Governing cross-border data flows

Reconciling EU data protection and international trade law

Yakovleva, S.

Publication date
2021

5. EU framework for transfers of personal data: critique and directions for reform

5.1 Introduction

This Chapter addresses the problem of the 'two necessities' identified in Chapter 2 of the thesis from an EU Charter and EU data protection law perspective. The arguments in this Chapter are structured along the following three broad issues: (1) the constitutional boundaries the EU Charter imposes on EU secondary law governing transfers of personal data outside the EEA; (2) the ability of the current EU framework for transfers of personal data outside the EEA to perform its constitutional function; and (3) the reform proposal for such framework in response to changed (geo)political and economic circumstances.

The first issue on the constitutional boundaries set by the EU Charter on EU secondary law is a relatively unexplored topic in current academic debates. Relying on prevailing opinion, this Chapter approaches this issue through the prism of Article 51(2) of the Charter, which contains two layers of requirements with respect to derogations from fundamental rights: such derogations must respect the 'essence' of those fundamental rights and be 'strictly necessary'[948] and proportionate. In other words, the essence (or the core) of fundamental rights cannot be interfered with by secondary EU law. Other derogations from fundamental rights are possible, provided that they meet the necessity and proportionality tests. This Chapter argues that there is a dynamic relationship between the GDPR (as a secondary EU law instrument) and the EU Charter (as a primary law instrument), in that EU secondary law has, to some extent, influenced the essence of the fundamental right to the protection of personal data. At the same time, only a few aspects of the current framework for transfers of personal data constitute the *essence* of the fundamental rights to privacy, to the protection of personal data and to effective judicial remedy (in the context of the first two rights), which cannot be changed by secondary EU legislation. The concept of 'essential equivalence', which, following the CJEU *Schrems II* judgement, can be seen as the constitutional benchmark for the secondary law framework on transfers of personal data, does not constitute a part of the essence of the above-mentioned fundamental rights. Instead, this concept is an instantiation of the strict necessity and proportionality requirements under Article 52(1) of the EU Charter in the context of transfers of personal data. It governs the balancing of the above-mentioned fundamental rights against competing policy objectives, primarily economic benefits inherent in unrestricted cross-border flows of personal data, and the national security interests of foreign countries. Building on this normative legal framework under EU law,

[948] As explained in Section 2.3.3, the for derogations from the fundamental rights to privacy and data protection, the CJEU has elevated the 'necessity' threshold under Art. 52(1) EU Charter to 'strict necessity'.

this Chapter contends that the EU legislator has sufficient wiggle room to change the design of the rules currently codified in Chapter V of the GDPR.

The second issue is the ability of the current EU framework for transfers of personal data under Chapter V of the GDPR to perform its constitutional function against the background of circumstances that have changed since this framework was first designed. As already mentioned elsewhere in this thesis, this framework's main function is to prevent circumvention of the high level of personal data protection in the EU and, ultimately, to ensure 'effective and complete' protection of fundamental rights.[949] This Chapter identifies four weaknesses in this framework.

The first weakness is that, despite the recent *Schrems II* judgement, there is a persistent qualitative gap between the adequacy decisions on the one hand, and the appropriate safeguards under Article 46 of the GDPR on the other (both of which serve as mechanisms for systematic transfers). In other words, the level of protection ensured by adequacy decisions, even considering their flaws, is higher than the level of protection that can be achieved through private law mechanisms under Article 46 of the GDPR. In the *Schrems II*, the CJEU shifted the requirements of assessing the adequacy of foreign legal frameworks towards the companies, many if not most of which lack the necessary expertise, resources and incentives to conduct those assessments, or even to the DPAs, which lack human and financial resources. This is unlikely to solve the problem. Instead, this Chapter predicts that the lawfulness of transfers of personal data will ultimately be decided by EU member state courts following private enforcement efforts, which, at least in the short and medium term, may lead to the fragmentation of the rules for transfers of personal data outside the EEA across Europe. Only in the long term can this fragmentation be remedied through references for preliminary ruling to the CJEU. This Chapter argues that the EU should address the foreign surveillance problem – which is the main reason why issues relating to transfers of personal data land at the CJEU – on the international level rather than through its own secondary law. The second weakness is, as this Chapter argues, that adequacy decisions are prone to political pressures in the context of EU trade policy. The third weakness is that adequacy decisions are unable to perform their constitutional function due to lack of regular reviews of the assessment on which the adequacy decisions are based (the 'snapshot' problem), the difficulties of enforcing individual rights in foreign jurisdictions (the 'heavy burden' problem), and the inadequacy of onward transfer mechanism embedded in the adequacy decisions (the 'onward transfer' problem). The fourth and last weakness is, on a more abstract level, the limited scalability of the current regime for personal data transfers in Chapter V of the GDPR in view of the

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

technological developments that have occurred since the 1990s, when the core of the framework was first designed.

The third and final issue addressed in this Chapter is the reform proposal for a new EU framework for transfers of personal data outside the EEA. Relying on the analysis in this thesis and existing reform proposals in the literature, this Chapter suggests three directions or lines of thought on how to improve the framework of Chapter V of the GDPR, reflecting possible short, medium, and long term strategies for the EU in this area.

To make those points, the Chapter proceeds as follows. Section 5.2 examines the constitutional contours of the EU's framework for transfers of personal data, including the room for manoeuvre the EU legislator has in designing such a framework. Section 5.3 of this Chapter addresses the weaknesses of the current framework in Chapter V of the GDPR. Section 5.4 elaborates on the three directions of thought on how to ameliorate these weaknesses through a reform of the GDPR's Chapter V. Section 5 concludes.

5.2 Constitutional contours of the EU's framework for transfers of personal data

The EU maintains a 'multi-level protection of fundamental rights' comprised of primary and secondary law, which applies equally to the rights to privacy and the protection of personal data.[950] As already mentioned elsewhere in this thesis, Articles 7 and 8 of the EU Charter protect the rights to privacy and the protection of personal data as fundamental rights. The EU legislator's competence underlying the adoption of the GDPR is provided for in Article 16 TFEU, namely, the competence to 'lay down the rules relating to the protection of individuals with regard to the processing of personal data'.

This Section tackles two questions regarding the relationship between EU primary and secondary data protection rules in the context of cross-border transfers of personal data. First, whether, and to what extent, the *design of the current framework* for transfers of personal data in Chapter V of the GDPR is grounded in the EU Charter. Another way to approach this question is to ask which parts of the framework cannot be changed without running afoul of the EU Charter requirements for data transfers. The second, and more general, question is how much leeway, in the view of the EU Charter, the EU legislator has in designing the mechanisms for transfers of personal data in the GDPR.

5.2.1 The relationship between the EU Charter and EU secondary data protection law

In the hierarchy of EU law, secondary law is, as the name suggests, below primary law, which, in turn, has the highest legal force in the EU.[951] Therefore, from a formalistic perspective, secondary law should be consistent with primary law. However, in practice –

[950] Brkan (2019), p. 865.
[951] Craig, De Burca (2015), pp. 105, 110.

as demonstrated by CJEU jurisprudence – this relationship is not as clear-cut as it may seem[952] and is underexplored in academic literature, especially when it comes to the relationship between the EU Charter and the EU framework for data transfers.

Based on CJEU case law, Syrpis argues that EU secondary law may relate to EU primary law in at least three different ways. First, as just mentioned, in some cases the CJEU views primary law as hierarchically superior to secondary law, meaning that secondary law is rendered inapplicable when in conflict with primary law. Second, in other cases, the CJEU interprets primary and secondary law 'neutrally', meaning that interpretation of primary law affects the interpretation of secondary law and vice versa. Third, in yet other cases, secondary law has a significant impact on the CJEU's interpretation of primary law and, to some extent, determines its content.[953] In sum, Syrpis claims that the CJEU's approach on this issue has been inconsistent, which gives the EU legislator the power to affect the CJEU's interpretation of EU Treaties.[954]

Thus, the modes of relationship between primary and secondary law that can be deduced from CJEU case law broadly represent two diverging approaches to the 'proper' relationship between EU primary and secondary law. The first, which this Chapter calls a *static* approach, puts the emphasis on the formal CJEU powers to interpret secondary law in the light of primary law and invalidate the former when contrary to the latter,[955] and corresponds with the hierarchical relationship between EU primary and secondary law. The second, which this Chapter calls a *dynamic* approach, adopts a less hierarchical view of primary and secondary law, in which secondary law, although limited by the primacy of primary law (and should be annulled if the legislature has 'manifestly' or 'manifestly and gravely' exceeded the limits of its powers[956]), reflects the '(democratic) will expressed by the political [EU] institutions' and, therefore, should able to affect the interpretation of EU primary law by the Court.[957] This dynamic approach corresponds to the second and third ways of interaction between primary and secondary law, as identified by Syrpis.

Following the dynamic approach to the relationship between EU primary and secondary law, Muir explains that EU secondary legislation can implicate fundamental rights in three ways.[958] First, based on the EU competence to legislate on fundamental rights, some EU secondary legislation is *designed* to 'give specific expression' to a

[952] Syrpis (2009), p. 465.
[953] *Ibid.*, pp. 465-467.
[954] *Ibid.*, p. 466.
[955] *Ibid*., pp. 482-483.
[956] *Ibid*., pp. 484.
[957] *Ibid*., p. 483-485
[958] Muir (2014), p. 223.

fundamental right.[959] Second, legislative instruments designed to implement an 'ordinary' EU competence – a competence other than fundamental rights protection – can incidentally set fundamental rights standards.[960] Finally, EU secondary legislation can merely define the scope of the EU courts' fundamental rights jurisdiction.[961]

Based on the ways of thinking about the relationship between EU primary and secondary law proposed by Syrpis and Muir, this Section contends, first, that Chapter V of the GDPR (as well as Section V of the GDPR's predecessor – the Data Protection Directive) should be viewed as secondary legislative instruments 'giving specific expression' to the fundamental rights, and establishing a system of checks and balances on the limitations of those fundamental rights. Second, the Chapter argues that there is a dynamic relationship between the EU framework on transfers of personal data and the EU Charter. This relationship manifests itself in the concept of 'essential equivalence', first introduced through the interpretation of the concept of 'adequacy' in Article 25 of the Data Protection Directive in the light of the EU Charter, and later injected into Chapter V of the GDPR as the central constitutional requirement for compliance of *any* systematic transfer of personal data outside the EEA, rather than just adequacy. The discussion below elaborates on each of these points.

