU should not hesitate to use a cooperation mechanism to promote its approach to data protection simply because a forum for dialogue is non-binding. Federica Velli also stresses that this exclusion prevents influences or negotiations to lower data protection standards, while at the same time underlining that the rejection of regulatory cooperation for data protection is a missed opportunity to promote the EU's position and discuss new developments in digital trade.[136] Similarly, Isabella Mancini emphasizes that the EU overlooked that data protection is an issue that arises across several diverse fields.[137] Finally, Mira Burri underlines that as the complexity of the data-driven society rises, enhanced regulatory cooperation seems indispensable for moving forward, since data issues cannot be covered by the mere 'lower tariffs, more commitments' stance in trade negotiations but entail the need for reconciling different interests and the need for oversight.[138]

It is not completely understandable why the EU explicitly excluded data protection from regulatory cooperation in trade agreements. Digital trade increasingly relies on cross-border flows of personal data and global divergences hamper trade. The EU could use regulatory cooperation mechanisms to nudge convergence while guaranteeing high standards of protection for the right to data protection in Article 8 CFR.[139] The EU should conceive regulatory cooperation as a venue to reach greater convergence for data protection standards. It has also been shown that Article 50 GDPR encourages the EU to develop means for cooperating with third countries. Previous EU trade agreements like the EU-CARIFORUM EPA and other trade agreements between third countries like the Costa Rica-Colombia trade agreement

[134] Streinz (2019), p. 336.
[135] ESF (2018), p. 2.
[136] Velli (2019), p. 893.
[137] Mancini (2020), p. 200.
[138] Burri (2021), p. 41.
[139] Ibid., 204.

include such cooperation provisions. The European Commission has stated in its recent communication on a European Strategy for Data from 2020 that it is convinced that international cooperation must be based on an approach that promotes the EU's fundamental values, including the protection of privacy.[140] Regulatory cooperation can be framed and organized in way that safeguards the right to continuous protection of personal data in Article 8 CFR.

5.4.5 Summary

The EU model data flow clauses underline the fact that high data protection standards contribute to trust in the digital economy and to the development of trade. In addition, the first paragraph of Article B creates a common understanding of data protection as a fundamental right. However, the paragraph does not include the different written constituent parts of the right to data protection in Article 8 CFR. Doing so would have been helpful to clarify its scope. The EU chose a strategy for its model data flow clauses that does not entail a commitment to the free flow of personal data across borders. The second paragraph of Article B allows the parties to adopt and maintain regulations for the protection of personal data and privacy, including rules for cross-border flows of personal data, without any conditions. The EU uses international trade law to immunize its own regulation of data protection. Nothing in the trade agreement may affect the safeguards for the protection of personal data and privacy adopted and maintained by the parties according to the second paragraph of Article B. At the same time, the EU model data flow clauses offer no solution to address protectionist data protection rules. As long as a contracting party justifies its restrictions on cross-border flows of personal data with the protection of personal data and privacy, they are exempt from the trade agreement. This is a consequence of completely excluding data protection rules from trade negotiations. The ban on data localization in Article A of the EU model data flow clauses concerns localization requirements based on other reasons than data protection or privacy. The ban is useful to target security-based data localization requirements motivated by a protectionist agenda. Considering that the EU model data flow clauses immunize data protection rules in the EU, it is not entirely clear why Article X of the EU model data flow clauses explicitly excludes data protection from regulatory cooperation. Article 50 GDPR challenges the EU to develop means for cooperating with third countries. Previous EU trade agreements like the EU-CARIFORUM EPA and other trade agreements between third countries like the Costa Rica-Colombia FTA include such cooperation provisions. The EU should conceive regulatory cooperation as a venue to reach greater convergence for data protection standards, precisely because it emphasizes in the first paragraph of

[140] European Commission (2020), p. 23.

Article B that high data protection standards also contribute to trust in the digital economy and to the development of trade.

5.5 Conclusion

In reaction to the stalemate in the multilateral trading system, international governance of digital trade has gradually shifted to bilateral and regional trade agreements.[141] It is therefore not surprising that countries have started to regulate cross-border flows of personal data outside the WTO in bilateral and regional trade agreements.

