Governing cross-border data flows

Reconciling EU data protection and international trade law

Yakovleva, S.

Publication date
2021

2. Personal data transfers in international trade and EU law: a tale of two 'necessities'

2.1 Introduction

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

The Chapter proceeds as follows. Section 2 offers a historical background and explains the EU restrictions on transfers of personal data outside the EEA. It then demonstrates a possible inconsistency between these rules and the EU commitments under the GATS. Section 3 juxtaposes the interpretation of the trade necessity test and the EU Charter necessity test and explains why there is a risk of a catch-22 type of compliance deadlock for the EU when the two necessity tests are applied simultaneously. Section 4 outlines ways out of the potential deadlock. Section 5 concludes.

2.2 EU data protection and international trade law

Restrictions on transfers of personal data outside the EEA have been characteristic of the EU data protection framework since its inception. Therefore this Section introduces these restrictions in a historical context, which allows for a deeper understanding of the concerns underlying them. It also explains the prevailing uncertainty surrounding the notion of 'transfer' in the EU data protection framework and its evolution over time. This Section then positions the EU restrictions on transfers of personal data against the EU commitments under the GATS and other trade agreements that require liberalisation of such transfers in the context of international trade in services.

2.2.1 The EU regime for transfers of personal data outside the EEA

2.2.1.1 Historical background

Rules governing cross-border transfers of personal data began to emerge in EU member states, alongside the first data protection laws in the 1970s, in response to the increasingly automated processing of personal data.[81] While the first 1970 data protection law of the German federal state of Hessen did not contain any restrictions on transfers of personal data, the data protection laws of Austria, Norway, Sweden, Ireland and Finland, adopted shortly after, did include such restrictions.[82] As classified by Kuner, these restrictions fell into one of the following three categories: (1) requiring an explicit authorisation by a Data Protection Authority (DPA); (2) incorporating provisions on data flows from Article 12 of the Council of Europe Convention 108 (Convention 108);[83] and (3) requiring an individual's consent or a similar level of protection in the country of destination.[84] Different approaches across EU member states were evidenced not only at the level of regulation, but also at the level of enforcement.[85] On a par with restrictions on the exporting of personal data, some domestic laws also regulated the importing of such data.[86] The strictness of rules governing transfers of personal data at that time was, however, counterbalanced by the relatively small volume of personal data in the overall data flows, which mostly comprised of non-personal data.[87]

Concerns that motivated the adoption of the rules on transfers of personal data, both in EU member states and in other countries, included not only the risk of the circumvention of domestic privacy and data protection rules, but also the risk that national, cultural and economic sovereignty could be undermined by personal data being processed abroad.[88] Examples of risks tied into sovereignty concerns were: inability to administer justice;

---

[81] Kuner (2013), p. 26.
[82] *Ibid*., p. 27-28.
[83] Article 12 'Transborder flows of personal data and domestic law' of the Convention 108 (prior to reform completed in 2018) stated that:

> 1. The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.
> 2. A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.
> 3. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:
> a)insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;
> b) when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.

[84] Kuner (2013), p. 27-28.
[85] *Ibid*.
[86] For example, Austrian and Luxemburgish data protection acts. Kuner (2013), p. 27-28.
[87] *Ibid*.
[88] Kuner (2013), p. 28-29.

information dependency on other states; and political risks resulting from information flows being controlled from another country.[89]

Increasing adoption of data protection laws across Europe, as well as on the international level, such as the Convention 108 and the OECD Guidelines,[90] led to a fragmentation of data protection standards.[91] Despite the recommendation from the European Commission, in an effort to contribute to an organic harmonisation of data protection laws across Europe – by the end of 1989 only seven EU member states ratified Convention 108.[92] Against the backdrop of increasing cross-border data flows in the 1990s, the lack of a cohesive data protection landscape and the emerging enforcement actions restricting personal data flows *between* the EU member states (such as the so-called 'FIAT' case), prompted the need for harmonised European data protection rules.[93] This need was given further impetus by the European Commission's ambition to develop a data processing industry in Europe.[94] These rules, 'clearly intended to improve the functioning of the internal market',[95] were codified in 1995 in the form of the Data Protection Directive. The Data Protection Directive was based on the EU competence to regulate the internal market,[96] although critics have described it as 'a tool of neutralisation of national rights in favour of economic efficiency'.[97]

It should, however, be noted that not only furthering the internal market, but also the protection of fundamental rights, were codified as equal objectives of the Directive.[98] As the European Commission noted in its first review of the Data Protection Directive, this Directive 'enshrine[d] two of the oldest *ambitions of the European integration project*: the achievement of an Internal Market (in this case the free movement of personal information) and the protection of fundamental rights and freedoms of individuals. In the Directive, both objectives are equally important'.[99] Despite the latter statement, in practice fundamental rights were viewed – at that time and up until 2009 when the EU Charter became legally binding – as merely 'derogat[ions] from internal market freedoms'.[100] From the rights perspective, the assumption was that those rights will not be violated because the

[89] Kuner (2013), p. 29-30.
[90] For example, in 1981, the Council of Europe adopted Convention 108, OECD adopted the 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
[91] Kuner (2013), p. 27; Lynskey (2015), p. 47-48.
[92] Lynskey (2015), p. 48.
[93] *Ibid*., p. 49; Kuner (2010), p. 19, Schwartz (2009), p. 11.
[94] Lynskey (2015), p. 47.
[95] *Ibid*., p. 49; González Fuster (2014), p. 134; van Hoboken (2014b).
[96] Recitals 3, 5 and 8 Data Protection Directive. For a discussion, see Lynskey (2015), p. 47-50.
[97] González Fuster (2014), p. 135.
[98] Article 1 Data Protection Directive.
[99] Report from the Commission, First Report on the Implementation of the Data Protection Directive (95/46/EC), COM/2003/0265 final, 15 May 2003, p. 3 (emphasis added).
[100] González Fuster (2014), p. 135. See also Petkova (2019), p. 148.

implementation of the Directive will lead to 'equivalent' levels of protection.[101] In its early jurisprudence, the CJEU tended to prioritise market integration ahead of the fundamental rights limb of the Directive.[102]

Moving forward to the twenty first century, the Lisbon Treaty, which took effect in 2009 and made the EU Charter legally binding for the EU, transformed the right to the protection of personal data into a *sui generis* binding fundamental right under Article 8 of the EU Charter, separate from the fundamental right to privacy enshrined in Article 7 of the Charter. It also granted the EU competence to legislate on the protection of personal data as a fundamental right.[103] The EU later relied on this competence to adopt the GDPR.[104] At the same time, just as its predecessor did, the GDPR also pursues the dual objective of safeguarding the fundamental rights, such as that to the protection of personal data, and ensuring the free flow of personal data within the internal market.[105] Furthermore, the EU data protection reforms that led to the adoption of the GDPR were one of the pillars of the Digital Single Market project, presented by the European Commission as the key for making the European Union thrive in the emerging global data economy.[106] It should also be recalled that back in 2012, the process of drafting the GDPR and the revision of the Data Protection Directive was initiated with a promise to simplify and streamline the mechanisms for cross-border data transfers, and to create more interoperability with the data protection regimes of the EU's strategic partners, including the US.[107] Despite the 'intense lobbying by and on behalf of US multinationals to limit what are characterized as unnecessarily restrictive rights for individuals',[108] the rules for transfers of personal data became even more stringent and only marginally more flexible.[109]

The constitutionalisation of the fundamental rights to privacy and the protection of personal data eventually not only shifted the core normative rationale of protecting these rights within the EU from the predominantly economic goal of ensuring the free flow of personal data in the EU, to the protection of individual rights, but also altered the balance

---

[101] Recitals 8 and 9 Data Protection Directive; Bygrave (2014), p. 192.
[102] Lynskey (2015), p. 51-54.
[103] Art. 16(1) of the TFEU.
[104] Recitals 1 and 12 GDPR.
[105] Art. 1 GDPR.
[106] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Completing a Trusted Digital Single Market for All, COM (2018) 320 final, 15 May 2018, p. 2–3.
[107]Van Hoboken, Arnbak, van Eijk (2013), p. 28; Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century, COM/2012/09 final, 25 January 2012, Section 5.
[108] Kuner, Cate, Millard, Svantesson (2013), p. 218.
[109] For a discussion of the changes to the EU framework on transfers of personal data outside the EEA introduced by the GDPR, see Section 5.1.

between economic and non-economic values in the EU's external economic policy.[110] As Pollicino and Bassini argue, '[w]hile at the very beginning of the European constitutionalism protection of fundamental rights [could] justify restrictions to the economic freedoms provided by the treaties, as exceptions to the same', after the Lisbon Treaty, the level of protection of fundamental rights began 'to determine the degree of openness of the European Union towards other orders'.[111] Entrusted with the power to interpret the EU Charter, the CJEU has taken up the role of a guarantor of EU fundamental rights. It played an important role in building up jurisprudence on Articles 7 and 8 of the Charter as well as in the interpretation of the derogation clause of Article 52(1) of the EU Charter in relation to these rights. Some even argue that in the 2015 Opinion concerning the validity of the draft EU-Canada PNR Agreement (the *Opinion on EU-Canada PNR Agreement*),[112] the CJEU has used data protection 'as a vehicle to assert EU fundamental rights in an international context'.[113]

The shift of balance between economic and non-economic values is most apparent in a line of post-EU Charter CJEU jurisprudence. In contrast to its prior case law, the Court's jurisprudence now prioritised the rights to privacy and data protection ahead of other rights, such as the freedom of expression and information (Article 11) and the freedom to conduct a business (Article 16), and conferred on them the status of 'leading rights' in Europe.[114] As the CJEU noted in *Google Spain*, '[i]n the light of the potential seriousness of that interference, it is clear that it cannot be justified *by merely the economic interest* which the operator of such an engine has in that processing'.[115] One year before the EU Charter became binding, in the *Satamedia* judgement[116] the Court took an approach to balancing the right to the protection of personal data against the right to freedom of expression that 'demonstrates that the protection of personal data weighs heavily relative to that part of freedom of expression which falls under "journalistic purposes." In other words, the CJEU place[d] greater weight on the protection of personal data than on freedom of expression in this context'.[117] Similarly, although in the *Schrems I* and *II* cases, the CJEU did not explicitly address the underlying issue of balancing trade and privacy,

---

[110] Under the TEU, as amended by the Treaty of Lisbon, negotiation and conclusion of international trade agreements must be guided by the universality and indivisibility of human rights and fundamental freedoms, respect for human dignity and principles of the United Nations and international law (Arts. 2(5) and 21 of the TEU).
[111] Pollicino, Bassini (2017), p. 262.
[112] CJEU, *Opinion on EU-Canada PNR Agreement*.
[113] Kuner (2018), p. 858.
[114] Petkova (2019), p. 154; Petkova (2016), pp. 430-432. See also Irion (2016), p. 7 (noting that 'the relative weight the CJEU accorded to the rights to privacy and data protection steadily expanded corresponding to the increasing significance of personal data processing and flows'.)
[115] CJEU, *Google Spain*, para. 81, emphasis added.
[116] CJEU, *Satamedia*, para. 56.
[117] Tranberg (2011), pp. 239–248.

Petkova argues that the Court did implicitly put the protection of fundamental rights to privacy and the protection of personal data above the commercial interests vested in transatlantic data flows.[118] The higher importance of the fundamental rights to privacy and the protection of personal data, as compared to other fundamental rights, also reveals itself through the higher 'strict necessity' threshold for derogation from these fundamental rights under Article 52(1) of the EU Charter, as is discussed in Section 2.3.3 below. It is also reflected in the desired level of protection of the right to the protection of personal data – 'effective and complete'[119] as pronounced by the CJEU.[120] The requirement of 'complete' protection could make the balancing of this right with other competing fundamental rights challenging and leave suboptimal room for respecting those other rights.[121] Although Lenaerts, the President of the CJEU, contended that 'there is no hierarchy of qualified rights under the Charter',[122] in practice, the CJEU *de facto* tends to rank fundamental rights to privacy and data protection above other rights in the internal hierarchy of values.[123]

In a broader perspective, EU law scholars link the European fundamental rights discourse to the growing demand for legitimacy following the expansion of the Union's competences.[124] To Muir, this discourse 'tends to become a legitimating battle horse for the European Union' and an increasingly 'important part of the EU "political messianism."'[125] The strengthening of the fundamental rights to privacy and the protection of personal data in the CJEU jurisprudence is, arguably, a part of this broader phenomenon and is liable to affect the balance of competences between the Union and its constituencies.[126] For example, the broadening of the scope of EU privacy legislation in relation to foreign countries' surveillance practices involving personal data transferred from the EEA by the CJEU in *Schrems I* and *II*, is likely to broaden the scope of EU Charter application to the EU member states' surveillance activities, as Section 2.2 further elaborates. Furthermore, EU competence to legislate fundamental rights to privacy and the protection of personal data increasingly underlies EU ambitions in regulating technology through framing legal challenges, such as those posed by artificial intelligence (AI), as data protection issues. In this sense, despite the shift of EU competence underlying data protection legislation from internal market to fundamental rights, this legislation is still an important pillar of the European project. At the same time, asserting the EU values as

[118] Petkova (2016), p. 431.
[119] CJEU, *Google Spain*, para. 34; CJEU, *Wirtschaftsakademie*, para. 28; CJEU, CJEU, Jehovan todistajat, para. 66; CJEU, *Fashion ID*, paras. 66, 70.
[120] Granger, Irion (2018), p. 4.
[121] Van Hoboken (2014a).
[122] Lenaerts (2012), pp. 392-393.
[123] Pollicino, Bassini (2017), pp. 247-248; Petkova (2016), pp. 430-432.
[124] Von Bogdandy, Kottmann, Antpöhler, Dickschen, Hentrei, Smrkolj (2012), p. 496; Muir (2014), p. 223.
[125] Muir (2014), p. 223.
[126] Petkova (2019), p. 147. See also Granger, Irion (2018), pp. 11-12.

global is also a part of the EU's political project of expanding the reach of EU law over internet-related issues globally.[127] As Eckes notes, 'in European law, constitutional law is the new internal market. Indeed, both in importance and in development, European constitutional law is today what the internal market was in the eighties and early nineties.'[128]

In recent years, as mentioned in the Introduction, robust protection of the fundamental rights to privacy and protection of personal data has also become part of the EU's 'technological' or 'digital sovereignty' narrative.[129] Although these notions are not directly linked by the EU to the regulation of transfers of personal data outside the EEA in the present day EU policy discourse, they do resonate well with the concerns that led to the development of such regulation in EU member states back in 1970s and 80s.