The relationship between EU primary and secondary law in the area of data protection is not clear-cut. On the one hand, the limited CJEU case law concerning the fundamental right to the protection of personal data enshrined in Article 8 of the Charter leans towards a more hierarchical approach between the two. For example, in *Digital Rights Ireland* the CJEU invalidated the EU Data Retention Directive because by adopting it 'the legislature exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter (of Fundamental Rights)'.[962] In *Schrems I*, the CJEU invalidated the Commission's implementing act approving the EU-US Safe Harbor,[963] and in *Schrems II*, the Commission's implementing act approving the Safe Harbor's successor – the EU-US Privacy Shield.[964] In the *Opinion on EU-Canada PNR Agreement*, the CJEU found the draft EU-Canada PNR agreement inconsistent with the EU Charter, treating the agreement as an 'equivalent externally, of that which is a legislative act internally'.[965] On the other hand, the origins of this fundamental right, as well as the evolution of the concept of 'essential equivalence' in the

[959] *Ibid*., pp. 223-226, emphasis added.
[960] *Ibid*., pp. 226-227.
[961] *Ibid*., pp. 227-229.
[962] CJEU, *Digital Rights Ireland*, para 69.
[963] CJEU, *Schrems I*.
[964] CJEU, *Schrems II*, paras. 150-202.
[965] CJEU, *Opinion on EU-Canada PNR Agreement*, para. 146.

design of the EU framework for transfers of personal data, show that EU secondary law also influenced the conceptualisation of this right. This influence demonstrates a dynamic approach between the two.

The Data Protection Directive was adopted before the Lisbon Treaty and, as already mentioned above, was based on the EU internal market competence.[966] It had a profound effect on the formation and the content of the fundamental right to the protection of personal data in the Charter.[967] According to the Explanations relating to the Charter, one of the foundations of Article 8 of the Charter is that the Data Protection Directive contains 'conditions and limitations for the exercise of the right to the protection of personal data'.[968] Indeed, paragraph 2 of Article 8 can be seen as codifying the secondary law principles of fair and lawful data processing, the right of individuals to access their personal data, the right to rectification as well as the establishment of an independent supervisory authority to ensure compliance with the fundamental right – all of which were already present in the Data Protection Directive.[969] In its 2015 *Schrems I* judgement, the CJEU pointed to a reverse relationship between the Data Protection Directive and the EU Charter (which was already legally binding at that time). The CJEU held that the Directive's Article 25(6) governing the adequacy mechanism for transfers of personal data outside the EEA '*implements the express obligation laid down in Article 8(1) of the Charter* to protect personal data and … is intended to ensure that the high level of that protection continues where personal data is transferred to a third country'.[970] This demonstrates that the relationship between the fundamental right to the protection of personal data and the EU Data Protection Directive was a two-way street.

Unlike the Data Protection Directive, the GDPR was '*specifically* adopted in order to give expression' to the fundamental right to the protection of personal data.[971] It constitutes secondary legislation adopted on the basis on Article 16 of the TFEU and the Charter. As rightly pointed out by Ausloos, the GDPR 'has a primarily enabling or instrumental role' of putting in 'place an infrastructure of checks and balances to ensure fairness [of personal data processing]' and setting 'the parameters for legitimate processing

---

[966] See Section 2.2.1.1.
[967] Dalla Corte (2020), p. 45 (arguing that '[t]he right to data protection has been strongly shaped by the evolution of the secondary legislation'). See also Muir (2014), p. 226 (stating that '[a]lthough adopted in the mid–1990s as an internal market instrument on the basis of the equivalent of today's Article 114 TFEU, in substance the Directive is specifically designed to give shape to a fundamental right'). Similar point of view is expressed by Dalla Corte (2020), pp. 44-45. But see Tzanou (2017), pp. 38-39, arguing that the meaning of Article 8 should be independent from EU secondary law.
[968] Explanation to Art. 8, Explanations Relating to the Charter of Fundamental Rights, 2007 O.J. (C 303).
[969] See Arts. 6, 7, 12 and 28 of the Data Protection Directive respectively. Art. 8 EU Charter is also based on Art. 8 ECHR and Convention 108, which has been ratified by all the Member States.
[970] CJEU, *Schrems I*, para. 72. This goal is now explicitly incorporated in Art. 44 GDPR (emphasis added).
[971] Muir (2014), p. 224.

of personal data in the light of the Charter as a whole'.[972] This not only includes articles codifying the substantive fundamental rights, but also Article 52(1) of the EU Charter setting the boundaries for derogation from those fundamental rights. In general terms, while 'Article 8 [of the] Charter is substantive, the GDPR is procedural'.[973] This, however, does not mean that the right to the protection of personal data is the only fundamental right operationalised by the GDPR.[974] In addition, just like the Data Protection Directive, the GDPR *limits* the fundamental rights enshrined in the EU Charter,[975] as any processing of personal data constitutes a derogation from the fundamental right under Articles 7 and 8 of the Charter.[976] The GDPR sets the rules for lawful processing of personal data, which must remain within the boundaries of Article 52(1) of the Charter governing derogations from the fundamental rights. This also means that the requirements of this article serve as a constitutional compass in the interpretation and application of the GDPR.

5.2.2 'Essential equivalence': from EU secondary law to EU Charter and then back again

In the spirit of the dynamic relationship between EU primary and secondary law on data protection, in its *Schrems I* judgement the CJEU interpreted the term 'adequate level of protection' from Article 25(6) of the Data Protection Directive in the light of the EU Charter, 'as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is "*essentially equivalent*" to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter.'[977] This Article's aim is to ensure continuity of the high level of personal data protection after personal data is transferred outside the EEA and to prevent circumvention of the EU data protection framework.[978] Several scholars have argued that by interpreting 'adequacy' as 'essential equivalence' the CJEU has elevated the standard of data protection that a third country must meet to be afforded an adequacy decision.[979]

In the *Opinion on EU-Canada PNR Agreement*, the CJEU applied the 'essentially equivalent' standard outside the context of the Data Protection Directive, in relation to the

[972] Ausloos (2018), pp. 62-63. See also Clifford, Ausloos (2018), p. 147 (arguing that 'the GDPR is a clear manifestation of a secondary framework built on checks and balances in order to respect 'control' as the essence of the right to data protection'), See also Dalla Corte (2020), p. 45.
[973] Ausloos (2018), p. 63.
[974] Oostveen, Irion (2017); Ausloos (2018), pp. 62-63; Clifford, Ausloos (2018), p. 147. See also Section 1.1.3.
[975] For a discussion, see Clifford, Ausloos (2018), pp. 148, 152-154.
[976] 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.
[977] CJEU, *Schrems I*, para. 73 (emphasis added).
[978] *Ibid*.; CJEU, *Opinion on EU-Canada PNR Agreement*, para. 214; CJEU, *Schrems II*, para. 93.
[979] See, e.g., Roth (2017), p. 63; Petkova (2019), p. 153.

draft EU-Canada PNR Agreement. Its compliance with the EU Charter was assessed in that case and did not fall under the scope of the Directive. Just as in *Schrems I*, however, the Court invoked the concept of 'essential equivalence' as an *interpretation of the notion of 'adequacy'* incorporated into the text of the draft Article 5 of the EU-Canada PNR Agreement.[980] In that Opinion, the CJEU referred to the *Schrems I* judgement – without referring to the adequacy provision of the Directive – and stated that:

> the transfer of personal data, such as PNR data, from the European Union to a non-member country is lawful only if there are rules in that country which ensure a level of protection of fundamental rights and freedoms that is *essentially equivalen*t to that guaranteed within the European Union.[981]

This led Kuner to conclude that the CJEU's reference to the standard of essential equivalence 'leaves no doubt that this standard also applies to data transfers under international agreements'.[982]

Although the CJEU did not explain the relationship between the concept of 'essential equivalence' and the assessment under Article 52(1) of the Charter, this Chapter contends that the Court used the concept of 'essential equivalence' as an instantiation of balancing under Article 52(1) of the EU Charter in application to the EU secondary law's concept of 'adequacy'. In other words, by ensuring that an adequacy decision guarantees that the level of personal data protection abroad is 'essentially equivalent' to that in the EU, the European Commission can strike the right balance under the strict necessity test of Article 52(1) of the EU Charter. This indirectly follows from the fact that, in *Schrems I,* the CJEU first conducted an assessment under Article 52(1) of the Charter (paragraphs 92 – 95) but then in paragraph 96 returned to the principle of 'essential equivalence' and finally in paragraph 98 concluded that the Commission's decision was incompliant with Article 25(6) of the Directive read in the light of the Charter.

The relationship between restrictions on transfers of personal data as a component of the fundamental right under Article 8 of the Charter and its implementation in secondary law can also be illustrated by this quote from the CJEU *Opinion on EU-Canada PNR Agreement*:

> That right to the protection of personal data requires, inter alia, that the high level of protection of fundamental rights and freedoms conferred by EU law *continues*

---

[980] This Article states that '[s]ubject to compliance with this Agreement, the Canadian Competent Authority is deemed to provide an *adequate level of protection, within the meaning of relevant European Union data protection law*, for the processing and use of PNR data'. CJEU, *Opinion on EU-Canada PNR Agreement*, para. 86.
[981] CJEU, *Opinion on EU-Canada PNR Agreement*, para. 93; see also *ibid.*, paras. 134 and 214.
[982] Kuner (2018), p. 872.

> where personal data is transferred from the European Union to a non-member country. Even though the means intended to ensure such a level of protection may differ from those employed within the European Union *in order to ensure that the requirements stemming from EU law are complied with*, those means must nevertheless prove, *in practice*, effective in order to ensure *protection essentially equivalent to that guaranteed within the European Union*.[983]

This quote suggests that the principle of 'essential equivalence' is also a *practical implementation of the constitutional requirement* of continuity of protection in EU secondary law. Extrapolating the relationship between the fundamental right in Article 8 of the EU Charter and secondary data protection law, to the relationship between Article 52(1) of the EU Charter and the concept of 'essential equivalence', one can thus conclude that the first is substantive and the second is procedural; it is one of the tools in the toolbox of secondary law ensuring that the fundamental right is not derogated from further than is allowed under Article 52(1) of the EU Charter.