The EU has tried different approaches to address data protection and cross-border flows of personal data in its trade agreements over the past 20 years. The EU started to qualify data protection as a contributing factor in the elimination of barriers to cross-border data flows in the EU-Algeria AA from 2002. The EU then went on to underline the fundamental rights character of data protection and commit all involved parties to establishing data protection regimes, as well as appropriate administrative capacities, including independent supervision, in order to ensure an adequate level of protection and facilitate cross-border flows of personal data in the EU-CARIFORUM EPA from 2008. Then came a clear break with this strategy. The CETA from 2016 makes a clear distinction between domestic data protection regulation and international trade law.[142] The CETA does not contain any data protection obligations and there are no rules for cross-border flows of personal data in the trade agreement. In short, the EU separated the regulation of data protection from trade rules. The EU continued to do this in the EU-Japan EPA from 2018. Here, the parties agreed on a *rendez-vous* clause in the agreement and settled the issue with reciprocal adequacy decisions based on domestic data protection law. The EU's opposition to include a commitment on cross-border data flows was also a stumbling block in the negotiations of the TiSA and the TTIP in the late 2010s. In contrast, the CPTPP from 2018 or US-led trade agreements such as the USMCA from 2018 entail binding commitments for the cross-border flow of personal data. The USMCA imposes strict conditions on exceptions, including the standards from the *chapeau* of Article XIV GATS and two necessity tests. In contrast, the CPTPP leaves more room to accommodate data protection or privacy-based restrictions on cross-border flows of personal data.

The EU's reluctance to commit to the free flow of personal data across borders in trade agreements might be explained through an appeal to Union law: the right to continuous protection for personal data in Article 8 CFR, the GDPR, and other regulations impose requirements upon the EU. The most important requirement is the primacy of fundamental rights over international law in the EU. Any data flow

[141] López González/Ferencz, OECD Report 2018, 15.

[142] Irion and Bartl (2017), p. 5.

clause in an EU trade agreement must respect the right to continuous protection of personal data in Article 8 CFR. Furthermore, data flow clauses in an EU trade agreement should be designed in a way that accommodates the legal mechanisms for data transfers in the GDPR. The data flow clauses should not replace the legal mechanisms for the transfer of personal data in the GDPR because these mechanisms provide the necessary details for safe data transfers. The framework for data flow clauses also requires the inclusion of a provision on cooperation for the protection of personal data in EU trade agreements in line with the objectives of Article 50 GDPR. Recital (101) GDPR acknowledges that flows of personal data to and from countries outside the EU are necessary for the expansion of international trade. This implies that restrictions on cross-border flows of personal data that are not motivated by data protection or privacy should be banned.

However, there are different possibilities for combining these requirements with a commitment to the free flow of personal data across borders and integrating them in data flow clauses of EU trade agreements. Four suggestions for the design of data flow clauses in EU trade agreements were presented and all foregrounded the primacy of fundamental rights over international law from the perspective of EU law and all accommodated the legal mechanisms for the transfer of personal data in the GDPR.

The first design combines a data flow obligation with a general data protection exception. The second design uses a more specific adequacy exception. The disadvantage of these designs is that the justification for a restriction on cross-border flows of personal data lies with the defendant. The EU would have to prove that a measure is taken for the protection of personal data that is transferred to the contracting party (in case of the first design) or that the level of protection for personal data in the contracting party is not adequate (in case of the second design). The third design combines a data flow obligation with an adequacy condition. The parties allow the cross-border transfer of personal data in cases in which the level of protection for the transferred personal data is adequate. The advantage of this design is that the defendant does not bear the burden of proof because the criterion of an adequate level of protection is not integrated as an exception. However, the term "adequate level of protection" might have a different interpretation in trade agreements than in EU law based on interpretations according to the VCLT. This could provoke problems with the right to continuous protection for personal data in Article 8 CFR. A footnote referring to an autonomous definition of the term could prevent such problems. Another solution could be a provision on cooperation that establishes a dialogue on adequate protection for personal data. The documentation of that dialogue could be used as supplementary means of interpretation according to Article 32 VCLT. The fourth design for a data flow clause is the same as the third design with regards to containing an adequacy obligation and an adequacy condition, but it also has a separate chapter on data protection. The advantage of the fourth design over the third design is that the trade agreement itself provides the basis for an adequate level of protection for personal data.