2.2.1.2 The notion of transfer

Although the concept of 'transfer' is central in triggering the application of the restrictions on transfers of personal data, nether the GDPR nor its predecessor – the Data Protection Directive – define the concept of 'transfer' of personal data outside the EEA.[130] Although the restrictions on transfers of personal data were in place for more than 20 years, there is still no clarity or specific guidance on what this concept means.

The CJEU specifically addressed this issue only once, in one of its earliest cases on data protection. In its 2003 *Lindqvist* judgement, the CJEU concluded that uploading materials onto an internet page, which can be consulted, and which is hosted by, a person established in a third country, thereby making that data accessible worldwide, does not constitute transfer of data to a third country in the meaning of Article 25 of the Data Protection Directive.[131] The Court also noted that in these circumstances, it is irrelevant whether an individual from a third country has accessed the internet page.[132] The CJEU based its reasoning on what Svantesson calls a 'reasonableness test'.[133] The Court explained that given that, first, the state of development of the internet at the time Data

[127] Kuner (2019), pp. 137-138, criticising these EU practices.
[128] Eckes (2012), p. 230.
[129] Madiega, T. (2020), p. 1; Communication from the Commission, *A New Industrial Strategy for Europe*, COM/2020/102 final, 10 Mach 2020, pp. 1,4; Communication from the Commission, *A European strategy for data*, COM(2020) 66 final, 19 February 2020; European Commission, *White Paper on Artificial Intelligence. A European Approach to Excellence and Trust*, COM(2020) 65 final, 19 February 2020, p. 3; Von der Leyen (2020).
[130] The European Commission's proposal for the GDPR also failed to define the term 'transfer'. For a discussion and approaches to the notion of 'transfer' in other international frameworks on data flows, see Kuner (2013), p. 12.
[131] CJEU, *Lindqvist*, para. 4 of the conclusions.
[132] *Ibid.*,para. 70.
[133] Svantesson (2010), p. 15. Kuner agrees that the CJEU's decision was 'based partly on pragmatic considerations'. Kuner (2013), p. 13.

Protection Directive was drawn up and, second, the absence (in Chapter IV of the Directive governing transfers of personal data), of criteria applicable to use of the internet:

> one cannot presume that the Community legislature intended the expression transfer [of data] to a third country to cover the loading, by an individual in Mrs Lindqvist's position, of data onto an internet page, even if those data are thereby made accessible to persons in third countries with the technical means to access them.[134]

In other words, there is no 'transfer' in the meaning of the Data Protection Directive, whenever there is no 'direct transfer' of personal data between the person posting personal data on the server and the person accessing personal data.[135] The Court further explained that if those rules

> were interpreted to mean that there is 'transfer [of data] to a third country' every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet. The special regime provided for by Chapter IV of the directive would thus necessarily become a regime of general application, as regards operations on the internet.[136]

There are several reasons to treat this rather narrow interpretation of 'transfer' with caution and, instead, adopt a broader understanding of this notion, 17 years after the *Lindqvist* judgement. First, the judgement concerns a fact-specific, particular case and may not have a universal application to all cases of online data sharing. To illustrate the point, in explaining its position, the CJEU refers to the 'action of a person in Mrs Lindqvist's position' and 'actions such as those of Lindqvist'.[137] Adopting this line of thinking, Kuner argues that making personal data available online can be viewed as cross-border data transfer if it involves 'granting access to the data of other parties on a large scale for business purposes'.[138] Second, unlike the Data Protection Directive, the GDPR was drafted in different economic circumstances, where data was increasingly labelled as 'the new oil',[139] and cross-border data flows as the 'hallmark of 21st-century globalization'.[140]

---

[134] CJEU, *Lindqvist*, para. 68.
[135] Kuner (2013), p. 13; Esayas (2012), p. 669; Bygrave (2014), p. 192.
[136] CJEU, *Lindqvist*, para. 69.
[137] See e.g. Dutch DPA Publication of Personal Data on the Internet, December 2007, section V, para. 5, p. 50.
[138] Kuner (2007), p. 83. Factors that could be relevant in assessing the likelihood of data transfer rules being applicable, include the presence of an establishment of data controller in the country of the individual whose data is processed, the targeting of the individual by company's activity, and the degree of control over the purposes or means used by the individual to process the data. *Ibid.*, p. 15.
[139] See Kuneva (2009). See also The Economist. (2016). But see Marr, B. (2018).
[140] Manyika, Lund, Bughin, Woetze, Stamenov, Dhingra (2016), p.10.

Therefore, one can no longer argue that the legislator could not foresee the application of the rules on transfers of personal data to pervasive transfers on the internet. Third, and most importantly, as already mentioned above, the GDPR was adopted on the basis of the EU competence to legislate on the fundamental right to the protection of personal data, rather than internal market competence, on which the Data Protection Directive was based.[141] Analogous with the CJEU's approach to a broad interpretation of the notions of 'personal data'[142] and 'controller' under the GDPR in a recent line of cases,[143] is a broad interpretation of the notion of 'transfer' of personal data, which could be necessary to ensure 'effective and complete'[144] protection of fundamental rights.

Despite the fact that cross-border flows of personal and other data have become the backbone of present-day digital commerce, online social networks and cloud computing, the uncertainty as to the meaning of 'transfer' in the EU data protection framework remains.[145] Based on the recent guidance of the European Data Protection Board (EDPB)[146] and the CJEU judgement in *Schrems II* it is only clear that:

1) 'granting direct access to a database (e.g. via an interface to an IT-application) on a general basis' constitutes a transfer of personal data in the meaning of the GDPR,[147] and
2) data in transit is equally subject to the rules on transfer of personal data outside the EEA under the GDPR.[148]

Based on the discussion above, this thesis takes the approach that - in the light of the constitutional role of the GDPR to ensure 'effective and complete' protection of personal

---

[141] Lynskey criticises the qualification of Mrs. Lindqvist activities as falling under the scope of the Data Protection Directive in the first place, calling the judgement 'integrationist'. Lynskey (2015), pp. 54-55. It could thus be argued, that a pragmatic approach of the Court to the scope of the rules on transfers of personal data was aimed at counterbalancing the broader scope of application of the Data Protection Directive.

[142] CJEU, *Nowak*, para 34 (stating that

> [t]he use of the expression 'any information' in the definition of the concept of 'personal data', within Article 2(a) of Directive 95/46, reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject)

[143] CJEU, *Google Spain*, para. 34; CJEU, *Wirtschaftsakademie*, para. 28; CJEU, *Fashion ID*, paras. 50, 66.

[144] CJEU, *Google Spain*, para. 34; CJEU, *Wirtschaftsakademie*, para. 28; CJEU, CJEU, Jehovan todistajat, para. 66; CJEU, *Fashion ID*, paras. 66, 70.

[145] Bygrave (2014), p. 193.

[146] The European Data Protection Board is a consultative body comprising all EU member states' data protection authorities. EUROPEAN DATA PROTECTION BOARD, About EDPB, https://edpb.europa.eu/about-edpb/about-edpb_en

[147] EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018, p. 4.

[148] CJEU, *Schrems II*, paras. 183-185. See also Kuner (2013), p. 176, agreeing with such approach, but proposing to take the fact that data are merely in transit in the analysis of risk of harm to individuals.

data[149] and the increasing prominence of the fundamental rights to privacy and the protection of personal data in CJEU case law,[150] in border-line cases the term 'transfer' should be understood broadly. Therefore, for the purposes of this thesis, collection of personal data by a data controller that does not have an establishment in the EEA, from individuals located in the EEA, especially where such individuals are specifically targeted by those controllers, is also considered a 'transfer' of personal data outside the EEA under the GDPR.[151] This approach does create an overlap between the rules on transfer of personal data outside the EEA under Chapter V of the GDPR and extraterritorial application of the GDPR framework under Article 3(2) of the GDPR. The problem of this overlap is recognised, but not yet resolved, by the European Commission and the EDPB.[152] Article 3(2) of the GDPR (which extends the scope of the GDPR to the controllers and processors who process personal data related to the offering of goods or services to individuals in the EU or monitoring of their behaviour within the EU) triggers the application of the whole GDPR, which should also include the rules of Chapter V. In addition, a narrow understanding of 'transfer' as *not* including the situations where personal data is collected by entities located outside the EEA would allow multinational companies to structure their data flows in a way that avoids the application of GDPR's Chapter V altogether. This would be problematic, because unlike Article 3(2) of the GDPR, the rules of Chapter V governing systematic transfers of personal data outside the EEA 'export' more than just the GDPR framework. As the following Section explains, the 'essential equivalence' standard requires that foreign recipients of personal data must also provide the effective protection of such personal data from access by foreign surveillance

---

[149] CJEU, *Google Spain*, para. 34; CJEU, *Wirtschaftsakademie*, para. 28; CJEU, CJEU, Jehovan todistajat, para. 66; CJEU, *Fashion ID*, paras. 66, 70.

[150] For a discussion, see the following Section.

[151] An argument to the contrary could, however, be based on the EDPB's guidance and the Standard Contractual Clauses approved by the European Commission. Both the guidance and the Standard Contractual Clauses use the terms 'data exporter,' 'data importer' and the 'data subject'. This suggests that a 'transfer' in the meaning of the GDPR is always a transfer from a controller or processor in the EEA ('data exporter') to a controller or processor outside the EEA ('data importer'). Therefore, the collection by a controller or processor located outside the EEA of personal data *directly from a data subject* (as data subject is never considered to be controller or processor of their own personal data) in the EEA does not a constitute a 'transfer' in the meaning of the GDPR. See, e.g., EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018; Standard contractual clauses (Set I) for controller to controller transfers.

[152] The question on the relationship between GDPR Chapter V rules on transfers of personal data and extraterritorial application of the GDPR under Art. 3(2) GDPR remains an open question. See Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), 16 November 2018, version 1.0, for publication consultation; the mentioning of this issue was removed from the version of the guidelines adopted after public consultation; Communication from the Commission, *Data Protection Rules as a Pillar of Citizens Empowerment and EUs Approach to Digital Transition - Two Years of Application of the General Data Protection Regulation*, COM(2020) 264 final, 24 June 2020, p. 12, calling on the EDPB to clarify 'the interplay between the rules on international data transfers (Chapter V) with the GDPR territorial scope of application (Article 3)'.

authorities.[153]

2.2.1.3 Restrictions on transfers

The EU legal framework for personal data protection includes two sets of rules: substantive rules regulating access to, and processing of, any personal data; and the rules governing transfers of personal data *outside* the EEA.[154] When it comes to the latter, the EU's current framework is one of the most restrictive in place in any democratic jurisdiction. The EU 'border control approach' to transfers of personal data is often contrasted to the United States 'open skies' policy on this issue.[155] Regulation of cross-border data flows gives EU domestic data protection rules an international dimension.[156] The EU framework governing transfers of personal data outside the EEA is based on a 'prohibition with derogations' principle. Under the GDPR, transfers of personal data to a country or territory outside the EEA or to an international organisation may only occur if the conditions of Chapter V of the GDPR are met.[157]

The EDPB advocates a layered approach to cross-border transfers of personal data outside the EEA.[158] The distinction is also made between systematic, as opposed to occasional and non-repetitive transfers.[159] Transfers of personal data can occur without restrictions only if the destination country, territory, or international organisation ensures an 'adequate' level of personal data protection.[160] First introduced by the 1995 Data Protection Directive, the adequacy mechanism predates the EU Charter. But, in the 2015

[153] This interpretation, however, as explained in Section 2.2.2 may lead to discrimination between EEA and non-EEA service providers, which could violate the most-favoured nation principle under trade law. When collecting personal data necessary for the provision of services in the EEA, non-EEA providers have to comply with all GDPR rules plus Chapter V (which limits the possibilities for collection of such data), while EEA providers do not have to comply with Chapter V if they operate locally in the EEA. It could, therefore, be argued, that the doctrine of parallel interpretation requires that the 'transfer' should be interpreted narrowly and not include the initial cross-border collection of personal data from data subjects in the EEA by foreign providers. Under the doctrine of parallel interpretation, if a (trade) agreement contradicts the EU secondary law, the preference will be given to the meaning of the secondary law that is more consistent with the provisions of the agreement. See e.g. CJEU, *Commission / Germany*, para. 52.
[154] Ferracane, van der Marel, (2018b) ('We identify two main categories of data policies. The first category covers those policies that impact the cross-border transfer of data whilst the second category covers policies that apply to the use of data domestically'.)
[155] Svantesson (2011), p. 184 ('The relatively strict border control scheme introduced through this has had a significant impact in other countries striving towards meeting the privacy standard set by the EU'); see also LeSieur (2012), pp. 101, 103–04; Schwartz, Peifer (2017), p. 135 (stating that '[u]nlike EU law, U.S. law starts with a principle of free information flow and permits the processing of any personal data unless a law limits this action'.)
[156] See LeSieur (2012), p. 93.
[157] Art. 44 GDPR.
[158] EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018, pp. 3,12,14. Kuner, however, argues that the CJEU's Schrems II decision may be undermining this layered approach. Kuner (2020b).
[159] EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018, pp. 4-5.
[160] Art. 45 GDPR.