The interpretation of 'adequacy' as 'essential equivalence' later found its way to the text of the GDPR. Recital 104 of the GDPR states, in relation to the adequacy framework in Article 45 of the GDPR, that [t]he

> third country should offer guarantees ensuring an adequate level of protection *essentially equivalent* to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress. (emphasis added)

The criteria to assess whether a foreign legal framework affords 'essentially equivalent' protection are listed in Article 45 GDPR. For systematic transfers of personal data to third countries not afforded an adequacy decision by the EU, however (such as those governed by Article 46 GDPR), the GDPR sets forth a requirement of 'appropriate safeguards'.[984] It should, therefore, be emphasised that, until *Schrems II*, as discussed below, the 'essential equivalence' requirement featured both in the CJEU case law discussed above, and in the GDPR, as the instantiation of the proportionality and strict necessity balancing under Article 52(1) of the EU Charter *solely in relation to the adequacy mechanism* for transfers of personal data, rather than in relation to the EU secondary law

[983] CJEU, *Opinion on EU-Canada PNR Agreement*, para. 134. (emphasis added)
[984] See also recital 107 GDPR.

framework for transfers of personal data *as a whole*. This created a qualitative gap – criticised in academic and policy discourse and discussed in more detail in Section 5.3.1 of this Chapter – between the level of protection that must be guaranteed to transferred personal data by an adequacy decision, on the one hand, and by appropriate safeguards under Article 46, such as the SCCs and the BCRs, on the other hand. In *Schrems II*, the CJEU confirmed its prior analysis of what the 'essential equivalence' standard requires in relation to an adequacy decision,[985] but it also took an important step towards reinstating a consistent and holistic approach to the EU framework for transfers of personal data.[986] In particular, the Court held that

> data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded, as in the context of a transfer based on an adequacy decision, a level of protection *essentially equivalent* to that which is guaranteed within the European Union.[987]

The CJEU further explained that the level of protection of fundamental rights required by Article 46(1) of the GDPR 'must be determined on the basis of the provisions of that regulation, read in the light of the fundamental rights enshrined in the Charter'.[988] The factors that should be taken into account for such assessment in the context of Article 46 'correspond to those set out, in a non-exhaustive manner, in Article 45(2) of [the GDPR]'.[989] One could, therefore, argue that not only adequacy decisions, but indeed *all* mechanisms for systematic transfers of personal data outside the EEA should provide an 'essentially equivalent' level of protection. Despite the fact that factors outlined in Article 45(2) of the GDPR – based on the textual interpretation – only apply to adequacy decisions, they should, when interpreted in the light of the EU Charter, be considered in the assessment related to any other mechanism for systematic transfer of personal data. By doing so, as explained above, the CJEU asserted the 'essential equivalence' standard as an instantiation of the 'strict necessity' and proportionality balancing under Article 52(1) of the EU Charter in the context of the whole framework for systematic transfers of personal data in EU secondary data protection law. It is no longer a constitutional *interpretation* of 'adequacy', but has acquired a meaning independent of 'adequacy'. The factors for adequacy assessment became a part of such 'essential equivalence' requirement. This outcome fits with the understanding of the GDPR as a legal framework creating the system of checks and balances that enable the protection of the fundamental rights. Based on this, all provisions of the GDPR, and therefore, all mechanisms for systematic transfers of

---

[985] CJEU, *Schrems II*, para. 176.
[986] For a discussion, see Christakis (2020); Kuner (2020d).
[987] CJEU, *Schrems II*, para. 96 (emphasis added); see also *Ibid.*, para. 105
[988] CJEU, *Schrems II*, para. 101.
[989] CJEU, *Schrems II*, para. 104.

personal data, should meet the strict necessity test provided in Article 52(1) of the Charter.[990]

To sum up, 'essential equivalence' is the EU Charter requirement in relation to the level of personal data protection that any EU secondary law mechanism for transfers of personal data should ensure. Recall, in addition, that the standard of 'essentially equivalent' protection is not only the CJEU's creation in the line of cases on cross-border transfers of personal data.[991] It closely resembles the 'essentially comparable' standard used by the German Constitutional court in the 1986 *Solange II* case when assessing the level of fundamental rights protection in the EU as compared to the German legal order, and codified in Article 23 of the German Basic Law.[992] The fact that the *Solange I* was one of the reasons that prompted the EU transition from an economic to a constitutional union,[993] supports the conclusion that the standard of 'essential equivalence' is very likely to 'stick' even without adequacy being mentioned in the EU secondary law. In any event, what matters is that the CJEU determined that this standard constitutes a yardstick to gauge the permissible derogations from the fundamental rights set forth in Article 52(1) of the Charter in the context of transfers of personal data outside the EEA.

5.2.3 The concept of the 'essence' of fundamental rights

The previous Section has argued that the GDPR sets up a system of checks and balances for the legitimate processing of personal data in the light of the EU Charter. It has concluded that the EU primary law, and more specifically the EU Charter, set the boundaries for the legislature to regulate transfers of personal data outside the EEA in the form of the 'essential equivalence' requirement. This Section looks into the question of those boundaries more specifically and circumscribes the degree of discretion that the EU legislature has in designing the framework of cross-border transfers of personal data outside the EEA.

The EU law concept that seems to be most helpful in drawing a red line between the elements of a fundamental right that can and cannot be restricted is the concept of the 'essence' of fundamental rights, which appears in Article 52(1) of the EU Charter.[994] This provision requires that any limitation on the exercise of the fundamental rights must (a) be

[990] Clifford, Ausloos (2018), pp. 148, 152.
[991] Azoulai, van der Sluis (2016), p. 1363.
[992] *Ibid.*, p. 1363; Mayer (2015); Wünsche Handelsgesellschaft decision of 22 October 1986, BVerfGE 73, 339, case number: 2 BvR 197/83, Europäische Grundrechte-Zeitschrift, 1987, 1, [1987] 3 CMLR 225 (*Solange II*).
[993] For a discussion, see, e.g., Perju (2017).
[994] Dawson, Lynskey, Muir (2019), p. 767.

provided for by law (first sentence), (b) respect the essence of those rights (first sentence) and (c) meet the principles of proportionality and necessity (second sentence).

The concept of the 'essence' of fundamental rights in general, and of the fundamental rights to privacy and the protection of personal data in particular, remains 'elusive' in the CJEU case law and relatively unexplored in academic literature.[995] Gellert and Gutwirth even dismiss the 'assumption that there is, eventually and behind all descriptions, such thing as an essence of privacy and data protection'.[996] This Section looks into the meaning of the 'essence' of fundamental rights, in general and in application to the fundamental rights to privacy and the protection of personal data, with the aim to determine what – if anything – constitutes the essence of those fundamental rights in relation to transfers of personal data outside the EEA. In doing so, this Section relies on the relatively scarce literature and CJEU case law available on this topic.

Scholars generally agree that the notion of 'essence' is an 'absolute limit to balancing, i.e. to underline that a certain interference actually "destroys" a certain right or strips it of any content.'[997] Relying on the CJEU case law on the fundamental rights to privacy and the protection of personal data, Brkan convincingly argues that the concept of the 'essence' of fundamental rights contained in Article 52(1) of the EU Charter is 'an independent constitutional concept that is not a part of the principle of proportionality.'[998] This means that an interference with the essence of a fundamental right cannot be justified based on a necessity and proportionality assessment.[999] Along similar lines, CJEU's President Koen Lenaerts noted that where an 'EU measure fails to take due account of the essence of a fundamental right, that measure is incompatible with the Charter and must be annulled or declared invalid.'[1000] As the Advocate General Henrik Saugmandsgaard Øe argued in the *Schrems II* case,

> when an interference compromises [the essence of] those rights and freedoms, no legitimate objective can justify it. The interference is then deemed to be contrary to the Charter without it being necessary to examine whether it is appropriate and necessary for the purpose of achieving the objective pursued.[1001]

---

[995] Lynskey (2015), pp.. 270-272. See also Dalla Corte (2020), p. 48; Porcedda (2018), p. 2.
[996] Gellert, Gutwirth (2013), p. 522.
[997] Von Bogdandy, Kottmann, Antpöhler, Dickschen, Hentrei, Smrkolj (2012), p. 511. See also Clifford, Ausloos (2018), pp. 146-147; Porcedda (2018), p. 3; Dalla Corte (2020), p. 50.
[998] Brkan (2019), p. 868.
[999] *Ibid.*, p. 883.
[1000] Lenaerts (2019), pp. 779, 782.
[1001] Opinion AG in *Schrems II*, para. 272. See also EDPS, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 19 December 2019, p. 8.

In other words, a measure interfering with the essence of a fundamental right is 'automatically disproportionate',[1002] which makes, in Lenaerts' view, the 'essence test' and the 'proportionality test' (including where there is a particularly serious interference with a fundamental right at stake) two separate lines of inquiry under Article 52(1) of the EU Charter.[1003] Building on the CJEU's judgement in *Schrems I,* Lenaerts further explains that the 'essence' of a fundamental right refers to its 'hard nucleus', which is *absolute* and 'must always remain free from interference'.[1004] This concept thus suggests that the EU legislator may only 'determine non-essential elements' of those rights, and that secondary law may not affect the absolute 'nucleus' of those rights under the Charter.[1005] More generally and relatedly, the EU legislator's discretion in using secondary law to operationalise fundamental rights is proportionate to the level of interference with fundamental rights that the legislation in question entails.[1006] Applying this line of reasoning to the GDPR, one can conclude that the GDPR, which operationalises the fundamental rights to privacy and data protection by setting the limits within which these fundamental rights can be interfered with,[1007] may only permit derogation from these fundamental rights to the extent it does not interfere with their nucleus. Put differently, any GDPR rule must respect the 'essence' of the fundamental rights affected by data processing, and primarily the rights to privacy (Article 7 of EU Charter), the protection of personal data (Article 8 of EU Charter) and judicial remedy (Article 47 of EU Charter), which most often feature in the CJEU case law touching upon the 'essence' of fundamental rights in the context of personal data processing.

To sum up, unlike the shades of grey in balancing in the assessment of necessity and proportionality under Article 52(1) of the EU Charter, the assessment of whether the 'essence' of fundamental rights was respected is black and white: either the interference with the fundamental right respects the essence of that right, or it does not.