The EU model data flow clauses, which the European Commission endorsed as a model for future negotiation of trade agreements in January 2018, do not contain a

commitment to the free flow of personal data across borders. Rather, they create a common understanding of data protection as a fundamental right without specifying its scope and underline that high data protection standards contribute to trust in the digital economy and to the development of trade. The EU model data flow clauses allow the parties to adopt and maintain regulations for the protection of personal data and privacy, including rules for cross-border flows of personal data, without any conditions. The EU uses international trade law to immunize its own regulation of data protection. Nothing in the trade agreement may affect the safeguards for the protection of personal data and privacy adopted and maintained by the parties. At the same time, the EU model data flow clauses offer no solution for addressing protectionist data protection rules. As long as a contracting party justifies its restrictions on cross-border flows of personal data under the protection of personal data and privacy, they are exempt from the trade agreement. The ban on data localization in the EU model data flow clauses only concerns localization requirements based on other reasons than data protection or privacy. This is useful to target security-based data localization requirements motivated by a protectionist agenda. Considering that the EU model data flow clauses immunize data protection rules in the EU, it is not entirely clear why they explicitly exclude data protection from regulatory cooperation. The EU should conceive regulatory cooperation as a venue to reach greater convergence for data protection standards, precisely because it emphasizes that high data protection standards also contribute to trust in the digital economy and to the development of trade. To combat data protectionism, while protecting its own data protection standards, the EU would be better advised to use one of the four proposed designs for data flow clauses.

References

Bibliography

Aaronson SA (2015) Why Trade Agreements are not setting information free: the lost history and reinvigorated debate over cross-border data flows, human rights, and national security. World Trade Rev 14(4):671–700

Aaronson SA, Townes MD (2012) Can trade policy set information free? Trade agreements, internet governance and internet freedom. George Washington University Policy Brief. Washington DC

Barents R (2004) The autonomy of community law. Kluwer Law, The Hague

Barnard C, Peers S (2017) European Union law, 2nd edn. Oxford University Press, Oxford

Berka W (2017) CETA, TTIP, TiSA and data protection. In: Griller S, Obwexer W, Vranes E (eds) Mega-Regional Trade Agreements: CETA, TTIP, and TiSA: new orientations for EU external economic relations. Oxford University Press, Oxford, pp 175–186

Burri M (2017) The governance of data and data flows in trade agreements: the pitfalls of legal adaptation. UC Davis Law Rev 51(1):65–133

Burri M (2019) Understanding and shaping trade rules for the digital era. In: Elsig M, Hahn M, Spilker G (eds) The shifting landscape of global trade governance. Cambridge University Press, Cambridge, pp 73–106