Schrems I judgement, the CJEU retroactively gave it constitutional meaning.[161] 'Adequate', as interpreted by the CJEU, means 'essentially equivalent' to the level of protection of fundamental rights and freedoms guaranteed by the EU Charter.[162] The European Commission unilaterally evaluates the adequacy of the data protection regime of a country, territory, or international organisation on a case-by-case basis, taking into account its legal and administrative mechanisms of personal data protection.[163] If the Commission's assessment results in a positive finding, it issues a legally binding 'adequacy decision'.[164]

Currently, only 12 countries have a valid adequacy decision,[165] including the mutual adequacy arrangement with Japan.[166] An adequacy decision for the US, the so-called EU-US Privacy Shield framework, was invalidated by the 2020 CJEU judgement in *Schrems II*. The CJEU has concluded that the Privacy Shield does not ensure 'essentially equivalent' levels of protection for personal data transferred to the US, because it cannot remedy the absence of (1) necessary limitations and safeguards in US law with regard to the interferences caused by access to personal data by US surveillance authorities in the national security context, and (2) effective judicial protection against such interferences.[167] The *Schrems II* judgement has confirmed the CJEU's conclusions in 2015's *Schrems I*, which invalidated the Privacy Shield's predecessor – the EU-US Safe Harbor. Both *Schrems I* and *II* judgements embody European discontent with the US foreign surveillance practices[168] exposed by Edward Snowden's revelations. Awareness of the risks of US mass surveillance to Europeans' privacy has put the rules concerning foreign governments' access to EU individuals' data, for national security or law enforcement purposes, in the spotlight of adequacy assessment of a foreign country's data protection framework.

None of the adequacy assessments has yet resulted in a decision finding that the protection of personal data in a third country is not adequate. In the past, if the Commission

---

[161] For a discussion, see Section 5.2.
[162] See, e.g., CJEU, *Schrems I*, para. 73; CJEU, *Schrems II*, para. 94.
[163] For a list of criteria for assessment, see Art. 45(2) GDPR.
[164] 'Adequacy decisions' are adopted as Commission implementing acts based on Art. 288 TFEU.
[165] EUROPEAN COMMISSION, Adequacy of the protection of personal data in non-EU countries, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
[166] European Commission, Press Release: European Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows, IP/19/421, 23 January 2019.
[167] CJEU, *Schrems II*, paras. 168-197. For further discussion, see Section 5.3.1.
[168] *See* Kuner (2015a), p. 2092 (
The transfer of national borders to the online space reflects society's ambivalence about the benefits and drawbacks of globalization: on the one hand we have grown accustomed to the global availability of goods and services, but on the other hand we are unsettled by the breakdown of barriers that seems to threaten our national and regional identities. The Snowden revelations and other recent developments have increased the pace and intensity of these anxieties, but the deep-seated nature of these concerns shows the importance of developing an underlying normative framework to address them.)

was not able to certify the adequacy of personal data protection in the country under assessment, such assessment did not result in any decision at all. This was, for example, the case with the adequacy assessment for Australia.[169] In 2017, the European Commission started the review of all adequacy decisions that were in force at that time.[170] The 2019 adequacy decision for Japan appears to be under review at the moment of writing.[171] The European Commission is currently conducting an adequacy assessment for South Korea;[172] for the UK following Brexit;[173] and is actively exploring the possibility of adequacy assessments of the EU's important trading partners in Asia, Africa and Latin America.[174]

Transfers of personal data to countries, territories, or international organisations that have not been granted an adequacy decision, can only lawfully occur subject to 'appropriate safeguards', named in Article 46 of the GDPR, and put in place by the data controller or prossessor transferring personal data.[175] The most commonly used appropriate safeguards include:

- Standard data protection clauses, also known as standard contractual clauses (SCCs), either adopted by the European Commission[176] or adopted by a DPA of an EU member state and approved by the Commission,[177] and
- Binding corporate rules (BCRs), approved by competent DPAs, for multinational companies or companies conducting joint economic activity.[178]

As compared to the Data Protection Directive, the GDPR also introduced two new appropriate safeguards for transfers of personal data, which are not yet operational at the time of writing: approved industry codes of conduct[179] and certification mechanisms,[180]

---

[169] Newman (2018), p. 109; Bygrave (2014), p. 194.
[170] Stupp (2017).
[171] Agenda of the 40th EDPB meeting, 20 October 2020, mentioning the Review of the Adequacy Decision of Japan.
[172] EUROPEAN COMMISSION, Adequacy of the protection of personal data in non-EU countries, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.
[173] Stolton (2020); Christakis (2020). An adequacy decision for the UK following Brexit could be problematic following the CJEU *Schrems II* decision. See, e.g., Docksey, Kuner (2020).
[174] Commission Staff Working Document Accompanying the Document: Communication from the Commission, *Data Protection Rules as a Pillar of Citizens Empowerment and EUs Approach to Digital Transition - Two Years of Application of the General Data Protection Regulation*, COM(2020) 264 final, 24 June 2020, Communication from the Commission, *Data Protection Rules as a Pillar of Citizens Empowerment and EUs Approach to Digital Transition - Two Years of Application of the General Data Protection Regulation*, COM(2020) 264 final, 24 June 2020.
[175] Arts. 46–47 GDPR.
[176] Art. 46(2)(c) GDPR; EUROPEAN COMMISSION, Standard Contractual Clauses (SCC), https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en
[177] Art. 46(2)(d) GDPR.
[178] Arts. 46(2)(b), GDPR.
[179] Arts. 46(2)(e), 40 GPDR.
[180] Arts. 40(2), 42(2), 46 GDPR.

when complemented with binding and enforceable commitments by the controller or processor in the third country to apply the appropriate safeguards, including those in respect of the data subjects' rights.

In practice, until recently, SCCs were the most widely used mechanism for systematic transfers of personal data to countries without an adequacy decision.[181] This, however, is likely to change following the CJEU *Schrems II* judgement. Part of the questions referred for a preliminary ruling to the CJEU in this case concerned the validity of the SCCs approved by the European Commission in the light of the EU Charter.[182] Although the CJEU has concluded that the SCCs are valid in the light of the EU Charter, the Court explained that, in practice, the use of the SCCs is only allowed if they yield a standard of protection for the transferred personal data 'essentially equivalent' to that in the EU.[183] If this is not the case, data exporters must put in place supplementary measures to remedy the lack of essential equivalence of personal data protection or, alternatively, suspend or stop transferring personal data.[184] The DPAs are obliged to proactively monitor the use of SCCs for the purposes of transfers of personal data, and must suspend or prohibit personal data transfers when data exporters fail to implement necessary additional measures.[185] This requirement, especially in the absence of any concrete guidance on what the additional measures could be,[186] makes the use of SCCs problematic for transfers of personal data outside the EEA, especially to non-democratic countries. The same requirements are also likely to apply to other appropriate safeguards under Article 46 GDPR.[187]

Appropriate safeguards, such as the SCCs and the BCRs are applicable when a foreign recipient of personal data receives or obtains personal data from an establishment in the EEA. As a result, foreign companies that collect the personal data of Europeans via the internet and do not have a local establishment or business partner (for example, mobile app providers), may only rely on the codes of conduct and certification, none of which

[181] IAPP-EY (2019), p. 110 (showing that in 2019 (i.e. prior to the CJEU *Schrems II* judgement) 88% of personal data transfers from the EU to the US are based on the SCCs.)
[182] CJEU, *Schrems II*, paras. 122-149.
[183] CJEU, *Schrems II*, paras. 96, 99, 100, 133-137, 142; Kuner (2020d).
[184] For a more detailed summary of the CJEU's conclusions regarding the SCCs, see Chapter 5 section [x].
[185] CJEU, *Schrems II*, paras. 108, 121.
[186] At the time of writing, the EDPB has created a task force to work on those guidelines. EDPB, Press Release, Thirty-seventh Plenary session: Guidelines controller-processor, Guidelines targeting social media users, taskforce complaints CJEU Schrems II judgement, taskforce supplementary measures, 4 September 2020.
[187] EDPB, Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, 23 July 2020, question 7.

appear to be currently operational.[188]

If it is not reasonably possible for a company to adopt any of the appropriate safeguards under Article 46 GDPR, a data controller or processor may rely on the specific derogations contained in Article 49 GDPR, which include the explicit consent of a data subject, necessity of transfer for the conclusion or performance of a contract, or necessity for the establishment, exercise or defence of legal claims. Unlike the adequacy mechanism and appropriate safeguards, however, these derogations – in accordance with the EDPB guidance – are only suitable for 'occasional' or 'non-repetitive' transfers, and cannot be relied upon for the purposes of regular and systematic transfers.[189] The layered approach adopted in such guidance requires that before using these derogations, data exporters should first 'endeavour possibilities to frame the transfer' with one of the adequate safeguards.[190] Derogations are the only legal grounds that companies from the so-called 'non-adequate' countries that have no presence or business partner in the EEA, can use for cross-border collection of personal data in the absence of the codes of conduct or certification. Given that the EDPB guidance is not legally binding, the restrictive interpretation of the derogations' scope of application could be challenged in courts following the *Schrems II* judgement. In the new circumstances, specific derogations are the only legal mechanisms many companies can rely on for transferring personal data to the US and other countries that have not been afforded adequacy by the EU.

2.2.2 Compatibility of the EU regime for data transfer with international trade law

Shortly after the EU data protection framework was introduced in 1995, several commentators flagged the potential inconsistency of the rules for transfers of personal data with the EU's commitments under the GATS, such as most-favoured nation (MFN) treatment, national treatment and market access, and cannot be justified under the Article XIV GATS general exception.[191] The EU is bound by these commitments not only under

---

[188] At the time of writing, the author is not aware of any approved codes of conducts or certification mechanisms serving as appropriate safeguards for international transfers of personal data. The EDPB has, however, adopted some of the necessary guidance on the certification mechanisms. EDPB, Guidelines 1/2018 on certification and identifying certification criteria in accordance with arts 42 and 43 of the Regulation, including Annex 2, 4 June 2019. See also Chiavetta (2018). EDPB has not yet adopted guidance on the codes of conduct as a tool for transfers of personal data outside the EEA.

[189] EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018, p. 4.

[190] *Ibid.*, p. 4.

[191] Swire, Litan (1988), pp. 188-196; Reidenberg (2001), pp. 736-737; Bergkamp (2002), pp. 39-40. On the contrary, Shaffer argued that a hypothetical US claim regarding WTO inconsistency of EU's framework for personal data transfers 'would likely not prevail'. Shaffer (2000), pp. 46-51. Asinari admits that EU regime for transfers of personal data may violate the EU's WTO commitments, but concludes that the violation can be justified under the general exception. Asinari (2002), p. 277. It should however be noted that Asinari's article predates the WTO's interpretation of the necessity test in most recent WTO case law as well as the CJEU's case law on privacy and data protection as fundamental rights. Meddin also argues that

the GATS,[192] but also under virtually all the EU's post-GATS bilateral or plurilateral trade agreements.[193] Such warnings have intensified over time[194] under the influence of several factors: the increasing importance of international transfers of personal data for digital trade; the above-mentioned Edward Snowden's revelations; the challenge to the validity of the SCCs and the Privacy Shield at the CJEU, which resulted in higher standards for the former and invalidation of the latter;[195] the adoption of the GDPR in 2016 (which introduced a stricter enforcement regime); and the recurring pressure to include cross-border data flow provisions in trade agreements, such as TTIP and TiSA.[196]

Although the GDPR only marginally changed the framework for personal data transfers compared to the 1995 Data Protection Directive, it significantly raised the stakes of violating these rules by introducing harsh penalties, which include a fine of up to 4 % of the total worldwide annual turnover of an *undertaking* for the preceding financial year.[197] Under certain circumstances, this fine could be based not just on the turnover of a business unit that has violated the rules, but instead on the turnover of a multinational entity as a whole.[198] Higher stakes for violating the rules on transfers of personal data outside the EEA increase the risks of a collision between international trade law and the EU's data protection framework. Although the GATS does not specifically regulate cross-border flows of (personal) data, such flows may still be captured by obligations under the GATS applicable to trade in services from one WTO member into the territory of another WTO member ('mode of supply 1')[199] when data transfers enable cross-border provision of such services.[200]

Some authors have rightly argued that differences in the treatment by the EU of

---

the EU restrictions on transfers of personal data are inconsistent with the chapeau, while assuming that the 'necessity test' would be justified without explicating the underlying analysis. Meddin (2020), p. 1027-1028. On the possibility of violation of the chapeau, see also Bygrave (2014), p. 198; Baker (2020); Yakovleva, Irion (2016).

[192] Arts. II, VI and VII of the GATS.

[193] Such obligations are part of the most EU's international trade agreements, the most recent examples being Arts. 9.3, 9.5 and 9.6 CETA, Arts. 8.5, 8.6 of the EU-Singapore FTA, Arts. 8.15-8.17 of the JEFTA.

[194] See, e.g., Reyes (2011), pp. 24-26; Keller (2011); Weber (2012); Weber, Staiger (2017), pp. 58-59; MacDonald, Streatfeild (2014); Yakovleva, Irion (2016); Sen (2018); Coldicutt, Sen; Mattoo, Meltzer (2018). In contrast, acknowledging that the EU adequacy assessment may violate the EU's WTO commitments, Chen envisions the possibility of such violation being justified under art XIV(c)(ii) GATS. Chen (2015), p. 218.