5.2.4 The 'essence' of the fundamental rights to privacy, protection of personal data and judicial remedy

In order to operationalise the concept of the 'essence' of fundamental rights in the context of this thesis, it is important to understand what – if anything – constitutes the essence of the fundamental rights to privacy and the protection of personal data, as well as

---

[1002] Lenaerts (2019), p. 781.
[1003] *Ibid.*, p.781.
[1004] *Ibid.*, p. 782.
[1005] Dawson, Lynskey, Muir (2019), p. 767.
[1006] Lenaerts (2019), p. 793.
[1007] As noted above, in the view of the CJEU and the EU Data protection Authorities, any processing of personal data constitutes a derogation from the fundamental right to privacy and the protection of personal data. 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.

the right to effective remedy in the context of interferences with the first two fundamental rights, as applied in a line of CJEU jurisprudence. Unfortunately, both the role of the 'essence' and the definition of the 'essence' in relation to the above-mentioned fundamental rights is not yet fully developed in the CJEU jurisprudence and academic literature.[1008]

Although the Court's approach to the conceptualisation of essence and its conclusions could be criticised as 'contentious'[1009] and lacking 'coherence' and 'conceptual clarity',[1010] it is beyond the scope of this thesis to engage more fully with such critique. Using available CJEU jurisprudence on the topic and its interpretation in literature, this thesis addresses only three issues that are germane to it. First, it considers the aspects that constitute the essence of the fundamental rights protection of privacy, personal data and the right to effective remedy in the context of the first two rights based on existing CJEU case law. Second, it analyses whether restrictions on transfers of personal data outside the EEA, and the concept of 'essential equivalence', constitute a part of the essence of the right to the protection of personal data. Third, it examines whether there is a 'rule of thumb' on how to identify the essence of the relevant fundamental rights in situations not yet addressed by the CJEU, in particular, in relation to transfers of personal data outside the EEA.

The CJEU has interpreted the notion of the 'essence' of the fundamental rights to privacy, the protection of personal data and judicial remedy (in the context of the other two rights) in five judgements thus far: *Digital Rights Ireland*, *Tele2 Sverige*, *Schrems I and II*, and *Opinion on EU-Canada PNR Agreement*. In *Schrems I*, the CJEU held that 'legislation permitting the public authorities to have access on a generalised basis *to the content of electronic communications* must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.'[1011] In contrast, legislation, which 'authorises, on a generalised basis, *storage of all the personal data of all the persons* whose data has been transferred … without any differentiation, limitation or exception being made' does not interfere with the 'essence' of the right to privacy, but rather violates the principle of 'strict necessity' under the second sentence of Article 52(1) of the Charter.[1012] The Court reached the same conclusion in

[1008] Dawson, Lynskey, Muir (2019), p. 769; Kuner (2018), p. 87; Lynskey (2015), p. 268; Clifford, Ausloos (2018), pp. 130–187.
[1009] See, e.g., Brkan (2019), p. 865.
[1010] Dawson, Lynskey, Muir (2019), p. 769.
[1011] CJEU, *Schrems I*, para. 94 (emphasis added). Brkan extensively criticises this distinction between the data that constitutes the content of electronic communications and the metadata, as large volumes of metadata can reveal almost as much personal data about the individuals as, or even more than, the content of communications. Brkan (2019), pp. 872-873, 879.
[1012] CJEU, *Schrems I*, para. 93.

Digital Rights Ireland[1013] and *Tele2 Sverige*.[1014] In his Opinion in *Schrems II*, the Advocate General continued the CJEU's approach in prior cases that, as long as there is no 'generalised access by the public authorities to the content of the electronic communications', there is no 'breach of the very essence' of the right to privacy.[1015] In its *Schrems II* judgement, the CJEU, however, followed neither its own line of reasoning in *Schrems I* nor that of the Advocate General; it remained silent on whether the EU-US Privacy Shield interfered with the essence of the right to privacy or the right to protection of personal data.[1016] Instead, it held that EU-US Privacy Shield did not ensure 'essential equivalent' protection because 'limitations on the protection of personal data arising from the domestic law of the United States … are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law, by the second sentence of Article 52(1) of the Charter.'[1017] The CJEU also did not mention the issue of generalised access by public authorities to the content of electronic communications. In the *Opinion on EU-Canada PNR Agreement*, where access to content or other electronic communications data was not the issue, the CJEU concluded that the EU-Canada PNR Agreement did not interfere with the right to privacy because although 'PNR data may, in some circumstances, reveal very specific information concerning the private life of a person, the nature of that information *is limited to certain aspects of that private life*, in particular, relating to air travel between Canada and the European Union.'[1018]

In relation to the right to effective remedy under Article 47 of the Charter, in the context of the rights to privacy and the protection of personal data, the CJEU found that the essence of this right was not respected in two cases. In *Schrems I* and *Schrems II* the CJEU held that 'legislation *not providing for any possibility* for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter.'[1019]

Unlike the fundamental right to privacy, the CJEU has not yet found a violation of essence of the fundamental right to the protection of personal data. In *Digital Rights Ireland*, the Court concluded that there was no such interference because the contested Data Retention Directive required respect of 'certain principles of data protection and data

---

[1013] CJEU, *Digital Rights Ireland*, paras. 37, 39, 69, 73.
[1014] CJEU, *Tele2 Sverige*, para. 101.
[1015] Opinion AG in *Schrems II*, para 278.
[1016] CJEU, *Schrems II*, para. 185. This deviation from *Schrems I* could be attributed to the critique of the CJEU's *Schrems I* approach to finding the interference with essence of the fundamental right. See e.g. Brkan (2019), pp. 877-878.
[1017] *Ibid.*
[1018] CJEU, *Opinion on EU-Canada PNR Agreement*, para 150.
[1019] CJEU, *Schrems I*, para. 95; CJEU, *Schrems II*, para. 187 (emphasis added).

security' in order to 'ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data.'[1020] In *Tele2 Sverige*, where the CJEU discussed the right to privacy and to the protection of personal data jointly, the CJEU held that as long as the contested legislation 'does not permit retention of the content of a communication', it does not affect adversely the essence of the right to the protection of personal data.[1021] In the *Opinion on EU-Canada PNR Agreement*, the CJEU found that the EU-Canada PNR Agreement did not interfere with the essence of the fundamental right to data protection for two reasons: first, because it limited 'the purposes for which PNR data may be processed', and second, because it contained the rules to ensure 'the security, confidentiality and integrity of that data, and to protect it against unlawful access and processing'.[1022] The Advocate General in his Opinion in *Schrems II* followed the CJEU's line of reasoning in *Opinion on EU-Canada PNR Agreement*, namely that the

> essence of the right to protection of personal data, guaranteed in Article 8 of the Charter, is preserved when the purposes of the processing are limited and the processing is accompanied by rules designed to ensure, inter alia, the security, confidentiality and integrity of the data, and also to protect them against unlawful access and processing.[1023]

The Advocate General further noted that, although there was a doubt whether the US surveillance programmes, allowed under the EU-US Privacy Shield, defined the purposes of processing of personal data 'with sufficient clarity and precision to ensure a level of protection essentially equivalent to that prevailing in the legal order of the Union', 'those possible weaknesses would not suffice … to substantiate a finding that such programmes would … violate the essence of the right to protection of personal data'.[1024] In its *Schrems II* judgement, the CJEU did not separate the issue of interference with the essence of the fundamental right to protection of personal data from the interference with the fundamental right to privacy.[1025]

Brkan criticises the CJEU's approach to the essence of fundamental rights, noting that in relation to privacy it is quantitative instead of qualitative,[1026] and in relation to the protection of personal data – 'extremely restrictive and technical'.[1027] In the latter case, she

---

[1020] CJEU, *Digital Rights Ireland*, para. 40.
[1021] CJEU, *Tele2 Sverige*, para. 101. The Court discusses the right to privacy and the right to the protection of personal data at the same time by referring to 'these rights'.
[1022] CJEU, *Opinion on EU-Canada PNR Agreement*, para 150.
[1023] Opinion AG in *Schrems II*, para 279.
[1024] *Ibid.*, para 280.
[1025] See, e.g., CJEU, *Schrems II*, paras. 169-172, 178, 199.
[1026] Brkan (2019), pp. 872, 877.
[1027] *Ibid.*, pp. 878-879.

argues, the Court reduced the essence of the right to certain aspects of it, turning the core of the right to a minimum rather than a maximum standard.[1028] In contrast, Lenaerts argues that the essence of the fundamental rights to privacy and the right to effective judicial remedy is only compromised when 'the limitation in question empties those rights of their content or calls their very existence into question'.[1029] The same logic arguably applies to the protection of personal data. From his perspective, the 'essence' should be interpreted restrictively so that it can only be compromised in 'extreme cases', because a broad understanding of this concept would make fundamental rights absolute, which is undesirable in a democratic society.[1030]

This overview of the CJEU case law shows that the nucleus of the fundamental right to privacy and, even more so, the fundamental right to the protection of personal data is rather small. To sum up, the CJEU case law suggests that secondary EU law must:

- Not permit generalised access to the content of electronic communications *in order to respect the essence of the fundamental right to privacy*.
- (a) Limit the purposes of processing (i.e. respect the purpose limitation principle); (b) require that the processing of personal data is accompanied by rules designed to ensure, inter alia, the security, confidentiality and integrity of the data, and also to protect them against unlawful access and processing, and (c) not permit retention of the content of communications *in order to respect the essence of the fundamental right to the protection of personal data; and*
- Provide scope for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, in order to respect the *essence of the fundamental right to judicial remedy in the context of privacy and data protection*.

From this summary it is clear that, rather than defining the 'essence' of the fundamental rights to privacy, protection of personal data and effective remedy, the CJEU has chosen to distil, on a case-by-case basis, a number of requirements that EU secondary law should meet in order for the essence of the respective rights to be respected.

The next question is whether restrictions on transfers of personal data and in particular the standard of 'essential equivalence' constitute the essence of the fundamental rights to privacy and the protection of personal data. At the outset, it should be mentioned that restrictions on transfers of personal data are not mentioned among the elements of this

[1028] Brkan (2019), pp. 878-879.
[1029] Lenaerts (2019), p. 784.
[1030] *Ibid.*, p. 793.

fundamental right codified in Article 8(2) of the EU Charter. This, however, is not a decisive factor, because, as Brkan convincingly argues, although these elements are 'constitutive of this fundamental right' they do not automatically constitute its essence.[1031] Conversely, the fact that a certain element of the right is not mentioned in this provision does not mean that it does not constitute the essence of the right.

Based on the fact that both in *Schrems I and II* as well as in *Opinion on EU-Canada PNR Agreement* the CJEU assessed whether EU law instruments ensured an 'essentially equivalent' level of protection by conducting a balancing exercise on the basis of the second sentence of Article 52(1) of the EU Charter, one can conclude that the 'essential equivalence' requirement does not constitute the essence of any of the fundamental rights discussed in this Section.[1032] The assessment of whether the standard of 'essential equivalence' is met is the second step in the assessment under Article 52(1) of the EU Charter. This conclusion confirms the finding above that 'essential equivalence' is the instantiation of the 'strict necessity' requirement of Article 52(1) of the EU Charter in application to transfers of personal data outside the EEA.