Burri M (2021) Data flows and global trade law. In: Burri M (ed) Big data and global trade law. Cambridge University Press, Cambridge, pp 11–41
Castro D (2013) The false promise of data nationalism. The Information Technology & Innovation Foundation. Washington DC
Chander A, Le UP (2015) Data nationalism. Emory Law J 64(3):677–739
Craig P, de Búrca G (2017) EU law, 6th edn. Oxford Academic, Oxford
Cremona M (2020) The Opinion procedure under Article 218(11) TFEU: reflections in the light of Opinion 1/17. Europe World A Law Rev 4(1):1–11
Eeckhout P (2011) EU external relations law, 2nd edn. Oxford University Press, Oxford
Fleming J (2013) Reding warns data protection could derail US trade talks. Euractive. 30 October 2013. https://www.euractiv.com/section/digital/news/reding-warns-data-protection-could-derail-us-trade-talks/. Accessed 3 January 2021
Fontoura Costa JA (2020) Data protection in international trade law. In: Moura VD, de Vasconcelos CS (eds) Data protection in the internet. Springer, Heidelberg, pp 479–517
Geist M (2018) How the USMCA falls short on digital trade, data protection and privacy. Washington Post. 3 October 2018. https://www.washingtonpost.com/news/global-opinions/wp/2018/10/03/how-the-usmca-falls-short-on-digital-trade-data-protection-and-privacy/. Accessed 3 January 2021
Greenleaf G (2014) Asian data privacy laws: Trade and human rights perspectives. Oxford University Press, Oxford
Greenleaf G (2018) Free Trade Agreements and data privacy. Future Perils of Faustian Bargains. In: Svantesson DJB, Kloza D (eds) Trans-Atlantic data privacy relations as a challenge for democracy. Intersentia, Cambridge, pp 181–212
Gstöhl S, Hanf D (2014) The EU's Post-Lisbon Free Trade Agreements: commercial interests in a changing constitutional context. Eur Law J 20(6):733–748
Irion K (2018) Public Security Exception in the Area of non-personal Data in the European Union. Research paper commissioned by the European Parliament Committee on the Internal Market and Consumer Protection. Amsterdam
Irion K, Bartl M (2017) The Japan EU Economic Partnership Agreement: Flows of Personal Data to the Land of the Rising Sun. Research paper commissioned by the European Parliamentary Group GUE/NGL. Amsterdam
Kelsey J, Kilic B (2014) Wikileaks Briefing on US TISA proposal on E-commerce, technology transfer, cross-border data flows and net neutrality. Washington DC
Koutrakos P (2016) Public Security Exceptions and EU Free Movement Law. In: Koutrakos P, Shuibhne NN, Sypris P (eds) Exceptions from EU Free Movement Law. Bloomsbury, Oxford, pp 190–217
Kuner C (2020) Chapter V transfers of personal data to third countries or international organisations (Articles 44-50). In: Kuner C, Bygrave L, Docksey C (eds) The EU general data protection regulation (GDPR). Oxford University Press, Oxford, pp 755–862
Lacey SBC (2020) Reality check: the lack of consensus on new trade rules to govern the digital economy. J World Trade 54(2):199–218
Lenaerts K (2010) Droit international et monisme de l'ordre juridique de l'Union. Revue de la faculté de droit de l'Université de Liège 46(4):505–520
Lenaerts K, Van Nuffel P (2011) European Union law, 3rd edn. Thomson Reuters, Sweet & Maxwell, London
López GJ, Ferencz J (2018) Digital trade and market openness. OECD Report, Paris
Mancini I (2020) Deepening trade *and* fundamental rights? Harnessing data protection rights in the regulatory cooperation chapters of EU Trade Agreements. In: Weiß W, Furculita C (eds) Global politics and EU Trade Policy. European yearbook of international economic law. Springer, Heidelberg, pp 185–207
Mattoo A (2015) Services Trade and Regulatory Cooperation. E15 Initiative Think Piece. Geneva
Mohay Á (2017) The status of international agreements concluded by the European Union in the EU legal order. Pravni Vjesnik 33(3-4):151–164

Monteiro J-A, Teh R (2017) Provisions on electronic commerce in regional trade agreements. WTO Working Paper, Geneva

Mucci A, Cerulus L, von der Burchard H (2016) Data fight emerges as last big hurdle to EU-Japan trade deal. Politico. 12 August 2016. https://www.politico.eu/article/eu-japan-trade-deal-caught-up-in-data-flow-row-cecilia-malmstrom/. Accessed 3 January 2021

noyb (2022) New US executive order unlikely to satisfy EU law. 7 October 2022. https://noyb.eu/en/new-us-executiveorder-unlikely-satisfy-eu-law. Accessed 30 October 2022

Peng S-y, Liu H-w (2017) The legality of data residency requirements: how can the trans-pacific partnership help? J World Trade 51(2):183–204

Peters A (1997) The position of international law within the European community legal order. German Yearb Int Law 40:9–77

Sargsyan T (2016) Data localization and the role of infrastructure for surveillance, privacy, and security. Int J Commun 10:2221–2237

Semertzi A (2014) The preclusion of direct effect in the recently concluded EU Free Trade Agreements. Common Mark Law Rev 51(4):1125–1158

Somaini L (2020) Regulating the dynamic concept of non-personal data in the EU: from ownership to portability. Eur Data Protect Law Rev 6(1):84–93