[195] CJEU, *Schrems II*; Manancourt (2020).

[196] Irion, Yakovleva, Bartl (2016), p. 41; Fontanella-Khan (2013).

[197] Art. 83(5) GDPR.

[198] Article 29 Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP253, 3 October 2017, p. 6; CJEU, *Höfner and Elser*, para. 21; CJEU, *Confederación Española*, para. 40; CJEU, *Akzo Nobel and others*, para. 60; CJEU, *Elf Aquitaine*, para. 56; CJEU, *ICI / Commission*, paras. 125-146.

[199] Art. I(2)(a) GATS.

[200] Hodson (2018), p. 586.

services and service providers from countries that have, and those from countries that do not have an adequacy decision, may amount to a violation of the *MFN principle*.[201] Indeed, even the 'Article 29 Working Party'[202] noted in one of its early opinions that 'some third countries might come to see the absence of a finding that they provided adequate protection as politically provocative or at least discriminatory'.[203] Moreover, restrictive rules for transfers to countries that have not been afforded an adequacy decision have been characterised as discrimination between foreign service providers, especially those who do not have an establishment or business partner in the EEA; and providers from the EEA, thus constituting another potential violation of the GATS, namely the *national treatment obligation*.[204] For example, if 'transfer' of personal data in the GDPR's Chapter V is to be understood broadly and include the collection of personal data in the EEA by foreign service providers, as discussed in section 2.2.1.2 above, then unlike EEA providers, those providers face stricter requirements for the collection of personal data as compared to their domestic counterparts. In particular, such providers cannot use legitimate business interest as a lawful ground for collecting Europeans' personal data. While legitimate interest is mentioned as one of the lawful grounds for processing personal data in Article 6(1)(f) GDPR, it does not constitute a lawful ground for a transfer of personal data outside the EEA under Chapter V of the GDPR. The European Commission attempted to remedy this issue by including legitimate interest pursued by the controller or processor, as one of the specific derogations for occasional and non-repetitive transfers in its proposal for the GDPR.[205] However, this provision was later removed during negotiations at the European Parliament.[206] Instead, Article 49 GDPR provides a possibility to rely on 'compelling legitimate interest', which can only be done to a very limited extent. Similarly, the standard

---

[201] See, e.g., Asinari (2002), p. 273; Yakovleva, Irion (2016), 203; Irion, Yakovleva, Bartl (2016), pp. 28-30; Bergkamp (2002), p. 39; Keller (2011), p. 353; Reyes (2011), pp. 14-16; Sen (2018), pp. 335-338.
[202] Article 29 Working Party (full name: 'The Working Party on the Protection of Individuals with regard to the Processing of Personal Data') was an advisory body formed under Article 29 of the Data Protection Directive. It consisted of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission. Article 29 Working Party was replaced by the European Data Protection Board on 25 May 2018, when the GDPR entered into force.
[203] Working Document Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, WP 12, 24 July 1998, pp. 26-27.
[204] See, e.g., Coldicutt, Sen; Yakovleva, Irion (2016), p. 204.
[205] Art. 44(1)(g) of the Commission's initial Proposal for the GDPR (which corresponds to Article 49 of the adopted version of the GDPR) contained the following text:
the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.
Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), /* COM/2012/011 final - 2012/0011 (COD).
[206] See Lynskey (2015), p. 44.

for individual's consent, as a ground for a cross-border transfer of personal data (namely, explicit consent in Article 49(1)(a)) is higher than the equivalent standard in Article 6(1)(a) GDPR mentioning consent as a lawful ground for personal data processing.

The 2020 *Schrems II* judgement further intensifies the tension between the international trade and EU law frameworks governing transfers of personal data. The central role that access to Europeans' personal data by foreign authorities in the national security context plays in the CJEU's assessment of 'essential equivalence' of a third country's legal framework has intensified claims of a double-standard for personal data flows within the EEA and outside the EEA.[207] As Article 29 Working Party and academics explain, unlike foreign surveillance programmes, such programmes run by the EU member states are generally not subject to EU law, and specifically the EU Charter.[208] The reason for this is that under Article 4(2) of the Treaty on European Union national security is excluded from the EU competence and 'remains the sole responsibility of each member state'.[209] As a result, one could argue that by requiring foreign countries to meet the high EU Charter standards for the protection of the fundamental rights to privacy and personal data that the EU's own constituencies are not subject to, the CJEU has adopted a measure[210] violating the GATS *national treatment principle*. For example, it has been argued that in some EU member states (for example, Germany, France, the Netherlands, Sweden and the UK), privacy safeguards in the national security context are equally suboptimal or even weaker than those in the US, which have repeatedly been deemed inadequate by the CJEU.[211] Although all EU member states are also members of the Council of Europe, and

---

[207] See, e.g., Chander (2020), pp. 8-11; Swire (2016); Roth (2017), p. 65; Baker (2020); Swire (2020); Irion (2020).

[208] Irion (2020); Article 29 Working Party, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, WP 215, 10 April 2014, pp. 6-7. See also Buchta, Kranenborg (2020), p. 105 (arguing that

[a]s follows from article 2 TEU the Union is founded on the values of respect for the rule of law and for human rights. As the CJEU has stated in the Opinion on the accession of the EU to the ECHR, the Union is based on the fundamental premise that each Member State shares with all the other Member States a set of common values which implies and justifies the existence of mutual trust between the Member States that those values will be recognised. Against this background it is justified to leave certain matters to the Member State without further assessment, while for third countries a further assessment as regards those values still remains necessary.)

[209] Art. 4(2) TEU states that:

The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. *In particular, national security remains the sole responsibility of each Member State*. (emphasis added)

[210] It is established WTO case law that the notion of 'measure' is not restricted by requirement to form, and therefore, can also reflected in judicial decisions. See, e.g., WTO, Panel Report, *Saudi Arabia – Protection of IPR*, para. 7.49; WTO, Appellate Body Report, *US – Shrimp*, para. 173; WTO, Appellate Body Report, *US – Gasoline*, p. 28.

[211] Irion (2020); Roth (2017), pp. 64-65; Bigo, Carrera, Hernanz, Jeandesboz, Parkin, Ragazzi, Scherrer (2013); Swire (2016), p. 1-2.

are therefore, subject to the requirements of Article 8 of the European Convention on Human Rights (ECHR), it is generally agreed that – in view of the current CJEU and the European Court of Human Rights (ECtHR) case law – the standard of the EU Charter in relation to surveillance laws and measures is higher than that of the ECHR.[212]

In the light of the recent CJEU judgement in four cases, including *Privacy International*, the above-mentioned argument on the violation of national treatment cannot be made successfully.[213] From the Advocate General's Opinions in these cases, it follows that the fundamental rights standards developed by the CJEU in a line of cases concerning access to data transmitted by the telecommunications providers[214] equally apply to EU member states legislation governing access to such data in the national security context.[215] These standards, however, do not apply when national security authorities 'exercise that competence directly, using their own resources' without cooperation of private parties.[216] The CJEU followed the Advocate General's opinion and thus reinstated the equal treatment of EU member states and foreign countries following the two *Schrems* judgements.[217]

Furthermore, in a recent publication, Buchta and Kranenborg also suggest a way to interpret Article 4(2) TEU in a way that 'matters relating to national identities and essential State functions are not as such excluded from the scope of Union law but must be taken into account in the application of Union law.'[218]

As already noted above, the CJEU's *Schrems II* judgement may have implications beyond the EU-US Privacy Shield and the SCCs directly addressed by the judgement. Rather, as several scholars argue, the '*practical response*' to the restrictions introduced by *Schrems II* is data localisation.[219] This is exactly what one of the German DPAs recommended companies storing personal data in the US to do.[220] The DPA also raised similar concerns regarding transfers of personal data to China, India and Russia.[221] Depending on how restrictive on data flows supplementary measures will be, in the future EDPB guidance, the EU framework may become at risk of violating market access

---

[212] Opinion AG in *Schrems II*, para. 251. Christakis (2018); Irion (2020). An important decision is, however, pending at the Grand Chamber of the ECtHR, which could change the situation. ECtHR, *Big Brother Watch and others v. United Kingdom*.
[213] CJEU, *Privacy International*; CJEU, *La Quadrature du Net and Others*. For a discussion, see, e.g., Cameron (2020).
[214] CJEU, Tele2 Sverige; CJEU, Digital Rights Ireland.
[215] See, e.g., CJEU, *Privacy International*, para. 84. See also Opinions AG in *Privacy International and others*.
[216] Ibid.
[217] CJEU, Privacy International, para. 49.
[218] Buchta, Kranenborg (2020), pp. 100-103.
[219] Chander (2020), p.7-8; Churches, Zalnieriute (2020), p. 7-8; Propp, Swire (2020b).
[220] Berliner Beauftragte für Datenschutz und Informationsfreiheit, Pressemitteilung: Nach 'Schrems II': Europa braucht digitale Eigenständigkeit, 17 July 2020.
[221] Ibid.

commitments in data processing and database services, where transfers of data are essential for the production and delivery of services.[222]

2.3 Two necessities: a catch-22 for the EU

2.3.1. Framing the Issue

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

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

> Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures …
>
> (c) *necessary* to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to …
>
> (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts …

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

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

> [a]ny limitation on the exercise of the rights and freedoms recognised by this

[222] See, e.g., Sen (2018), p. 335; Reyes (2011), p. 22; Weber (2012), p. 33-34; Crosby (2016) p. 5-7; Coldicutt, Sen.

> Charter must be provided for by law and respect the essence of those rights and freedoms. *Subject to the principle of proportionality*, limitations may be made only if they are *necessary* and genuinely meet objectives of *general interest* recognised by the Union or the need to protect the rights and freedoms of others. (emphasis added)

'General interest recognised by the Union', according to the Explanations to the Charter covers, in particular, objectives of the Union in its external relations mentioned in Article 3 of the TEU, which include free and fair trade.[223] As the CJEU has explained, the derogation clause applies equally *to both internal and external legislative acts of the EU*, such as international agreements.[224] Affirming the supremacy of the EU Charter over the EU's international agreements, the CJEU confirmed that the EU may neither conclude nor implement through an EU legislative act, any international agreement (or decision of an international adjudicating body based on this agreement) if the conditions laid out in this derogation clause, namely the proportionality and necessity tests (that is, the 'EU Charter "necessity test"') are not fulfilled. [225] This conclusion echoes Article 207(3)(2) of the TFEU, imposing a responsibility on the Council and the European Commission to ensure 'that the agreements negotiated are compatible with internal Union policies and rules'. Then, Article 218(11) TFEU provides a mechanism to ensure that an international trade agreement is compatible with the EU's constitutional framework *before* it is concluded by the EU. It allows an EU member state, the European Parliament, the Council or the European Commission to request an opinion from the CJEU regarding the compatibility of a proposed international agreement with the EU Treaties, including the EU Charter. If the CJEU decides that such an agreement is incompatible with the Treaties, the international agreement cannot take effect until, and unless, it is brought in compliance with the Treaties. This provision was used at the request of the European Parliament concerning the EU-Canada agreement on the transfer and processing of Passenger Name Record data,[226] which, among other things, mandated transfers of Europeans' personal data to Canada. In this landmark ruling, having tested these provisions against the requirements of the derogation clause, including the EU Charter necessity test, the CJEU held that the agreement could not be concluded unless revised.[227]

It is now settled case law at the CJEU that international agreements entered into by the EU must be 'entirely compatible with the Treaties and with the constitutional principles

---

[223] Explanation on Article 52, Explanations Relating to the Charter of Fundamental Rights, 2007 O.J. (C 303), Art. 3(5) TEU.
[224] CJEU, *Opinion on EU-Canada PNR Agreement*, para. 146.
[225] Vedaschi (2018), p. 138.
[226] CJEU, *Opinion on EU-Canada PNR Agreement*.
[227] *Ibid.*, paras. 232(2)-232(3).

stemming therefrom'.[228] In particular, such agreements must be compatible with the right to privacy and the right to the protection of personal data.[229] This is crucial to the analysis in this thesis because, if the EU framework for personal data transfers was deemed inconsistent with a trade agreement – for example, for failing to meet the requirements of the trade necessity test contained in the general exception – and the EU was required to bring its laws into conformity with the trade agreement, compliance with the decision of a trade adjudicating body establishing such inconsistency would be a derogation from the fundamental rights codified by Articles 7 and 8 of the EU Charter. It follows from the CJEU's jurisprudence, however, that before such a decision of an international trade adjudicating body could be implemented, compliance would have to be tested under the requirements of Article 52(1) of the EU Charter. Yet, trade law's necessity test, when viewed as a derogation from the EU's fundamental right to privacy and the protection of personal data, is unlikely to meet the EU Charter necessity test.[230] Put another way, the trade necessity test obligates the EU to derogate from fundamental rights more than the EU is legally allowed to do under Article 52(1) of the EU Charter.

To sum up, not only could the EU framework for personal data transfers be found to be in violation of the EU's international trade commitments, but also international trade commitments requiring (unrestricted) transfers of personal data outside the EEA may be found *inconsistent with the EU Charter*. Simultaneous application of the two necessity tests (trade law and Article 52 of the Charter), thus puts the EU in a catch-22 situation, as discussed in Section 2.3.4 of this Chapter.