Until now, the CJEU dealt with the question of the essence of the fundamental rights to privacy, the protection of personal data, and to judicial remedy (in the context of the first two rights) on a case-by-case basis. One could ask whether there is, or could be, a rule of thumb which would allow a line to be drawn between the absence of respect of the essence of a fundamental right and a particularly serious interference with the right, which should be balanced with an overriding public interest on the basis of principles of necessity and proportionality.

Although the requirements listed above apply to all secondary data protection rules, including those governing transfers of personal data outside the EEA, the CJEU case law does not offer a rule of thumb to determine, more generally, what constitutes the essence of the fundamental rights to privacy, data protection and judicial remedy (in the context of the first two rights), and whether a specific *design* of rules on transfers of personal data outside the EEA is necessary in order to respect this essence. While some scholars argue that there is no 'fixed or universally valid essence of rights that can be conceptually deduced' and that the '"European essence" of fundamental rights' can only be determined 'inductively by analysing the jurisprudence of the courts with regard to certain infringements upon certain rights that cannot be justified',[1033] others offer ways of thinking

[1031] Brkan (2019), p. 881-882. See also Dalla Corte (2020), p. 46 (expressing the same point of view.) But see Kuner (2015b), pp. 243-244 (suggesting as a preliminary thought that rights listed in Article 8 of the EU Charter could be viewed as the 'essence' of the fundamental right to the protection of personal data.)
[1032] Brkan's analysis of whether essentially equivalent level of protection and the concept of essence of fundamental rights should be equated supports this conclusion. Brkan (2019), p. 865.
[1033] Von Bogdandy, Kottmann, Antpöhler, Dickschen, Hentrei, Smrkolj (2012), p. 511.

about the essence of the fundamental rights, which could be useful in answering the question posed above.

Generalising the Court's approach, Lenaerts concludes that the limitation of a fundamental right respects its essence if it 'does not call [it] into question as such'.[1034] Therefore, if a limitation concerns only 'certain aspects of a fundamental right, leaving others untouched, or that only applies in a specific set of circumstances regarding the individual conduct of the person concerned', the essence of the fundamental right is respected.[1035] The key factors the Court uses in this assessment are the *intensity* and the *extent* of the limitation of the fundamental right at issue.[1036] The next Section discusses how this analysis can apply to rules on transfers of personal data outside the EEA.

5.2.5 The 'essence' and restrictions on transfers of personal data outside the EEA

Although transfers of personal data outside the EEA affect not only the fundamental right to the protection of personal data but also the right to privacy, this Section focuses on the essence of the fundamental right to the protection of personal data. The reason for this is that the 'home' of the EU secondary law framework on transfers of personal data outside the EEA is in the GDPR, which, in the first place, effectuates the fundamental right to the protection of personal data. This right is thus most relevant for the purposes of this Section, which considers approaches to the essence of fundamental rights proposed in the context of the governance of data processing in the GDPR.

For the purposes of this Section, the most useful ways of thinking about the essence of the fundamental right to the protection of personal data are those proposed by Clifford and Ausloos and by Dalla Corte.[1037] Clifford and Ausloos claim that 'control constitutes the essence of the right to data protection. "Control" here - they argue - should be interpreted broadly and not simply as an individual's "control" over their personal data but

[1034] Lenaerts (2019), pp. 785, 792. Brkan proposes a second prong to this test, namely that to establish whether there is an interference with the essence of a fundamental right it is also necessary to evaluate whether there is an overriding public interest that can justify such interference. As long as there exists such an interest, the CJEU should engage in proportionality assessment and rule out the breach of essence of the fundamental right at issue. Brkan (2019), p. 869.
[1035] Lenaerts (2019), pp. 785, 792.
[1036] *Ibid.* See also Brkan (2019), pp. 877-878 (arguing that in EU-Canada PNR Opinion the CJEU 'adopts a position that the interference with the essence of the right to privacy is a question of a degree of interference with the fundamental right, given that it takes as a benchmark the limited nature of the acquired and processed data'.)
[1037] Porcedda also extensively discusses the essence of the fundamental right to data protection in her work. See, e.g., Porcedda (2018). Her proposal to defining the essence of the fundamental right to the protection of personal data by using the concept of 'attributes' of the right is less helpful for the purposes of analysis in this Section as she does not touch upon the rules on transfers of personal data outside the EEA.

as a *robust architecture of control* that actively pursues individual autonomy.'[1038] In arriving at such a conclusion, they emphasise the flexibility of the notion of 'respect' in Article 52(1) of the EU Charter in the protection of the essence of a right.[1039] In other words, it seems that, in these authors' view, the requirement of 'respect' allows a filtering out of the most appalling interferences with the right. Once the threshold of 'respect' is passed, interferences with the 'essence' of the rights are subject to a balancing test under the second sentence of Article 52(1) of the EU Charter. The checks and balances effectuating control as the essence of all fundamental rights and freedoms under the EU Charter (and not only the right to the protection of personal data), they argue, play a role at the level of the secondary framework, such as the GDPR.[1040]

Dalla Corte contends that the value of the fundamental right to data protection (as opposed to the right to privacy and other rights implicated by data processing), is 'in the very existence of a system of rules and norms applying to the processing of personal data, regardless of its connection with concepts like privacy, or the secrecy and confidentiality of the information processed.'[1041] In other words, from his perspective, the fundamental right to the protection of personal data is 'our fundamental "right to a rule" regulating personal data processing'.[1042] Thus, '[a] violation of the essence of the right to data protection would … exist in cases where the interference with the right challenges, explicitly or implicitly, the very societal choice of having an omnibus regime regulating the processing of personal data.'[1043] It 'endangers … the very functioning and legitimacy of the collective posture towards personal data processing in its entirety, and hence ultimately its deepest roots: the rule of law and the democratic legitimacy of EU regulation.' [1044] In this context, it is also worth recalling that, in a line of cases, the CJEU established that the objective pursued by the EU secondary data protection law (and, in particular, the Data Protection Directive) is to ensure 'effective and complete' protection of individuals.[1045]

Applying the – in a way similar – approaches to the essence of the right to the protection of personal data proposed by these authors, one could conclude that in relation to the governance of transfers of personal data outside the EEA, *the very presence of the*

[1038] Clifford, Ausloos (2018), pp. 144-145 (emphasis added). These authors also argue – as opposed to what has been discussed above - that the essence of the right to data protection can be limited, provided that 'effective balancing mechanisms are in place as specified in Articles 8(2) and 8(3) of the Charter'.
[1039] *Ibid.*, p. 145.
[1040] *Ibid.*, p. 152.
[1041] Dalla Corte (2020), p. 48.
[1042] *Ibid.*, p. 53.
[1043] *Ibid.*, p. 51-52.
[1044] *Ibid.*, p. 53.
[1045] CJEU, *Google Spain*, para 34; CJEU, *Wirtschaftsakademie*, para 28; CJEU, Jehovan todistajat, para. 66; CJEU, *Fashion ID*, paras. 66, 70.

restrictions (in general) on transfers of personal data outside the EEA constitutes a part of the essence of the right to the protection of personal data, as their complete absence would strip this fundamental right, and the system of checks and balances instantiating it in secondary law, of their meaning and content. This is because, in the absence of any restrictions on transfers of personal data, the entire EU legal framework governing the processing of personal data could be easily circumvented. It is the prevention of this circumvention, as has been shown above, that constitutes the very constitutional function of such restrictions. In a similar vein, restrictions on onward transfers of personal data from the first country of destination outside the EEA to other countries outside the EEA are equally essential in performing this function and, therefore, should also be considered a part of the essence of the fundamental right to protection of personal data. At the same time, the *particular design* of restrictions on transfers and onward transfers of personal data, apart from the rules identified in Section 5.2.5 above, is a matter of strict necessity and proportionality balancing.

To sum up, this Section has argued that there is a dynamic relationship between EU primary and secondary data protection law. 'Essential equivalence' is the constitutional benchmark for strict necessity and proportionality balancing in the design and application of rules on cross-border transfers. The essence of the fundamental rights to privacy, protection of personal data and judicial remedy will be respected – based on state of the art of CJEU case law and academic literature – when secondary data protection law meets all of the following conditions:

- provides for some limitations on transfers of personal data outside the EEA and on onward transfers,
- contains safeguards preventing generalised access of foreign authorities to the content of electronic communications,
- ensures that purposes for processing personal data are limited,
- requires that the processing of personal data is accompanied by rules designed to ensure, inter alia, the security, confidentiality and integrity of the data, and also to protect them against unlawful access and processing,
- does not permit retention of the content of communications, and
- provides for some possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data.

5.3 Weaknesses of the EU's framework for transfers of personal data from the EU Charter perspective

The previous Section has argued that the EU secondary law framework for transfers of personal data outside the EEA under Chapter V of the GDPR *can* and *should* be

evaluated for compliance with the EU primary law envisaged in the EU Charter. This Section conducts such an evaluation in the light of the constitutional function of this framework to prevent circumvention of the EU data protection framework and, ultimately, to ensure that the aim of the EU secondary data protection legislation – 'effective and complete' protection of fundamental rights in the course of processing personal data – is not undermined. This evaluation is conducted against the backdrop of ever-changing political, geopolitical and economic circumstances, which contrasts with the comparatively static nature of the EU secondary law framework for transfers of personal data outside the EEA. The discussion in this Section presumes, and does not question, the fact that the current GDPR rules respect the essence of the fundamental rights to privacy, the protection of personal data and judicial remedy and meets the strict necessity and proportionality tests under Article 52(1) of the EU Charter. The starting point for the analysis is that the rules on transfers of personal data in Chapter V of the GDPR may not be the most fit for the constitutional purpose of the framework.