Streinz T (2019) Digital megaregulation uncontested? TPP's model for the global digital economy. In: Kingsbury B, Malone DM, Mertenskötter P et al (eds) Megaregulation contested: global economic ordering after TPP. Oxford University Press, Oxford, pp 312–342

USTR (2017) Summary of Objectives for the NAFTA Renegotiation. November 2017. Washington D.C. https://ustr.gov/sites/default/files/files/Press/Releases/Nov%20Objectives%20Update.pdf. Accessed 22 May 2022

van Rossem JW (2009) Interaction between EU law and international law in the light of *Intertanko* and *Kadi*: The Dilemma of norms binding the member states but not the community. Netherlands Yearb Int Law 40:183–227

Van Vooren B, Wessel RA (2014) EU external relations law. Cambridge University Press, Cambridge

Van Waeyenberge A, Pecho P (2014) Free Trade Agreements after the Treaty of Lisbon in the light of the case law of the Court of Justice of the European Union. Eur Law J 20(6):749–762

Velli F (2019) The issue of data protection in EU trade commitments: cross-border data transfers in GATS and Bilateral Free Trade Agreements. Eur Pap 4(3):881–894

Weber PA, Zhang N, Wu H (2020) A comparative analysis of personal data protection regulations between the EU and China. Electr Commer Res 20(3):565–587

Willemyns I (2020) Agreement forthcoming? A comparison of EU, US, and Chinese RTAs in times of plurilateral E-Commerce negotiations. J Int Econ Law 23(1):221–244

Wolfe R (2019) Learning about digital trade: privacy and E-Commerce in CETA and TPP. World Trade Rev 18(1):63–84

Wu M (2017) Digital trade-related provisions in regional trade agreements: existing models and lessons for the multilateral trade system. ICTSD and IDB Overview Paper. Geneva/Washington DC

Wunsch-Vincent S (2008) Trade rules for the digital age. In: Panizzon M, Pohl N, Sauvé P (eds) GATS and the regulation of international trade in services. Cambridge University Press, Cambridge, pp 497–529

Yakovleva S (2018) Should fundamental rights to privacy and data protection be a part of the EU's international trade 'Deals'? World Trade Rev 17(3):477–508

Yakovleva S (2020) Privacy protection(ism): the latest wave of trade constraints on regulatory autonomy. Univ Miami Law Rev 74(2):416–519

Yakovleva S, Irion K (2020) Pitching trade against privacy- reconciling EU governance of personal data flows with external trade. Int Data Priv Law 10(3):1–21

Yin J (2018) Cross-Border Data Continues to Flow under the USMCA. DisCo. 5 October 2018. http://www.project-disco.org/21st-century-trade/100518-cross-border-data-under-the-usmca/#.XGcDCpNKiL4. Accessed 3 January 2021