An important doctrinal point should be clarified before moving on. Although international trade agreements are binding on the EU and constitute an 'integral part' of its legal system,[231] in the hierarchy of EU legal order, EU primary law (including the EU Charter) prevails over the EU's international trade commitments.[232] Moreover, neither international trade agreements nor the decisions of international trade adjudicating bodies

[228] *Ibid.*, paras. 67, 70.
[229] *Ibid*., paras. 70, 119.
[230] For further discussion, see section 2.3.3.
[231] See, e.g., CJEU, *Haegeman*, para. 5; CJEU, *Opinion 2/13*, para. 180.
[232] CJEU, *Kadi*, paras. 282, 307, 308, 316; recital 11 of the Preamble to Council Decision 94/800/EC of 22 December 1994 concerning the conclusion on behalf of the European Community, as regards matters within its competence, of the agreements reached in the Uruguay Round multilateral negotiations (1986-1994) [1994] OJ L336/1. Although this Decision, unlike the Schedule of Specific Commitments, does not constitute a part of the GATS, the CJEU deferred to it in Portugal v Council as an indication of political will of the EU in concluding the WTO Agreement. CJEU, *Portugal / Council*, para. 48. See also CJEU, *Air Transport Association of America and others*, para. 74; CJEU, *Portugal / Council*, para 42; *Germany / Council*, paras. 106, 108, 110. See also Eckes (2019), p. 152.

have direct effect in the EU.[233] This approach is based on the principle of the autonomy of the EU legal order in relation to international law, which cannot affect the constitutional values and internal division of competences in the EU.[234] From an international law perspective, the absence of direct effects of international court decisions in domestic legal systems is not uncommon.[235] The prerogative of domestic constitutional law to decide how international decisions affect their internal legal frameworks can be viewed as an internal control mechanism that supports the legitimacy of international adjudication.[236] This mechanism, therefore, 'relieves international legal decisions from the burdens of legitimation that they are not always capable of bearing by opening up another mechanism of democratic legitimation.'[237] Furthermore, the principle of autonomy of the EU legal order exemplifies a pluralist approach to the global legal order.[238]

The EU's stance in relation to international law and adjudication, nevertheless, does not make the EU's obligations under international trade law less binding from *an international law* perspective. Under international law, the EU must perform its obligations in good faith.[239] Moreover, the EU may face liability and retaliation under international trade law if it fails to comply with its trade commitments or a decision of a trade-adjudicating body, even if such compliance is not possible due to constraints contained in EU primary law.[240] This is why constitutional restrictions on compliance with such obligations or decisions could present a serious problem. This problem can manifest itself in at least two different contexts. First, in the context of the *existing* international trade norms, specifically those contained in the GATS. Second, in the context of *international*

---

[233] CJEU, *FIAMM and others*, paras. 120, 125-128. For a discussion see Semertzi (2014), pp. 1132-1135. See also Gáspár-Szilágyi (2015); Craig, De Búrca (2015), pp. 362-363; Martines (2014). For an elaborate discussion of these issues in the present context see Yakovleva, Irion (2016), pp. 200-202. See also Eckes, (2019), p. 187.

[234] Starting as early as in 1963 from CJEU case *van Gend & Loos*. Eckes explains that the CJEU's choice to protect supremacy of EU law from obligations originating outside the EU 'is a necessary consequence of the Union's complex constitutional set-up'. Eckes (2012), pp. 232, 244-249. See also Gaspar-Szilagyi (2015), 349.

[235] von Bogdandy, Venzke (2914), p. 196.

[236] *Ibid*., pp. 196-197.

[237] *Ibid*., p. 197. See also Howse (2007), p. 128; Howse, Langille (2012), p. 430.

[238] Krisch (2012), p. 103 (describing 'a model that requires each polity, in an exercise of public autonomy through its institutions, to define the terms on which it interacts with others' as an example of example of 'systemic pluralism'). De Búrca's reply to Weiler in Dialogical epilogue, See Weiler (2012), p. 282. In her own contribution to the book, De Búrca criticises the CJEU's approach and suggests that some version of Solange approach, to which she also refers to as a 'soft constitutionalist' (or 'soft pluralist') approach would be preferred. De Búrca (2012). There are, however, some divergences of view in scholarship on the exact meaning of the terms: what De Búrca refers to as 'pluralism', other scholars label 'dualism' for example. See, e.g., Besson (2009), p. 262-263, Kokott, Sobotta (2012). The CJEU, however, did imply in its decision that the Solange approach could be possible in different circumstances. Kokott, Sobotta (2012), p. 1019.

[239] Art. 31.1 VCLT.

[240] Art 27 VCLT.

negotiations concerning cross-border data flows and exceptions for privacy and data protection to be included in *future* trade agreements, including the ongoing digital trade talks at the WTO.

With respect to the *first context*, it should be acknowledged that the possibility of a conflict between EU law and EU obligations under the (existing) GATS and WTO legal framework cannot be avoided because the rules are already there. Indeed, it could be argued, from a pluralist perspective, that it *should not* necessarily be avoided, given divergent moral convictions on data privacy.[241] Instead, it can be viewed as an expression of pluralism. In other words, the absence of clear answers at the point of possible conflict could normatively be a preferred option compared to a clear hierarchy between conflicting norms, so that both international trade and EU law legal orders can decide autonomously on their stance on the issue, without having to fully align their perspectives. In such a pluralist structure, the conflict could be addressed in other ways, notably through dialogue and mutual permeation of rules following a potentially unfavourable outcome for the EU of a WTO dispute settlement, should one occur. At the heart of the normative argument in favour of such a pluralist approach is that it provides space for 'intense social contestation about the locus of authority and the right collective for decision-making' on matters surrounded by deep-seated disagreement.[242] Furthermore, '[p]luralism is also closer to foundational ideals of political order – namely public autonomy … the plural, divided identities, loyalties, and allegiances that characterize postnational society are better reflected in a multiplicity of orders than in an overarching framework that implies ultimate authority.'[243] In addition, a pluralist structure offers a potential for adaptation and builds in checks and balances into the global legal order.[244]

The GMO dispute between the EU and the US, where two fundamentally opposing approaches clashed, is often cited as an example of successful cooperation that can be achieved in a pluralist setting.[245] Despite the clash, the WTO Panel, which found against the EU, did so on narrow, formal grounds and avoided any pronouncement on the substance of the EU's precautionary approach to GMOs, as opposed the risk-based

---

[241] For example, Krisch argues that pluralism
seeks to discern a model of order that relies less on unity and more on the heterarchical interaction of the various layers of law. Legally, the relationship of the parts of the overall order in pluralism remains open—governed by the potentially competing rules of the various sub-orders, each with its own ultimate point of reference and supremacy claim, the relationships between them are left to be determined ultimately through political, not rule-based processes.
Krisch (2012), p. 23.
[242] *Ibid.*, pp. 78, 189-190, 206.
[243] *Ibid.*, p. 106.
[244] *Ibid.*, pp. 78, 103.
[245] *Ibid.*, pp. 190-222.

approach mandated by the SPS Agreement.[246] This has been explained by the incentive of the WTO to preserve its own legitimacy and maintain social acceptance of its dispute-settlement system, as well as to avoid the risk that the EU would simply not comply with a 'hard' decision against it (an option, however, that seems available only to more powerful WTO Members).[247] On the EU side, the WTO dispute settlement reports has had a profound effect on EU domestic rules on GMOs, and the CJEU has integrated WTO law into its jurisprudence, despite its reluctance to grant it direct effect.[248] The pressure for compliance, arguably, came from the high costs of non-compliance with the WTO Panel's report.[249] In sum, the political dialogue that ensued after the unfavourable WTO dispute settlement reports led to 'far-reaching convergence on both principles and processes around the SPS approach.'[250]

There are at least two reasons, however, why a pluralist approach is unlikely to play out in the same way in relation to the clash between the rules on data privacy in the current circumstances. First, and most importantly, unlike the GMO debate, the clash between the EU approach to governing cross-border data flows and data privacy protection, and other countries, such as the US, which could potentially result in a confrontation at the WTO, concerns not only EU secondary, but also EU primary law, as this Chapter demonstrates. The new legal reality, in which the EU Charter is binding and constitutes a part of EU primary law, considerably limits the potential of trade law to shape EU governance of data privacy protection as compared to the GMO case. As a result, the EU may have to face the costs of trade retaliation, – no matter how high – should its framework for transfers of personal data outside the EEA be found to be inconsistent with the GATS. If retaliation resulted in a suspension of personal data flows *into* the EU, this would directly cut across the EU digital trade policy, which aims to liberalise such flows.[251] It is, however, possible that WTO adjudicators – in the spirit of a pluralist approach – would not come down too hard on the EU on the data privacy issue. For example, in his 2000 article, Shaffer argues that '[u]nder media scrutiny, WTO dispute settlement panels would prefer to refrain from engaging in a close balancing of competing trade and privacy interests, and rather review the process by which the European Union takes account of foreign privacy protections.'[252] Second, although, as mentioned above, the CJEU has used the tool of treaty-consistent interpretation to interpret EU law in the light of international law, including WTO law, it has not done so in areas with high salience, such as issues of the EU's banana market and

[246] *Ibid.*, pp. 195-196; Hakimi (2020), p. 573; Shaffer (2008), p. 70.
[247] Hakimi (2020), p. 573; Shaffer (2008), pp. 68-70.
[248] Krisch (2012), pp. 215-216.
[249] *Ibid.*, pp. 9-10, 20-21.
[250] *Ibid.*, p. 216.
[251] For a discussion, see Section 4.2.5.
[252] Shaffer (2000), p. 51

import of hormone treated meat.[253] In the latter case, the EU has been incompliant with its WTO commitments and has faced trade retaliation measures from the US and Canada for more than 20 years.[254] It is equally unlikely that the CJEU will take into account EU trade obligations under the WTO Agreements in its future jurisprudence on the issue of transfers of personal data, as it has already refrained from doing so in both *Schrems I* and *Schrems II* concerning transfers of personal data from the EU to the United States. As explained above, in some of its judgements the CJEU has implicitly ranked the fundamental rights to privacy and the protection of personal data above other relevant fundamental rights, such as the right to conduct business.

In the context of international negotiations of future trade agreements, the risk of a clash between the two necessities, as described above, makes replication of the GATS general exception for privacy and data protection problematic from an EU law perspective. This thesis addresses that problem in Chapter 4. The main legal reason for this is, as previously mentioned, that the EU institutions must ensure the compatibility of any trade agreements they negotiate with internal EU policies and rules.[255] Preserving uncertainty as to whether the proposed agreement is compatible with the EU *acquis* (which could be viewed as a normatively preferred option from a pluralist perspective), could result in a CJEU judgement under Article 218(11) TFEU finding such an agreement incompatible with the EU *acquis*. This would, ultimately, require a re-negotiation of the agreement, which would not only delay the conclusion of the agreement, but also result in the additional costs of renegotiation and forfeited benefits from delayed trade concessions under the proposed agreement. It is worth recalling that the conflict about the proper regulatory approach to GMOs in agriculture, which was used to illustrate why a pluralist approach could be normatively more desirable, itself resulted from a situation where European negotiators on the SPS Agreement did not insist on wording that would have shielded the EU approach to sanitary and phytosanitary measures in certain areas (based on the precautionary principle rather than a risk-based approach relying on science as justification for trade-restrictive measures).[256] In view of the above-mentioned TFEU provisions, as well as the fact that the rights to privacy and the protection of personal data

---

[253] Krisch (2012), p. 205.

[254] Although the EU never adjusted its legislation in compliance with the WTO decisions, the issue has been settled recently through EU giving Canada and the US concessions on import of hormone free beef. See European Commission, Press Release: *The European Union and the United States sign an agreement on imports of hormone-free beef*, 2 August 2019; Miles (2017).

[255] Art. 207(3)(2) TFEU.

[256] Krisch (2012), pp. 215-216, explaining that

the EC found itself with few allies and had to give in if negotiations were to continue—it was keen on a successful conclusion because it sought to reduce obstacles to its own market access in other countries and did not want to see this relatively low-priority issue threaten negotiations on other, more central parts of the Uruguay Round.

are binding fundamental rights in the EU, a similar outcome is simply not possible as a matter of EU law in the trade negotiations affecting EU data protection framework. Another related reason, is that the EU's position, according to which, data protection cannot be traded in international trade negotiations, as well as its commitment to safeguard its full autonomy to protect the rights to privacy and the protection of personal data as fundamental rights, is an important internal political message to the public.[257] From a political perspective, replication of the GATS general exception for privacy and data protection, in conjunction with a provision on cross-border data flows in the EU's future trade agreements, is also very likely to be opposed by the European Parliament. This may also lead to the European Parliament's refusal to consent to the trade agreement.[258] For example, the European Parliament strongly opposed replication of the GATS general exception in the failed TTIP and TiSA.[259]

2.3.2 Trade law necessity and EU Restrictions on data transfers

To be justified under the general exception contained in GATS Article XIV, a prima facie inconsistent measure has to meet one of the material requirements of the general exception set forth in Article XIV (a) to (e) and the introductory clause (or *chapeau*) of this Article. This general exception applies horizontally to measures that violate any obligation under the GATS. The wording of the general exception is remarkably consistent in most US- and EU-led trade agreements, in that they all closely follow GATS Article XIV.[260] This is why the interpretation of the trade necessity test at the WTO may be relevant also in the context of other trade agreements.