As already explained in this thesis, the EU framework for transfers of personal data outside the EEA was designed in early 1990s and first introduced by the 1995 Data Protection Directive. The GDPR changed the particularities of the framework by adding some flexibilities, but it did not alter its core structure. For the reader's convenience, this Section briefly reiterates the structure of the EU's framework for transfers of personal data outside the EEA. As discussed in Section 2.2.1.3, just like the Data Protection Directive, the GDPR, as interpreted by the EDPB, adopts a layered approach to transfers of personal data, where each of the subsequent layers is subsidiary to the one above it.[1046] The first layer is an adequacy decision by the European Commission establishing that a third country's legal framework – both in general and in relation to the protection of personal data – is 'essentially equivalent' to that of the EU.[1047] Personal data can flow freely to a third country that has been afforded an adequacy decision, as if it is being processed within the EEA. The second layer of mechanisms for transfers of personal data, which apply in the absence of an adequacy decision, is the 'appropriate safeguards' put in place by the data controller or possessor (such as standard contractual clauses (SCCs), binding corporate rules (BCRs), certification, or codes of conduct).[1048] Data exporters and data importers must include the model SCCs, approved by the European Commission, *verbatim* into their agreements involving transfers of personal data.[1049] BCRs are codes of conduct regulating the processing of personal data by a group of undertakings or group of

[1046] Kuner questions, however, whether this is still the case following the CJEU *Schrems II* judgement. Kuner (2020b).
[1047] Art. 45 GDPR; CJEU, *Schrems I*, para. 73.
[1048] Arts. 46-47 GDPR.
[1049] Recital 81, Art. 46(2)(c) GDPR.

enterprises engaged in a joint economic activity.[1050] As clarified by the CJEU in *Schrems II*, when using appropriate safeguards for transfers of personal data to third countries that have not been afforded an adequacy decision, data exporters and importers must conduct a comprehensive case-by-case assessment of whether the use of such safeguards will ensure *in practice* a level of personal data protection 'essentially equivalent' to that in the EU.[1051] In exceptional circumstances, exporters of personal data may resort to the third layer of data transfer mechanisms – limited derogations under Article 49 GDPR (such as unambiguous consent of the data subject or the performance or conclusion of a contract with or in the interest of the data subject).[1052] The derogations may only be used for non-repetitive and occasional transfers, however.[1053] The layered approach requires that before using any of the derogations data exporters should first 'endeavour possibilities to frame the transfer' with one of the appropriate safeguards.[1054]

Between 1995, when the Data Protection Directive was adopted, and 2016, the year of adoption of the GDPR, at least three changes occurred, and they are crucial for the discussion in this Section. First, as mentioned in Chapter 2, the rights to the protection of privacy and personal data became binding fundamental rights in the EU.[1055] Second, following the Edward Snowden revelations,[1056] access to personal data transferred outside the EEA in a commercial context by the public authorities of a third country, and the availability of judicial redress against such authorities, became the most contentious issue in assessing the essential equivalence of third countries' legal systems. Not only for the purposes of affording adequacy decisions under the GDPR but, in general, for the EU framework for transfers of personal data outside the EEA.[1057] Recall, that in the aftermath of those revelations, in its 2015 *Schrems I* judgement, the CJEU invalidated the EU-US Safe Harbor framework for transfers of personal data from the EU to the US.[1058] *Schrems I* marked a watershed in the history of transfers of personal data. Five years later, in its *Schrems II* judgement the CJEU invalidated the Safe Harbor's successor – the EU-US Privacy Shield – on similar grounds.[1059] Furthermore, as explained above, the court expanded the application of the 'essential equivalence' standard to all mechanisms for

[1050] Art. 47 GDPR.
[1051] For a discussion, see Section 5.3.1.
[1052] Art. 49 GDPR.
[1053] EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018, p. 4ff.
[1054] *Ibid.*, at 4.
[1055] See Section 2.2.1.1.
[1056] See, e.g., The Guardian (2013).
[1057] 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, pp. 1, 6.
[1058] CJEU, *Schrems I*.
[1059] CJEU, *Schrems II*, paras 184-187.

systematic personal data transfers under the GDPR.[1060] The third and final change is that the last 25 years have seen an exponential growth of cross-border commerce powered by personal and other data.[1061] The importance of data flows for pan-European and global trade form an integral part of the EU's economic digital trade discourse advanced in parallel and, at times, contrary to the fundamental rights discourse.[1062] The ubiquitous character of data flows in digital commerce and online activities has further intensified global economic interdependence. It puts insurmountable pressure on the legal framework setting boundaries for the flows of personal data.

The changes introduced into the EU's framework for transfers of personal data in the GDPR, as compared to the Data Protection Directive, addressed some of the political, legal and economic changes identified above. Indeed, several recitals of the GDPR acknowledge the challenges for the data protection regime brought by technological developments and globalisation.[1063] In its 2017 Communication 'Exchanging and Protecting Personal Data in a Globalised World', the European Commission praised the GDPR for providing 'a diverse set of mechanisms that are flexible enough to adapt to a variety of different transfer situations', citing notably the SCCs, the codes of conduct and certification mechanisms.[1064] Indeed, as compared to the Data Protection Directive, the GDPR's transfer mechanisms are somewhat more flexible. For example, the GDPR allows for the adoption of an adequacy decision not only to a third country overall, but also to an international organisation, a territory or one or more specified sectors within that third country.[1065] In addition, the GDPR has explicitly codified the BCRs – which were applied in practice, but were merely implied in the text of the Directive – as one of the appropriate safeguards for transfers of personal data. The GDPR also added two new appropriate safeguards, namely certification and codes of conduct,[1066] which, at the time of writing, have not yet been operationalised. Finally, the specific derogations allowed under Article 49 of the GDPR were complemented by an open-ended, but extremely hard to comply with, safeguard allowing the transfer of personal data for the purposes of compelling legitimate interests of the data controller.

[1060] For a discussion, see Section 5.2.2.
[1061] See Introduction to this thesis.
[1062] See Section 3.3.2.
[1063] Recitals 5-7 GDPR.
[1064] Communication from the Commission to the European Parliament and the Council, *Exchanging and Protecting Personal Data in a Globalised World*, COM (2017) 7 final, 10 January 2017, p. 10.
[1065] Compare Art. 25(1) Data Protection Directive and Art. 45(1) GDPR. Note, however, that two adequacy decisions under the Directive (namely, Adequacy decision for Canada, EU-U.S. Safe Harbor), despite absence of a direct mentioning of the possibility to adopt and adequacy decision for a specific sector the text of the Data Protection Directive, were adopted solely for commercial sector transfers.
[1066] Article 46(2)(e) and (f) GDPR.

On a more critical note, more than four years after the adoption of the GDPR, few of these flexibilities have ever been used or operationalised. To wit: no adequacy decisions have been adopted for international organisations,[1067] territories or sectors of economy; only one adequacy decision for a third country (Japan) has been adopted under the GDPR; certification mechanisms and codes of conducts are not yet used as mechanisms for data transfers; and the SCCs for controller to controller and controller to processor transfers, adopted by the European Commission in 2004 and 2010 respectively, have not been updated to meet the GDPR standard and the demands of business.[1068] In practice, most of the systematic transfers of personal data outside the EEA still rely on the SCCs.[1069] This raises the question of whether the above-mentioned flexibilities are merely paying lip service to the EU's economic discourse on digital trade, as discussed in Chapter 3 of this thesis, rather than a genuine effort to reform the framework for transfers of personal data.

This Section argues that, although the framework did – on paper - become more flexible, these changes did not rectify the key structural issues inherent within it. Against the backdrop of the three developments mentioned at the beginning of this Section, the discussion below is centred around the *three principal deficiencies* of the EU's framework under Chapter V of the GDPR. First, although the CJEU's *Schrems II* judgement contributed to bridging the qualitative gap between adequacy decisions and private law mechanisms for systematic transfers of personal data, it did not eliminate the problem completely. Although it is too early to judge, this Section contemplates that *Schrems II* may instead lead to other problems, such as the fragmentation of standards for transfers of personal data across the EU due to: (a) the deficiencies of coordination between European DPAs; (b) limitations of enforcement resources of European DPAs and a resulting shift towards private enforcement; which will, in turn result in (c) a fragmentation of case law across the EU member states in the short and medium terms. It also argues that, overall, in the future the secondary EU framework for transfers of personal data may not be the right tool to address the surveillance issue in transfers of personal data outside the EEA. Second, in practice, the adequacy decisions themselves, including the most recent one for Japan adopted on the basis of the GDPR, suffer from a number of weaknesses which impair their

---

[1067] See Kuner (2020c).

[1068] At the time of writing, the European Commission is working on amending the SCCs to meet the GDPR standards and adapt to the CJEU *Schrems II* decision. See 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; 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.

[1069] 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.)

ability to ensure, in practice, continuity of personal data protection as required by their constitutional function. Third, there is a mismatch between the transformation of the role of personal data in cross-border commerce since 1995, when the core of the EU framework for transfers of personal data was designed, on the one hand, and the rigidity of this framework in the sense that it does not take into account the different degree of risks to fundamental rights inherent in transfers of personal data in different circumstances, on the other hand. The Section therefore contends that the rules of Chapter V of the GDPR lack scalability and are thus not fully adequate for the digital age. The discussion below elaborates on each of these arguments.

5.3.1 The foreign surveillance issue after Schrems II

The interpretation of 'adequacy' of personal data protection as 'essential equivalence' by the CJEU in *Schrems I* created a qualitative gap between the level of protection that, in theory, is given to personal data transferred on the basis of adequacy decisions, on the one hand, and the level of protection afforded to personal data transferred on the basis of so-called 'appropriate safeguards', on the other hand. The CJEU's conclusions and the ensuing guidance by the European DPAs,[1070] – as well as the above-mentioned qualitative gap – were later codified in the GDPR. As compared to Article 25(2) of the Data Protection Directive, the list of factors set forth in Article 45(2) of the GDPR (that the European Commission must consider when assessing the adequacy of the level of protection of personal data in a third country) has been sufficiently expanded. In particular, it requires the Commission to evaluate the access of public authorities to personal data, as well as the implementation of the foreign legislation to see whether it contains effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred.[1071] By strengthening the adequacy assessment, however, the GDPR inadvertently created a situation where the level of personal data protection achieved by all other mechanisms for data transfers (most importantly, appropriate safeguards under Article 46 GDPR, which on a par with adequacy, can underlie systematic transfers of personal data) became lower than that afforded (in theory) by an adequacy decision.