Jurisprudence

ECJ, AG Opinion, *Rízení Letového Provozu*: ECJ, Opnion of AG Mengozzi, *Rízení Letového Provozu,* C-335/05, EU:C:2007:103
ECJ, *Air Transport Association of America:* ECJ, Judgment of 21 December 2011, *Air Transport Association of America*, C-366/10, EU:C:2011:864
ECJ, *Commission v. Council*: ECJ, Judgment of 11 September 2003, *Commission v. Council*, C-211/01, EU:C:2003:452
ECJ, *Commission v. Grand Duchy of Luxembourg*: ECJ, Judgment of 19 June 2008, *Commission v Grand Duchy of Luxemburg*, C-319/06, ECLI:EU:C:2008:350
ECJ, *FIAMM*: ECJ, Judgment of 9 September 2008, *FIAMM*, C-120/06 P and C-121/06 P, EU:C:2008:476
ECJ, *Germany v Council*, ECJ, Judgment of 5 October 1994, *Germany v Council*, C-280/93, EU:C:1994:367
ECJ, *Germany v. Council (Bananas)*: ECJ, Judgment of 10 March 1998, *Germany v. Council*, C-122/95, EU:C:1998:94
ECJ, *IATA and ELFAA*: ECJ, Judgment of 10 January 2006, *IATA and ELFAA*, C-344/04, EU:C:2006:10
ECJ, *International Fruit Company:* ECJ, Judgment of 12 December 1972, *International Fruit Company*, C-21 to 24/72, EU:C:1972:115
ECJ, *Intertanko:* ECJ, Judgment of 3 June 2008, *Intertanko*, C-308/06, EU:C:2008:312
ECJ, *Kupferberg*, ECJ, Judgment of 26 October 1982, *Kupferberg*, C-104/81, EU:C:1982:362
ECJ, Opinion 1/15*:* ECJ, Opinion 1/15 of 26 July 2017, *Draft agreement between Canada and the European Union*, EU:C:2017:592
ECJ, Opinion 2/15*:* ECJ, Opinion 2/15 of 16 May 2017, *Free Trade Agreement between the European Union and the Republic of Singapore*, EU:C:2017:376
ECJ, Opinion 1/17*:* ECJ, Opinion 1/17 of 30 April 2019, *Comprehensive Economic and Trade Agreement between Canada, of the one part, and the European Union and its Member States, of the other part (CETA)*, EU:C:2019:341
ECJ, *Parliament v. Council and Commission*: ECJ, Judgment of 30 May 2006, *Parliament v. Council and Commission*, Joined Cases C-317/04 and C-318/04, EU:C:2006:346
ECJ, *Portugal v. Council*: ECJ, Judgment of 23 November 1999, *Portugal v. Council*, C-149/96, EU:C:1999:574
ECJ, *R. & V. Haegeman v. Belgian State*: ECJ, Judgment of 30 April 1974, *R. & V. Haegeman v. Belgian State*, C-181/73, EU:C:1974:41
ECJ, *Schrems:* ECJ, Judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650
ECJ, *Western Sahara Campaign UK:* ECJ, Judgment of 27 February 2018*, Western Sahara Campaign UK,* C-266/16, EU:C:2018:118

Documents

Council of the EU (2017) Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union. 2017/0228 (COD). 19 December 2017
Council of the EU (2019) Decision authorising the opening of negotiations with the United States of America for an agreement on the elimination of tariffs for industrial goods. 6052/19 LIMITE. 9 April 2019
ESF (2018) Commission's Proposal on Cross-border data flows in Trade Agreements. Letter to Kiril Yurukov, Chair of TPC Services and Investments. 12 June 2018

European Commission (2013a) Press Release. European Commission calls on the U.S. to restore trust in EU-U.S. data flows. 27 November 2013. https://ec.europa.eu/commission/presscorner/detail/en/IP_13_1166. Accessed 22 May 2022

European Commission (2013b) Viviane Reding. Speech - Towards a more dynamic transatlantic area of growth and investment. 29 October 2013. https://ec.europa.eu/commission/presscorner/detail/de/speech_13_867. Accessed 22 May 2022

European Commission (2017a) Communication on Exchanging and Protecting Personal Data in a Globalised World. COM(2017) 7 final. 10 January 2017

European Commission (2017b) Joint Declaration by Mr. Shinzo Abe, Prime Minister of Japan, and Mr. Jean-Claude Juncker, President of the European Commission. STATEMENT/17/1917. 6 July 2017

European Commission (2018) European Commission endorses provisions for data flows and data protection in EU trade agreements. Daily News. 31 January 2018

European Commission (2019) Communication Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union. COM(2019) 250 final. 29 May 2019

European Commission (2020) Communication, A European strategy for data. COM(2020) 66 final. 19 February 2020

European Parliament (2015) Resolution of 8 July 2015 containing the European Parliament's recommendations to the European Commission on the negotiations for the Transatlantic Trade and Investment Partnership (TTIP) [2017] OJ C 265/35

European Parliament (2016) Resolution of 3 February 2016 containing the European Parliament's recommendations to the Commission on the negotiations for the Trade in Services Agreement (TiSA) [2018] OJ C 35/21

HM Government, The exchange and protection of personal data, A future partnership paper, 24 August 2017

WTO (2015) Council for Trade in Service, Report of the Meeting held on 18 March 2015, Note by the Secretariat. S/C/M/122. 1 May 2015