This general exception requires a two-tier assessment: first it has to be established whether the contested measure meets one of the substantive requirements of paragraph (c); second, there is an examination of whether the contested measure satisfies the requirements

[257] For a discussion, see Section 4.2.1.
[258] For a discussion on the increased role of the European Parliament both at the stage of negotiation and adoption of international trade agreements after the Lisbon Treaty, and how the Parliament has used this role in practice see Eckes (2019), pp. 153-166.
[259] European Parliament 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) (2014/2228(INI)). European Parliament resolution of 3 February 2016 containing the European Parliament's recommendations to the Commission on the negotiations for the Trade in Services Agreement (TiSA) (2015/2233(INI)). In its resolution on TiSA (para. 1(c)(iii)), the European Parliament recommended European Commission:
… to incorporate a comprehensive, unambiguous, horizontal, self-standing and legally binding provision based on GATS Article XIV which fully exempts the existing and future EU legal framework for the protection of personal data from the scope of this agreement, without any conditions that it must be consistent with other parts of the TiSA;
The Resolution on TTIP contains an identical recommendation in para 2(xii).
[260] The most recent examples of EU trade agreements where the GATS art XIV was closely reproduced include Art. 28.3(2)(c)(ii) CETA, Art. 8.62(e)(ii) EU-Singapore FTA, and Art. 8.3 JEFTA.

of the *chapeau* of the exception.[261] The necessity test is the core of the first stage of the assessment.

Article XIV(c)(ii) has never been applied by a WTO panel. However, privacy and data protection is not the first public policy interest in tension with trade liberalisation. The interpretation of the necessity test in WTO cases touching upon other public policy interests listed in GATS Article XIV(c) and Article XX of the General Agreement on Tariffs and Trade (GATT) 1994 – applicable to international trade in goods instead of services, which also feeds into the application of 'necessity' in the GATS, and vice versa[262] – can inform the interpretation of paragraph (c)(ii). The method used to interpret 'necessity' applied by WTO adjudicating bodies is fairly consistent irrespective of the specific public interest invoked to justify the measure, be it the protection of public morals, public health, or securing compliance with a WTO-consistent law.[263] Existing WTO case law has established a high threshold for meeting the necessity test, which in some cases has been almost impossible to meet.[264]

The assessment of the necessity of a GATS-inconsistent measure applied by the WTO adjudicating bodies (first expounded in *Korea – Various Measures on Beef*[265] and recently confirmed in *US — Tariff Measures*) requires 'weighing and balancing' of the following factors:[266]

1. The relative importance of the protected public interest(s) pursued by such contested measure,
2. The contested measure's contribution to the achievement of objective pursued, manifested in the existence of a 'genuine relationship of ends and means between the objective pursued and the measure at issue',[267] and

---

[261] WTO, Appellate Body Report, *Argentina – Financial Services*, para. 6.161; WTO, Appellate Body Report, *US-Gambling*, para. 292.
[262] See e.g. WTO, Appellate Body Report, *US-Gambling*, para. 291.
[263] The WTO adjudicating bodies apply the same interpretation of 'necessity' as pronounced in WTO, Appellate Body Report, *Korea – Various Measures on Beef*, paras 160-164 irrespective of the specific paragraph of Art. XIV GATS or Art. XX GATT 1994. See, e.g., in relation to Art. XX(b) GATT - WTO, Appellate Body Report, *EC - Asbestos*, paras. 171-175; in relation to Art. XIV(a) GATS - WTO, Appellate Body Report, *US-Gambling*, paras. 291, 305-308; in relation to Art. XIV(c) GATS - WTO, Appellate Body Report, *Argentina – Financial Services*, paras. 6.202-205, 6.227ff. See also Delimatsis (2011), p. 262.
[264] Delimatsis (2011), p. 266; Venzke (2011), p. 1118-1119.
[265] WTO, Appellate Body Report, *Korea – Various Measures on Beef*, para 164.
[266] WTO, Panel Report, *Argentina – Financial Services*, para. 7.661; WTO, Appellate Body Report, *US-Gambling*, paras. 304-307; WTO, Appellate Body Reports, *EC – Seal Products*, paras. 5.169, 5.214; WTO, Panel Report, *US – Tariff Measures*, para. 7.158.
[267] WTO, Panel Report, *US – Tariff Measures*, para. 7.158; WTO, Panel Report, *Argentina – Financial Services*, para. 7.688; WTO, Appellate Body Report, *US-Gambling*, para. 306; WTO, Appellate Body Report, *Brazil – Retreaded Tyres*, para. 145; WTO, Panel Report, *Brazil – Taxation*, para. 7.526; WTO, Panel Report, EU – Energy Package, para. 7.1360 (currently under appeal); WTO, Panel Report, *Colombia – Textiles*, para. 7.315; WTO, Panel Report, *India – Solar Cells*, para. 7.361; WTO, Appellate Body Reports, *EC – Seal Products*, para. 5.210.

3. The trade restrictiveness of the measure,[268] followed by an assessment of whether, in the light of importance of the interests at issue, a less trade restrictive alternative is 'reasonably available'.

In application to EU restrictions on transfers of personal data, the 'relative importance' factor would be a translation of the requirement that the contested restrictions be designed to secure compliance with the laws and regulations relating to the protection of privacy and personal data. As the WTO Appellate Body stated in *US – Gambling*, the process of assessing 'necessity' "begins with an assessment of the 'relative importance' of the interests or values furthered by the challenged measure."[269] The more important the interest, the heavier it weighs in the assessment, and the heavier it weighs in the justification of a relatively more restrictive measure. In prior cases, the WTO adjudicating bodies have assigned different values to the various public policy objectives mentioned in the general exceptions of GATS Article XIV and GATT Article XX. For example, the protection of human health and life have been recognised as 'vital and important in the highest degree',[270] the aim of protecting environment as 'important',[271] and the protection of the tax collecting systems against tax evasion as being 'of vital importance'.[272] Some case law suggests that the level of international support of the interest at stake[273] or the actual (as opposed to desired) contribution of the measure to achieve a claimed level of protection of public policy interest[274] could weigh in this assessment. Beyond this factor, it is unclear how the WTO adjudicators assess the importance of different non-economic values. No objective has been characterised as 'unimportant'.

Assessment of factors 2 and 3 in the list above comprises a weighing and balancing of the contribution of the measure to the protected interest, with the trade restrictiveness of the measure in light of the relative importance of the protected interest or the underlying values of the objective pursued.[275] On a continuum between 'indispensable' and 'making a contribution to', 'necessity' is understood as being closer to 'indispensable' rather than

---

[268] Assessment of this factor was left out in WTO, Appellate Body Report, *EC - Asbestos*.
[269] WTO, Appellate Body Report, *US – Gambling*, para. 306; WTO, Appellate Body Report, *Korea – Various Measures on Beef*, para. 164; WTO, Appellate Body Report, *Brazil –Retreaded Tyres*, para. 143; WTO, Panel Report, *US — Tariff Measures*, paras. 7.168-7.169.
[270] WTO, Appellate Body Report, *EC – Asbestos*, para. 172; WTO, Appellate Body Report, *Brazil – Retreaded Tyres*, para. 179.
[271] WTO, Appellate Body Report, *Brazil – Retreaded Tyres*, para. 179.
[272] WTO, Panel Report, *Argentina – Financial Services*, para. 7.671.
[273] WTO, Panel Report, *Argentina – Financial Services*, paras. 7.671, 7.715; WTO, Appellate Body Report, *US – Shrimp*, para. 130.
[274] WTO, Appellate Body Report, *EC – Seal Products*, para. 5.502; Du (2016), p. 826-827.
[275] WTO, Appellate Body Report, *Brazil – Retreaded Tyres*, para. 210; WTO, Appellate Body Report, *EC – Seal Products*, para. 5.210, WTO, *US –Gambling*, para. 306; WTO, Panel Report, *Argentina – Financial Services*, para. 7.684.

'making a contribution to'.[276] Thus, the greater the contribution of the contested measure, and the less restrictive it is, the more likely it is to satisfy the necessity test.[277] It is, however, debatable whether this or the following factor is decisive in the assessment of necessity in practice.

If the defending party has succeeded in making a *prima facie* case of 'necessity', the complaining party may rebut it by showing that a less trade-restrictive measure was 'reasonably available' to the defending party. This assessment includes a 'comparison between the challenged measure and possible alternatives …, and the results of such comparison should be considered in the light of the importance of the interests at issue.'[278] 'Reasonably available' is interpreted as allowing a WTO member to achieve *the same level of protection* of the public interest or objective pursued without prohibitive cost or substantial technical difficulties.[279] Based on this interpretation, the comparison of alternative measures does not typically involve a fully-fledged proportionality assessment, which is arguably the case in the assessment of the trade-restrictiveness of the measure.[280] Rather, this comparison involves the balancing of the administrative and enforcement costs of alternative measures granting the same level of protection to a public interest at issue against the trade costs of such measures.[281] It is generally agreed that the factors in the assessment of 'necessity', which, on the one hand, include weighing and balancing, and on the other, the assessment of reasonable availability of a less trade-restrictive measure, contain a logical contradiction and are incompatible: the first assessment leaves WTO members much less regulatory autonomy than the other.[282] This has resulted in a disagreement between two groups of academics, one of which argues that the weighing and balancing in the assessment of necessity requires a fully-fledged proportionality or cost-benefits assessment.[283] The other group, however, contends that the analysis of necessity turns on the assessment of reasonable availability of a less trade-restrictive measure.[284]

In most instances, the WTO adjudicating bodies do base their reports on the

---

[276] WTO, Appellate Body Report, *Korea – Various Measures on Beef*, paras. 160-161; WTO, Appellate Body Report, *US – Gambling*, para. 310; WTO, Note by Secretariat, 'Necessity tests' in the WTO, S/WPDR/W/27, 2 December 2003, pp. 8-9.
[277] WTO, Panel Report, *Argentina – Financial Services*, paras. 7.685, 7.727, referring to WTO, Appellate Body Report, *Korea – Various Measures on Beef*, para. 163.
[278] WTO, Appellate Body Report, *US – Gambling*, para. 307.
[279] *Ibid*., para 308; WTO, Appellate Body Report, *Korea – Various Measures on Beef*, paras. 176, 178.
[280] Andenas, Zleptnig, p. 414; Hilf, Puth (2002), p. 199; Marceau, Trachtman (2002), pp. 826–828, 851–853; Marceau, Trachtman (2014), pp. 368-369; Weber (2012), p. 43.
[281] Regan (2007); McGrady (2009); Lang (2007).
[282] See, e.g., Venzke (2011), p. 1136; Regan (2007), p. 348; Lang (2007); Howse, Nicolaïdis (2001).
[283] Andenas, Zleptnig, p. 414; Hilf, Puth (2002), p. 199; Marceau, Trachtman (2002), pp. 826–828, 851–853; Marceau, Trachtman (2014), pp. 368-369; Weber (2012), p. 43; Venzke (2011), p. 1136.
[284] Kurtz (2016), p. 199-201, Regan (2007), p. 349; Venzke (2011), p. 1136.

assessment of reasonable availability of a less trade-restrictive measure, and rightly so. This is a more lenient approach than the proportionality assessment, which arguably allows WTO members to choose the level of protection of the public interest at issue.[285] In *US-Gambling*, the Appellate Body explicitly equated the absence of necessity with the reasonable availability of another WTO consistent measure.[286] However, the risk that those bodies will conduct a fully-fledged cost-benefit analysis always remains. For example, in one of the most recent WTO Panel reports, the Panel based its analysis on the weighing and balancing of the three factors mentioned above *without* engaging into a comparison of the contested measure with reasonably available alternative measures.[287] Furthermore, in practice, the WTO members' autonomy to choose and maintain their own level of protection could be much narrower than it may seem at first glance, notably because it can be narrowed depending on how the adjudicating bodies interpret the term '*same* level' of protection.

Does the 'same' level of protection mean a *desired* level of protection (subjectively determined by the State and not (yet) necessarily achieved) or the *actual* level of protection achieved by the disputed measures? The WTO adjudicating bodies have not been consistent in their answer to this question. For example, in *Korea – Various Measures on Beef*, based on the *actual* application of the contested measure, judging by the design of the contested measure the Appellate Body 'assumed' that 'Korea intended to reduce considerably the number of cases of fraud occurring with respect to the origin of beef sold by retailers' rather than to 'totally eliminate fraud'.[288] From this perspective, alternative measures (compared to the contested measure) should not be required to achieve a higher level of protection than that *actually* achieved by the contested measure. The level of protection *desired* by the defending WTO member is thus irrelevant. Remarkably, in that case, the alternative measure that, according to Appellate Body, was reasonably available to Korea, involved significantly higher administrative and enforcement costs.[289] This, however, did not prevent the Appellate Body from concluding that the contested measure

---

[285] Regan (2007), 350; Venzke (2011), 1138.
[286] WTO, Appellate Body Report, *US Gambling*, para. 307 (stating that: '[i]t is on the basis of this "weighing and balancing" and comparison of measures, taking into account the interests or values at stake, that a panel *determines whether a measure is "necessary" or, alternatively, whether another, WTO-consistent measure is "reasonably available"*.) (emphasis added).
[287] WTO, Panel Report, *US – Tariff Measures*, paras. 7.232-7.238. It could, however, also be argued, that in that particular case the Panel did not consider reasonably available alternatives because the contested measure did not meet step 2 in the assessment. In particular, as a reason for not engaging in such analysis the Panel states that '[t]he Panel's preliminary conclusion, based on a weighing and balancing of the relevant factors, is that the United States has not explained how the chosen measures are apt to contribute to the public morals objective, as invoked by the United States, and how they could therefore be "necessary"'.
[288] WTO, Appellate Body Report, *Korea – Various Measures on Beef*, para. 178, internal footnotes omitted.
[289] *Ibid*. para 175.

did not pass the assessment under the third factor. Conversely, in *US – Gambling*, where the alternative measure proposed by the claiming party was dismissed as 'not an appropriate alternative', the Appellate Body explained that a 'reasonably available' alternative measure should preserve the responding Member's 'right to achieve its desired level of protection'.[290] Although the Appellate Body did not elaborate on the degree of deference to the WTO member in the assessment of the '*desired level'*, it could still be argued that the choice of this word requires an assessment of what the WTO member aimed for, rather than an objective assessment of what the contested measure actually achieves. In *EC – Seals*, the WTO Panel concluded that because of the exceptions from the ban on seal products, which allowed certain commercial activities within the European Union, 'the level of protection actually achieved by the measure is as high as the European Union claims the measure initially aimed to achieve' and that the Panel 'will bear this in mind in … subsequent analysis of the reasonable availability of a less trade-restrictive alternative measure'.[291] Although in that particular case, both the Panel and the Appellate Body nevertheless concluded that a less restrictive measure was not reasonably available to the EU,[292] clearly the risk that trade adjudicating bodies may not respect the level of protection asserted by a defending party persists.[293]

More generally, even if the adjudicating bodies were to afford sufficient deference to the level of protection desired by the State, the analytical exercise of ensuring that an

---

[290] WTO, Appellate Body Report, *US – Gambling*, paras. 308, 317, footnotes omitted. (emphasis added). The WTO Appellate Body reiterated the same approach in WTO, Appellate Body Report, *EC – Seal Products*, para. 5.261: 'in order to qualify as a genuine alternative, the proposed measure must be not only less trade restrictive than the original measure at issue, but should also preserve for the responding Member its right to achieve its desired level of protection with respect to the objective pursued'. (internal footnotes and quotation marks omitted.)