Adequacy decisions are adopted by implementing acts of the Commission after a thorough assessment of the third country's legal system and data protection framework. The adequacy decision for Japan, which is the most recent – and so far, the *only* adequacy decision adopted under the GDPR, – contains commitments by Japan in relation to personal

[1070] 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.
[1071] Art. 45(2)(a) GDPR.

data transferred from the EEA. These commitments are included in the 'Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU based on an Adequacy Decision', hereinafter referred to as the 'Supplementary Rules', which are legally binding for Japanese businesses.[1072] In contrast, the appropriate safeguards and specific derogations are merely private law mechanisms. An adequacy decision certifies (in theory) that a particular third country ensures a level of personal data protection 'essentially equivalent' to that in the EU.[1073] The 'level of personal data protection' means here not only the quality of the data protection rules, but multiple other factors, including the respect for the rule of law and human rights, access of public authorities to personal data, existence and effective functioning of independent supervisory authorities, existence of effective judicial review designed to ensure compliance with provisions of EU law.[1074] None of the other mechanisms for data transfers required – until the *Schrems II* judgement – such a thorough assessment. Most specifically, these mechanisms as described in the GDPR, did *not* seem to provide individuals with any safeguards against the access to their data by third country's public authorities. After the CJEU's invalidation of the Safe Harbor framework in *Schrems I* in 2015, Kuner rightly noted that:

> [t]he conclusions of the CJEU in *Schrems* have thus undermined the logical consistency of using adequate safeguards to transfer personal data. The European Commission and the DPAs have allowed standard contractual clauses and BCRs to be used for years although it has been clear that they cannot provide effective protection against intelligence surveillance, suggesting that until now they have implicitly factored the possibility of such surveillance into the definition of "adequate safeguards." The strict standard for data protection rights applied by the CJEU in *Schrems* judgments raises the question of whether this is compatible with EU fundamental rights law.[1075]

It is precisely this deficiency of private law mechanisms for transfers of personal data that led to a challenge of the validity of the European Commission's Decision approving the SCCs, along with the EU-US Privacy Shield, in the light of the EU Charter, which resulted in the CJEU's 2020 *Schrems II* judgement.[1076] In particular, in the judgement of

[1072] Annex 1 to Adequacy decision for Japan.
[1073] CJEU, *Schrems I*, para. 73.
[1074] Art. 45 GDPR; CJEU, *Schrems I*, paras. 91-96; Article 29 Working Party, Working document on Adequacy Referential, WP 254rev.01, 6 February 2018, Chapter 4.
[1075] Kuner (2017), pp. 907-908.
[1076] CJEU, *Schrems II*, referred to the CJEU by Irish High Court (Commercial), *The Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems* 2016 No. 4809 P., 3 October 2017.

the Irish High Court referring the case to the CJEU, Justice Costello argued that neither the 'Privacy Shield' nor the SCCs are sufficient to protect the fundamental rights that apply to personal data in the EU Charter. In particular, they limit the right to an effective remedy before an independent tribunal guaranteed by Article 47 of the EU Charter beyond the limits set by Article 52(1) of the EU Charter.[1077] Justice Costello also noted that '[i]f there are inadequacies in the laws [of the foreign country] within the meaning of Union law, the SCCs cannot and do not remedy or compensate for these inadequacies'.[1078]

As has already been mentioned above, in *Schrems II*, the CJEU reinstated the logical consistency of the EU framework for data transfers.[1079] Despite running the risk of being repetitive, for the purposes of discussion below it is important to summarise *all* the CJEU's conclusions in relation to the validity of the SCCs and, indirectly, all other appropriate safeguards under Article 46 of the GDPR:

1. The requirement of 'essential equivalence' equally applies to all mechanisms for systematic transfers of personal data under the GDPR, including appropriate safeguards under Article 46 GDPR, also in the context of access to personal data by foreign authorities in a national surveillance context;[1080]
2. 'Essential equivalence' of the level of protection in third countries that have been afforded an adequacy decision is presumed;[1081]
3. The SCCs 'are solely intended to provide contractual guarantees … independently of the level of protection guaranteed in each third country',[1082] and are valid;[1083]
4. Prior to using the SCCs and other appropriate safeguards for third countries that have not been granted an adequacy decision, the data exporter must conduct a comprehensive assessment, in particular, on the basis of factors 'set out, in a non-

---

[1077] Irish High Court (Commercial), *The Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems* 2016 No. 4809 P., 3 October 2017, para. 334, stating that

> the limitations on the exercise of the right to an effective remedy before an independent tribunal, as required by Article 47 [of the EU Charter], for EU citizens whose data privacy rights are infringed by the intelligence agencies are not proportionate or necessary or needed to protect the rights and freedoms of others. Neither the introduction of the Privacy Shield Ombudsperson mechanism nor the provisions of Article 4 of the SCC decisions eliminate the well-founded concerns raised by the [Irish Data Protection Commissioner] in relation to the adequacy of the protection afforded to EU data subjects whose personal data is wrongfully interfered with by the intelligence services of the United States once their personal data has been transferred for processing to the United States.

[1078] CJEU, *Schrems II*, para. 154.
[1079] Kuner (2020d).
[1080] CJEU, *Schrems II*, para 96, 105; see also Opinion AG in *Schrems II*, para. 117. See also 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, questions 6 and 7.
[1081] CJEU, *Schrems II*, para. 118.
[1082] *Ibid*., para. 133.
[1083] *Ibid*., paras. 136, 147. See also Opinion AG in *Schrems II*, para.126.

exhaustive manner, in Article 45(2) [GDPR]' of whether those safeguards can, *in practice*, ensure essentially equivalent protection of personal data[1084] (so-called 'mini-adequacy' assessments[1085]);

5. If, based on the assessment above, the data exporter concludes that an 'essentially equivalent' level of data protection cannot be ensured by appropriate safeguards, the data exporter must implement what the CJEU calls 'additional safeguards' or 'supplementary measures', which should be determined on a case-by-case basis;[1086]
6. If the data exporter established in the EU is not able to take 'additional measures' to guarantee 'essentially equivalent' protection of personal data, the data exporter must suspend or end the transfer; this is, in particular, the case where the law of the third country imposes obligations on the recipient of personal data, which are contrary to the SCCs;[1087]
7. The DPAs must proactively monitor transfers of personal data under appropriate safeguards and suspend or prohibit data transfers that do not meet the requirement of 'essential equivalence';[1088] and
8. To prevent the fragmentation of rules, which could result from different EU member states' DPAs arriving at different conclusions regarding lawfulness of transfers, the DPAs must work together through coordination mechanisms under the GDPR.[1089]

On the face of it, the CJEU closed the qualitative gap between adequacy decisions and appropriate safeguards under Article 46 GDPR, while preserving the lawfulness of the most commonly used mechanism for data transfers in the absence of an adequacy decision.[1090] The way the CJEU answered the questions referred to it in *Schrems II* is, indeed, perhaps, the only logical way the Court could restore the consistency of the EU secondary law framework for transfers of personal data[1091] and assert the importance of fundamental rights vis-à-vis the economic interests embedded in data transfers, on the one hand, and without upsetting the delicate institutional balance in the EU, on the other hand. If the CJEU invalidated the SCCs as a mechanism for transfers of personal data, this would undermine the validity of all other private law mechanisms in the GDPR. Not only the BCRs but also the certification mechanisms and codes of conduct added into the GDPR,

[1084] *Ibid*., para. 105.
[1085] Kuner (2020d).
[1086] CJEU, *Schrems II*, paras. 131-134, 137, 142.
[1087] *Ibid*., para. 135.
[1088] *Ibid*., paras. 108, 121.
[1089] *Ibid*., para. 147.
[1090] 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.)
[1091] See Kuner (2020d); Christakis (2020).

which the European Commission frequently emphasises as bringing extra flexibility to the modernised 'toolbox' for data transfers.[1092] Such a state of affairs would also undermine the system of cross-border transfers in the GDPR as a whole.[1093] Thus, this approach would create – *de jure* – data localisation in respect of all countries, short of 12 afforded adequacy decisions, which would be contrary to the EU's external digital trade policy and digital trade discourse (discussed in Chapters 3 and 4 above). Specific derogations under Article 49 GDPR, which were not considered in *Schrems II*, can only be used for occasional and non-repetitive transfers.[1094] Neither could the CJEU invalidate the model SCCs approved by the European Commission: as the CJEU demonstrated itself, they do provide the safeguards required under Article 45(2) of the GDPR, provided that a third country's legal framework does not interfere with their application.[1095]

The CJEU also did not use the window of opportunity – opened by the Advocate General's opinion – to modify its position in *Schrems I* and apply a lower threshold for situations where foreign authorities' access transferred personal data for national security purposes, thus amplifying the tension between the CJEU's approach to national security measures interfering with fundamental rights abroad and in the EU member states.[1096] In particular, the Advocate General had noted that:

> 'essential equivalence' test should therefore … be applied in such a way as to preserve a certain flexibility in order to take the various legal and cultural traditions into account. That test implies, however, if it is not to be deprived of its substance, that certain minimum safeguards and general requirements for the protection of fundamental rights that follow from the Charter and the ECHR have an equivalent in the legal order of the third country of destination.[1097]

Thus, the Advocate General had argued that both the standards of the Charter and the ECHR are the relevant comparators for the assessment of the foreign legal framework. He had also observed that 'the standards resulting from Articles 7, 8 and 47 of the Charter, as interpreted by [the CJEU], are in certain respects stricter than those arising under Article 8 of the ECHR according to the interpretation of those provisions by the European Court of

---

[1092] See Communication from the Commission, *Exchanging and Protecting Personal Data in a Globalised World*, COM (2017) 7 final, 10 January 201; Communication from the Commission to the European Parliament and the Council, *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.
[1093] For a discussion of this scenario, see Swire (2016), pp. 1-33 – 1-36.
[1094] EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018.
[1095] CJEU, *Schrems II*, paras. 126-148.
[1096] See Section 2.2.2.
[1097] Opinion AG in *Schrems II*, para. 249.

Human Rights ("the ECtHR")."[1098] The ECtHR may, however, reconsider its approache in several pending cases.[1099]

In practice, the CJEU pushed the foreign surveillance problem in the context of personal data transfers further down the line. As argued in Chapter 2, the *Schrems II* has restricted the possibility of using the SCCs in practice, especially in the light of some of the DPAs recommending European companies to localise data where possible.[1100] Furthermore, and most importantly, it is questionable whether the *Schrems II* approach will allow a bridge to be built between the qualitative gap between the adequacy assessments and appropriate safeguards under Article 46 for several reasons. It is unclear whether companies are in the right position to conduct assessments of the third country's legal regime similar to adequacy assessments, which the European Commission typically conducts for several years and which, even then, do not always result in bullet-proof adequacy decisions as this Section illuminates below. Many companies, especially small and medium enterprises, will have neither the resources nor the expertise to conduct comprehensive research into third countries' legal frameworks. Companies that could have both the resources and expertise to do so, do not seem to have complied with the *Schrems II* requirements in a timely manner.[1101] Even more importantly, the CJEU's approach gives companies – the very actors which 'encroach upon the private sphere' – a crucial role in setting the boundaries for data transfers and resulting interference with fundamental rights.[1102] While companies are driven by their bottom-lines, it is the role of governments and European institutions to ensure that fundamental rights are protected. It is also questionable whether the lack of 'essential equivalence' can be remedied by additional guarantees that companies must implement in order to continue data transfers. Thus, on the one hand, it is clear, that many countries in the world do not meet the 'essential equivalence' standard as formulated by the CJEU. On the other hand, it is similarly clear that additional private law guarantees cannot remedy those deficiencies. In the present-day interconnected world, data flows will not simply stop and in practice (in the view of low risk of enforcement by DPAs), many companies are likely to continue with 'business as usual'. As a result, the level of compliance and the quality of assessment are unlikely to be satisfactory.