[291] WTO, Panel Reports, *EC – Seal Products*, para. 7.466; WTO, Appellate Body Report, *EC – Seal Products*, para. 5.203.

[292] WTO, Appellate Body Report, *EC – Seal Products*, para. 5.279; WTO, Panel Reports, *EC – Seal Products*, para. para. 7.504. Both the Panel and the Appellate Body, however, found that the contested EU ban on seal products did not meet the requirements of the Chapeau of Article XX GATT because the exceptions for some commercial activity with seal products in the EU lead to unjustifiable discrimination, and that discrimination could not be reconciled with, or is rationally related to, the policy objective of protecting public morals. WTO, Panel Reports, *EC – Seal Products*, para. 7.648; WTO, Appellate Body Report, *EC – Seal Products*, para. 5.339.

[293] From a pluralist perspective, there is an argument that by not establishing 'in any meaningful sense … concrete rules of decision on the public interest exceptions' and not settling 'the lines of authority' the WTO Appellate Body have 'moved toward a more pluralist structure. It has created space for states to use WTO law to keep fighting about the proper balance between the WTO policy on liberalization and their own idiosyncratic regulatory goals. This balance is unstable and consistently at issue in WTO legal disputes'. Hakimi (2020), p. 569. Thus, from this perspective, leaving the tests for assessing whether trade-inconsistent measures can be justified under public interest exceptions is a desirable outcome conducive to sustaining the WTO as a forum where 'trade governance happens'. See also Shaffer (2008), p. 71, arguing that by keeping their opinions ambiguous, WTO adjudicating bodies 'can shape their decisions to facilitate [compliance by powerful WTO Members] and amicable settlement, and thereby uphold the WTO legal system'.

alternative measure would achieve exactly the same level of protection would be nothing more than educated second-guessing. When the public policy goals pursued by contested measures are non-economic values, in practice it may be especially difficult to accurately define the level of their protection which serves as a benchmark for the comparison of alternative measures. It is equally difficult to determine *ex ante* whether alternative measures would secure the same level of protection.

Recall that, while the assessment of reasonably available alternative measures is conducted in the light of the importance of the public interest at stake, existing WTO case law does not shed much light on the weight of this factor in the assessment. There is, therefore, a related risk that the importance of the public interest, as determined by the adjudicating bodies, may influence the assessment of whether a less trade restrictive alternative measure is reasonably available. One could argue that the importance of the interest influences the deference to the level of protection chosen by the country. Thus, in *Korea – Various Measures on Beef*, where the Appellate Body did not make any statement as to the importance of the public interest pursued by the contested measure, the level of deference to the chosen level of protection was lower as compared to *US – Gambling*, where the Appellate Body agreed that the contested measure protected 'very important societal interests'.[294]

Relying on the analysis above, one may conclude that the application of trade law's necessity test to the EU framework for transfers of personal data to third countries, as implemented in the GDPR, may not result in the recognition of the 'necessity' of this framework by the WTO adjudicators.[295] Although the chances of this outcome are higher (should trade adjudicating bodies apply the proportionality assessment), the risk remains, even in the case of a more lenient interpretation of 'necessity', which amounts to the assessment of reasonably available alternatives to a contested measure.[296] There are at least two reasons for this. First, it could be argued that there is an insufficient nexus between the

[294] WTO, Appellate Body Report, *US – Gambling*, para 232, referring to WTO, Panel Report, *US – Gambling*, paras. 6.492, 6.533.

[295] Although there are statements in academic literature to the contrary, the publications that contain argumentation on this point are rather outdated and do not take into account the most recent developments in EU data privacy law, most importantly the CJEU's post-2009 jurisprudence on the fundamental rights to privacy and the protection of personal data, in particular the *Schrems I* and *II* decisions. See, e.g., Asinari (2002); Shaffer (2000). Of the most recent literature, those arguing that EU restrictions would satisfy the necessity test typically do not engage in elaborate discussion and rather presume that since there is an exception for data protection, there is a chance that EU framework can be justified. See, e.g., Chen (2015), p. 219, who limits the assessment to one sentence: 'Although until now, there hardly has been a case that the responding party won by claiming the general exceptions clause, one could still see the interest of privacy being recognized through the substantial establishment of an exclusive clause for privacy in Article 14 (c) subsection (ii) of the GATS'.

[296] Reyes (2011), p. 33-34. Generally, several scholars have highlighted the risk of unpredictability in the WTO jurisprudence on the necessity test. See, e.g., Bygrave (2014), p. 198; Weber (2012); Reyes (2011), p. 12; Venzke (2011), p. 191; Mishra (2020), p. 350.

contested restrictions on transfers of personal data, and the aim of achieving a high level of protection. Second, the EU framework for transfers of personal data may be recognised as not the least trade restrictive.

On the first point, it could be argued that the link between the existing EU framework for data transfers and the purpose of ensuring a high level of protection of personal data, particularly from foreign governments' ability to access this data, is closer to 'making a contribution to' rather than 'indispensable'. As demonstrated above, mechanisms for systematic personal data transfers under the GDPR must ensure that the level of protection that a particular third country ensures in respect to the transferred data is 'essentially equivalent' to that in the EU,[297] where the 'level of data protection' means not only the quality of the data protection rules, but multiple other factors, including: the respect for the rule of law and human rights, access of public authorities to personal data, the existence and effective functioning of independent supervisory authorities, etc.[298] There is, however, a sizeable gap between the level of protection that this framework *should* and *can* deliver in practice. The Transatlantic saga on cross-border data flows is but one illustration of the point.[299]

After the CJEU invalidated the adequacy decision for the US (the EU-US Safe Harbor framework) in 2015 by *Schrems I* judgement – which also introduced for the first time the 'essential equivalence' requirement – against a background of low level of enforcement, personal data continued flowing to the US despite the absence of 'essentially equivalent' protection of such data.[300] The 2016 EU-US Privacy Shield framework, which replaced the Safe Harbor and underlay transatlantic personal data transfers for almost four years, did not – as the CJEU confirmed in the *Schrems II* judgement – remedy the absence of 'essentially equivalent' protection of personal data under US law.[301] Although it is too early to judge, some predict that (as happened after the *Schrems I* judgement), even after *Schrems II* 'data will continue to flow across borders;[302] indeed, at the time of writing, it still does, both on the basis of the invalid Privacy Shield and the SCCs without additional safeguards.[303]

On the second point, one could argue that the EU framework is not the 'least trade restrictive', especially in relation to businesses not having an establishment or business partner in the EEA. For example, one could argue that 'it may be difficult to prove that

[297] CJEU, *Schrems I*, para 73; CJEU, *Schrems II*, para. 94; recital 104 GDPR.
[298] Art. 45 GDPR.
[299] For further discussion, see Section 5.3.
[300] See Sections 5.3.1 and 5.3.2.
[301] CJEU, *Schrems II*.
[302] Tene (2020b).
[303] See, e.g. Lee (2020).

privacy cannot be otherwise protected'.[304] The fact that compliance with the standard of the recently modified Convention 108 – characterised by Greenleaf as 'close to the current global average for data privacy laws'[305] – is in itself insufficient, especially in the light of the CJEU *Schrems II* judgement, to warrant an adequacy decision from the EU,[306] and demonstrates that the benchmark set by the EU is higher than that recognised by any other international standards. Under recital 105 of the GDPR, when assessing the adequacy of personal data protection in a third country, the EU Commission should take into account accession of that country to Convention 108.[307] However, Article 14(1) of the Convention 108+ allows a Party to the Convention to restrict transfers from another Party to the Convention if 'bound by harmonised rules of protection shared by States belonging to a regional international organisation'.[308] Given that compliance with the Convention 108+ does not constitute a sufficient ground for adequacy under the GDPR, it is possible that following the assessment by the European Commission of the legal framework of a Party to this Convention, the adequacy decision will not be granted.

One could assert, as a counter-argument, that the level of protection of the fundamental right to personal data protection chosen by the EU – 'effective and complete' protection[309] – makes other, less restrictive alternatives unavailable to the EU. In particular, in contrast to the EU Charter, some international standards on personal data protection, such as the OECD 2013 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the 2015 Asia-Pacific Economic Cooperation (APEC) Privacy Framework[310] take an *instrumental* approach to the protection of personal data and therefore warrant a *lower level* of personal data protection (their primary purpose is to keep restrictions on personal data transfers to a minimum).[311] At the same time, just like the EU Charter and the GDPR, the Convention 108+ recognises the right to the protection of personal data as a human right.[312] Nevertheless, the restrictions on transfers of personal data to countries that are not Parties to this Convention are still less stringent than those under EU data protection framework.[313] As explained above, it is entirely possible that,

[304] Burri (2017b), pp. 95-96.
[305] Greenleaf (2018a), p. 2.
[306] For a discussion, see, e.g., Duque de Carvalho (2019); Greenleaf (2018a), p. 5.
[307] See also Article 29 Working Party, Working document on Adequacy Referential, WP 254rev.01, 6 February 2018.
[308] Para. 107 of the Explanatory Report to the modernised Convention 108 clarifies that this provision applies in particular to the member States of the EU.
[309] CJEU, *Google Spain*, para. 34; CJEU, *Wirtschaftsakademie*, para. 28; CJEU, *Fashion ID*, paras. 50, 66.
[310] APEC Privacy Framework (2015).
[311] For a comparison of these standards with the European framework, see Yakovleva (2018), pp. 8-9.
[312] Art. 1 Convention 108+.
[313] While Art. 14 of Convention 108+ conditions transfers of personal data to a State or international organization that is not a party to the Convention on the requirement of securing an 'appropriate' level of

given the lack of international harmonisation of data privacy rules, trade adjudicators would give little deference to the EU's *desired* high level of protection, and would focus instead on the *actual* level of protection achieved.[314] In the absence of reliable statistics on this matter, and the difficulty of producing any concrete evidence of the level of data privacy protection,[315] the adjudicators may buy into empirical arguments, such as those offered by Bamberger and Mulligan, that compared the EU data protection regime to the more liberal US approach, and found that, although the latter was not as comprehensive 'on the books,' it operated much more effectively 'on the ground'.[316] Assessment of the 'effectiveness' of data protection on the ground, does not take into account the non-instrumental protection of fundamental rights to privacy and the protection of personal data as moral values.[317] Therefore, from an EU law perspective, it could be viewed as incomplete. However, it is precisely the instrumental approach that could be ultimately adopted by trade adjudicating bodies. As Howse and Langille argue:

> where the basis for arguing that a measure is not pretextual is at least partly motivated by noninstrumental moral concerns not universally shared by WTO members, there is a risk that a WTO official or adjudicator who does not share the value in question, or is unfamiliar from its own moral experience with this kind of belief, will begin from a presumption that there is a strong risk of pretextualism. … [T]he WTO insider community is drawn from a world of diplomats and bureaucrats where a certain kind of instrumental-often economic-rationality dominates conceptions of appropriate public policy. As our analysis of the Seal Products dispute has illustrated, using tests or devices that employ instrumental rationality, such as means/ends reasoning, simply does not work to establish the non-pretextual character of noninstrumental moral regulation.[318]

In addition, some studies suggest that restrictions on transfers of personal data do not sufficiently contribute to ensuring privacy protection against foreign surveillance.[319] The dual facts that the EU framework for transfers of personal data provides the same restrictive

---

protection, the GDPR conditions systematic transfers of personal data to a third country or international organisation subject to a requirement that that third country ensures an 'adequate' level of protection, interpreted as 'essentially equivalent' by the CJEU.

[314] Weber (2012), pp. 40-41, 45.

[315] This issue is discussed in more detail in Section 3.4.2.

[316] Bamberger, Mulligan (2015). Koops also underscores 'an enormous disconnect' between European data protection law and reality. Koops (2014), p. 256.

[317] For further discussion see Section 3.4.2.

[318] Howse, Langille (2012), p. 429. See also Howse, Langille, Sykes (2015), pp. 105-106. The authors make an argument in relation to the legislation that can be justified under the general exception for public morals. This reasoning is, however, also applicable to other legislation subject to justification under specific thematic exceptions of the general exceptions, such as the one for privacy and data protection.

[319] Maurer, Morgus, Skierka, Hohmann (2015), p. 61; Komaitis (2017), pp. 361-362.

approach to any information that qualifies as personal data (which includes a broad range of data under EU law),[320] and does not calibrate restrictiveness in relation to the severity of the risk of interference in individuals' fundamental rights, could also be used as an indication that other (more granular and overall less trade restrictive) frameworks are 'reasonably available' to the EU. Consequently, the importance of the right to the protection of personal data would be given relatively less weight in a trade dispute. While in EU law it is recognised as a fundamental right — and hence one of the highest values in the EU and on a par with other fundamental rights, trade adjudicating bodies may lean towards an economic approach to privacy and data protection that underlies the existing international standards on data protection mentioned above.[321]

2.3.3 Necessity under EU law

From the CJEU case law, it follows that any legislative act of the EU that involves personal data processing, such as the use or transfer of personal data, constitutes 'in itself' a limitation of the fundamental right to the protection of personal data, regardless of whether it can be justified.[322] Such a limitation first triggers the assessment under the requirements of Article 8(2) of the EU Charter. Then, any limitation on this right is only lawful if it meets the requirements of Article 52(1) of the EU Charter,[323] which provides a mechanism for balancing different fundamental rights and freedoms with each other, as well as with other competing policy objectives.[324]

It is the prerogative of the CJEU to conduct a fact-based assessment of whether a derogation is 'necessary' in each particular case.[325] As already mentioned above, since 2009, the CJEU has established a higher threshold for derogations from the fundamental rights to privacy and the protection of personal data under Article 52(1) of the EU Charter when balancing these fundamental rights with other competing rights and interests. In a line of cases, most notably *Volker und Markus Schecke*,[326] *Digital Rights Ireland*,[327] *Tele*

[320] See Purtova (2018).
[321] Yakovleva (2018), pp. 482-485, 489, 496.
[322] CJEU, *Digital Rights Ireland*, paras. 34 – 36; CJEU, *Volker und Markus Schecke*, para. 58. See also EDPS, Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit', 11 April 2017, p. 7.
[323] Existing CJEU case law suggests that the conditions of lawfulness of personal data processing contained in art 8(2) and art 52(1) of the EU Charter should analysed cumulatively. See, e.g., CJEU, *Opinion on EU-Canada PNR Agreement*, paras. 137-138, 142ff.
[324] Unlike international trade law, the text of art 52(1) EU Charter explicitly mentions that the assessment of 'necessity' should include a fully-fledged proportionality balancing.
[325] Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit', 11 April 2017, 8.
[326] CJEU, *Volker und Markus Schecke*, paras. 77 and 86.
[327] CJEU, *Digital Rights Ireland*, paras. 51 and 52.

2,[328] *Schrems I*,[329] *Schrems II*,[330] and *Opinion on EU-Canada PNR Agreement*,[331] the CJEU elevated the EU Charter necessity test to the level of 'strict necessity' when a derogation from the fundamental rights to privacy and the protection of personal data is at stake. This approach was later taken up by the Article 29 Working Party[332] and the European Data Protection Supervisor (EDPS).[333] It is now settled CJEU case law that the 'strict necessity' standard should apply horizontally in all contexts, to both commercial and national security, as long as limitation of the fundamental rights to privacy and data protection is involved.[334]

Just as with the trade necessity test, 'strict necessity' under Article 52(1) of the EU Charter in relation to privacy and data protection is hard to satisfy. In assessing 'strict necessity', the CJEU determines whether 'it is possible to envisage measures which affect less adversely that fundamental right of natural persons and which still contribute effectively to the objectives … in question.'[335] This approach resembles the least-restrictive-means principle in the interpretation of the trade necessity test. While trade law requires that measures aimed at protecting the right to protection of personal data should be least restrictive on trade, conversely, the EU Charter demands that trade rules should be least restrictive of fundamental rights.

According to the CJEU, legislation interfering with fundamental rights to privacy and the protection of personal data can only pass the 'strict necessity' if it:

> lay[s] down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where

[328] CJEU, *Tele2 Sverige*, paras. 96 and 103.
[329] CJEU, *Schrems I*, para. 92.
[330] CJEU, *Schrems II*, para. 176.
[331] CJEU, *Opinion on EU-Canada PNR Agreement*, para 140.
[332] See e.g. Article 29 Working Party, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), WP 237, 13 April 2016, p. 5.
[333] EDPS, Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit', 11 April 2017, p. 2.
[334] See EDPS, Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit', 11 April 2017, p. 7, referring to a line of the CJEU jurisprudence.
[335] CJEU, Volker und Markus Schecke, para. 86.

personal data is subject to automated processing.[336]

The CJEU factored in two other general considerations to its analysis: First, the seriousness of the interference that a particular measure limiting the fundamental rights to privacy and the protection of personal data entails[337] and second, the importance of the interest pursued by the measure. Concerning the latter factor, one might recall that the relative importance of competing interests also takes part in the assessment of trade 'necessity'. According to the CJEU, the objective of *public security can justify even serious interferences* with privacy and data protection, if such measures meet the 'strict necessity test'.[338] However, the economic interests of a private party, as explained above, seem to be at the other end of the importance continuum. Thus, although data protection may not be considered of highest importance in international trade law, cross-border digital trade is unlikely to weigh heavily against data protection in the EU's fundamental rights calculus.

2.3.4 The incompatibility of two 'necessities'

Now that both tests have been explicated, one can see that the risk of tension lies in the fact that neither the EU's trade liberalisation commitments to trade in services nor a potential decision of an international trade adjudicating body requiring the EU to reduce the restrictions on cross-border transfers of personal data to comply with such commitments, are likely to survive the EU Charter's 'strict necessity' assessment.

To show the polar opposition between the two tests, one could say that, because transfers of personal data outside the EEA amount to a limitation of the fundamental rights to privacy and the protection of personal data, the CJEU's assessment of the liberalisation of data transfers starts from the question of 'whether transfers *should be allowed* and under what conditions'. In trade law, the question is the opposite, namely 'whether transfers *should be limited*'. Implementing a decision by an international trade adjudicating body requiring the EU to lower the standard of 'essential equivalence,' which all the mechanisms for systematic personal data transfers should meet based on the CJEU jurisprudence,[339] would run afoul of the core of the conditions under which the CJEU considers transfers of personal data outside the EEA compliant with the EU Charter. It follows from the CJEU *Schrems II* judgment that, in the context of transfers of personal data outside the EEA, the 'essential equivalence' requirement is an instantiation of the strict necessity test of article

[336] CJEU, *Schrems II*, para. 176, internal footnotes omitted. See also CJEU, *Schrems I*, paras 93, 95; CJEU, *Opinion on EU-Canada PNR Agreement*, paras. 140-141, 154.
[337] EDPS, Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit', 11 April 2017, p. 7.
[338] CJEU, *Opinion on EU-Canada PNR Agreement*, paras. 149, 154. (emphasis added)
[339] CJEU, *Schrems I*, para. 73; CJEU, *Opinion on EU-Canada PNR Agreement*, paras. 93, 134; CJEU, *Schrems II*, paras. 96, 104-105.

52(1) of the EU Charter,[340] which makes it a matter of primary rather than secondary EU law.[341]

Two other core conditions for the compliance of a data transfer mechanism with the EU Charter are the existence and effective functioning of an independent supervisory authority, and effective administrative and judicial remedies for individuals. All the mechanisms allowing for systematic transfers of personal data outside the EEA meet, to some extent, this condition.[342] This component of the fundamental right to the protection of personal data alone renders infeasible, under the EU Charter, any approach to data transfers that does meet the following two criteria. First, those that do not allow for a preliminary assessment of the legal regime in the country of destination. And, second, those that do not require a commitment from a personal data recipient in a foreign country to grant EU individuals certain safeguards to exercise their rights to judicial remedy. Even if other mechanisms for data transfers are theoretically possible, those mechanisms, *if applied horizontally to all types of personal data*, would not be less trade restrictive than those already envisaged in the GDPR.

2.4 Ways forward

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

---

[340] CJEU, *Schrems II*, paras. 184-185.
[341] For further discussion on this issue see Section 5.2.2.
[342] E.g. Art. 45(2)(b) GDPR on adequacy assessment, Arts. 47(2)(e), 40(4) and 40(2)(k) GDPR, Clause 5(c) and 7(1)(b) Standard contractual clauses (Set I); Clause V(c) and para (7) of preamble to Commission Decision 2004/915/EC approving Standard contractual clauses (Set II); Clause 5(e) and 7(1)(b) of Standard contractual clauses for controller to processor transfers. In *Schrems II*, the CJEU explicitly confirmed that the latter SCC Decision meets the requirement to ensure an effective remedy. CJEU, *Schrems II*, paras. 144, 145, 148.

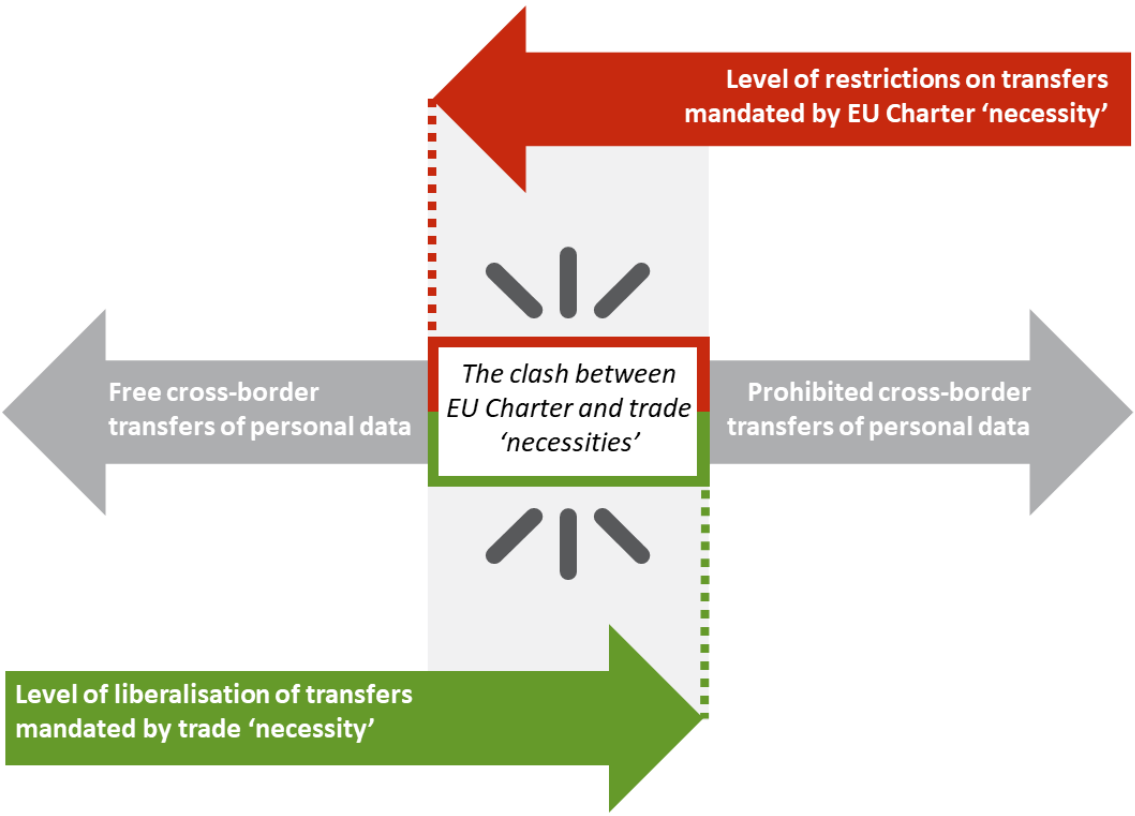

Figure 1: Overlap between the EU Charter and Trade 'Necessities' (Design: Helma van der Wal)

In the context of the ongoing digital trade negotiations that the EU is conducting with its trading partners on cross-border data flows, privacy and data protection, this state of affairs is not sustainable. As explained in Section 2.3.1 above, the EU should be able to comply with the Charter *and* its international trade obligations *simultaneously*. The path forward suggested in this thesis, and further elaborated on in Chapters 3 and 4, is guided by three principal considerations. First, from a practical perspective, it is risky to wait until the EU restrictions are struck down by – or even challenged by – an international trade adjudicating body which will force the EU's hand. A more proactive approach seems preferable. Second, and relatedly, ongoing uncertainty surrounding the lawfulness of transfers of personal data outside the EEA, on the one hand, and compliance with the restrictions on such transfers with EU's international trade commitments, on the other hand, may have a chilling effect on cross-border trade to the detriment of EU businesses. Third, although the approach to transfers of personal data outside the EEA that would make the most solid contribution to the 'effective and complete' protection of the fundamental rights to privacy and the protection of personal data is a total ban on such transfers, this rather extreme approach would undermine the very existence of digital cross-border trade with the EU and is thus unwarranted.

This thesis envisions that the problem explicated in this Chapter should be

addressed from both international trade and EU law perspectives. It elaborates on the ways this can be done in Chapters 4 and 5 respectively. From an international trade law perspective, as discussed in Chapter 4, one way out of the quandary is to negotiate a broader general exception for the protection of personal data in future trade agreements, one that would embrace the EU's restrictions on transfers of personal data without jeopardising EU trade policy ambitions. Chapter 5 of the thesis explores, from an EU law perspective, the possibility of reforming the current framework for transfers of personal data outside the EEA in a way more conducive to international trade, whilst keeping within the constitutional boundaries of the EU charter. However before the thesis moves on to those discussions, the next Chapter uses elements of discourse analysis to explicate the role of narratives in the negotiation and interpretation of trade agreements, and how such narratives could affect the baseline between legitimate protection of data privacy, and protectionism in trade adjudication.

2.5 Conclusion

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