[1098] *Ibid*., para. 251.
[1099] *Ibid*., para. 252.
[1100] See Section 2.2.2.
[1101] As of October 2020, big companies like Microsoft, have not adjusted their practices to comply with *Schrems II*. See, e.g., Unabhängibes Datenschutz Zentrum Saarnald, Pressemitteilung: Microsoft Office 365: Bewertung der Datenschutz-Konferenz zu undifferenziert – Nachbesserungen gleichwohl geboten, 02 October 2020.
[1102] For a discussion on why giving companies too much power in setting the boundaries for data processing could be a problem, see Quelle (2017a).

Furthermore, it is questionable whether the DPAs themselves are well situated to assess the adequacy of legal frameworks in third countries and monitor compliance with the new rules, given the pervasiveness of data flows and the lack of financial and human resources.[1103] The reluctance of the Irish DPA to take a firm action against Facebook's transfers to the US back in 2013, which resulted in *Schrems I* and *II* in the first place, and its reluctance to actively enforce the *Schrems II* judgement,[1104] is telling. Thus, although in *Schrems II* the CJEU restored the coherence of the framework for transfers of personal data, it did not close the gap between the 'reality and illusion' of personal data protection in the context of data transfers.[1105]

While it has put the DPAs at centre stage for ensuring the lawfulness of transfers, the CJEU has explicitly dismissed the risk of divergent decisions by the EU DPAs to suspend or prohibit transfers by referring to coordination mechanisms within the EDPB under the GDPR.[1106] This coordination mechanism, however, has not been effective until now, in part due to differences in administrative procedures in EU member states.[1107] While DPAs and the EDPB are crafting guidelines on additional safeguards that companies can implement to ensure the SCCs guarantee 'essentially equivalent' protection in practice, private lawsuits, including mass claims, may well take over as the primary mode of enforcement. The relatively new possibilities for mass damages claims under Articles 80 and 82 of the GDPR and EU member states' laws are becoming increasingly attractive for NGOs and professional litigation funders.[1108] The GDPR provisions allow a not-for-profit body, organisation or association that has been mandated by an individual – in some EU member states, this mandate is not needed – and meets certain requirements, to exercise individual rights to judicial remedy, including an ability to claim compensation.[1109] In response to the inaction of Irish and other DPAs following the *Schrems II* judgement, noyb, the NGO run by Max Schrems, has recently filed 101 complaints to various European

[1103] According to the EDPB's survey, as of 2019, more than 50% of EU member states DPAs have less than 60 FTE and budget below EUR 4,5 million. EDPB, Contribution of the EDPB to the evaluation of the GDPR under Article 97, Adopted on 18 February 2020, pp. 26-30. See also BEUC (2020).
[1104] Noyb (2020b).
[1105] Kuner (2017), discussing the 'reality and illusion' in EU personal data transfer regulation post *Schrems I*.
[1106] CJEU, *Schrems II*, para. 147.
[1107] See EDPB, Contribution of the EDPB to the evaluation of the GDPR under Article 97, Adopted on 18 February 2020, p. 3; 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. 5 (noting that 'developing a truly common European data protection culture between data protection authorities is still an on-going process. Data protection authorities have not yet made full use of the tools the GDPR provides, such as joint operations that could lead to joint investigations'.)
[1108] See, e.g., Manancourt (2020). See also The Privacy Collective (2020), para. 4.6.5 (in Dutch).
[1109] For an overview of collective damage compensation systems for data protection violations in different EU member states, see Pato (2019a); Pato (2019b), p. 98ff.

DPAs.[1110] Noyb also stated that it 'is planning to gradually increase the pressure on EU and US companies to review their data transfer arrangements and adapt to the clear ruling by the [CJEU]',[1111] hinting at the imminence of private enforcement. Sooner or later, domestic courts will need to evaluate whether transfers to certain jurisdictions with the use of the SCCs meet the *Schrems II* requirements and which additional measures are appropriate in specific circumstances. This may, as alluded to above, result in a fragmentation of the case law throughout the EU in the short and medium term, and in more references to the CJEU in the long term.

Despite this critique, it is undeniable that the *Schrems II* judgement marks an important milestone in asserting the fundamental rights to privacy and the protection of personal data in the context of digital trade. The fact that the CJEU put the burden on private companies and the DPAs, should be taken as an intermediary solution: the lesser of two evils, the other being the prohibition of systematic data transfers on the basis of appropriate safeguards. It is a wake-up call to the EU and its trading partners to start a dialogue on the interplay between digital trade, fundamental rights and national security. The core issue raised in *Schrems I* and *II* cannot be fully addressed by businesses, DPAs or even the EU secondary rules, such as the GDPR or the adequacy decisions.[1112] As rightly noted by several commentators in relation to the invalidation of the EU-US Privacy Shield and the standards the EU Charter requires from foreign legal frameworks, 'any hope of a stable and viable accommodation for data transfers between the EU and the US can only be based on changes to US law'.[1113] This is also true for other third countries: as discussed in the following Section, few of the existing adequacy decisions can meet the high threshold of essential equivalence set by the CJEU in *Schrems I* and confirmed in *Schrems II* judgements.

In a global – or, at a minimum, multilateral setting – reconciling the policy objectives of digital trade, national security and fundamental rights is an intricate political challenge. As Farrell and Newman demonstrate, global economic interdependence and seamless data flows have been 'weaponised' by surveillance authorities that leveraged global networks for surveillance purposes (authors call this phenomenon 'weaponized interdependence').[1114] *Schrems II*, they argue, is an opportunity to address this changed relationship between national security and civil liberties by democratic states, and primarily by the US and the EU.[1115] Arguably, putting the burden on companies to assess

[1110] Noyb (2020a).
[1111] *Ibid.*
[1112] For example, Reidenberg noted that Safe Harbor 'offered a mechanism to delay facing tough decisions about international privacy'. Reidenberg (2001), p. 739.
[1113] Kuner (2020b); Kuner (2020d); Propp, Swire (2020a); Churches, Zalnieriute (2020), pp. 7-8.
[1114] Farrell, Newman (2020b).
[1115] Farrell, Newman (2020a).

essential equivalence of third countries' legal frameworks and hoping for companies operating in legal regimes with insufficient privacy protection to push their governments to change this regime – a bottom-up change – has not worked in the past and, if the past is prologue, will not work in the future. Addressing the issue at the international level is much more in line with the EU's ambition to 'promote convergence of data protection standards at international level, as a way to facilitate data flows and thus trade'.[1116]

What the optimal forum for addressing this issue should be is a broader question, one which is outside the scope of this thesis. At this stage, one could, however, argue that this dialogue should *not* be part of international trade negotiations.[1117] As noted several times throughout this thesis, privacy and data protection as well as national security interests are built into the international trading system as exceptions. The economic ethos of the international trading system, as argued in Chapter 3, could lead to a lower level of fundamental rights protection. Furthermore, this would be against the current EU approach to digital trade negotiations discussed in Chapter 4.

5.3.2 Inadequacies of adequacy decisions

This Section argues that, although – based on the criteria for assessment in Article 45(2) of the GDPR – adequacy decisions, in theory, must ensure an essentially equivalent level of protection, in practice this mechanism for data transfers not only suffers from political pressures, which result in assessment less rigorous than required by Article 52(1) of the EU Charter, but also from the problems inherent in any domestic legal instrument with extraterritorial reach, namely, the 'snapshot', the 'heavy burden' and the 'onward transfer' problems. As a result, as Kuner argues, 'while adequacy purports to provide a strong level of protection for personal data, such protection is actually difficult to enforce outside the borders of the EU.'[1118] The flaws of adequacy decisions discussed in this Section suggest that the adequacy framework does not fully prevent, in practice, the circumvention of the EU data protection framework when personal data leaves the EEA borders and does not fulfil the function of securing 'effective and complete' protection of the fundamental rights to the protection of privacy and personal data in the EU.

5.3.2.1 Adequacy decisions: between protection of fundamental rights and trade politics

Despite being the primary mechanism for transfers of personal data outside the EEA in the layered structure of the EU legal framework, the adequacy assessments mechanism

---

[1116] 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.
[1117] Cf Irion (2020a). But see Reidenberg (2001), pp. 739, 748 proposing to negotiate a 'General Agreement on Information Privacy' at the WTO.
[1118] Kuner (2009), pp. 8-9.

lacks a clear procedure and is extremely slow. From 1995 when the adequacy mechanism was first introduced, the EU has granted adequacy only 14 times. EU Commission's adequacy decisions were challenged twice at the CJEU, both times for the US, and both challenges resulted in the invalidation of the decisions.[1119] It takes on average several years to obtain adequacy.[1120]

The adequacy mechanism is a powerful negotiation tool between the EU and its trading partners.[1121] For example, in its 2017 Communication, the European Commission stated that it will 'actively engage with key trading partners in East and South-East Asia', starting with Japan and Korea in 2017 and, depending on progress towards the modernisation of its data protection laws, with India, but also with countries in Latin America (in particular Mercosur members), and countries in the 'the European neighbourhood' that have expressed an interest in obtaining an 'adequacy finding'.[1122] Several leading scholars have argued that adequacy decisions are not strict legal assessments.[1123] For example, Schwartz contends that in evaluating adequacy 'the EU has demonstrated a wide range of flexible approaches with regard to this standard.'[1124] Although under the GDPR, adequacy is a unilateral assessment, the EU negotiators have not 'exercised unilateral power', but rather 'flexibly assessed the adequacy of different legal systems as it suits the EU's goals at the time'.[1125] Similarly, Kuner argues that 'adequacy decisions are far from always being objective and logical, and do not provide a watertight standard of data protection',[1126] and that '[i]n practice, it can be difficult for a State or regional organization to pass judgment on a foreign regulatory system without political considerations playing some role'.[1127] He illustrates his point by referring to the adequacy decision for Argentina, where serious human rights abuses were flagged by Amnesty International right after that decision was granted.[1128] The assessment of Argentina's adequacy by Article 29 Working Party was conducted 'on the basis of … assumptions and explanations and in the absence of any substantial experience with the practical application of the legislation, both at federal or provincial level.'[1129] In a similar

[1119] CJEU, *Schrems I* invalidated the EU-US Safe Harbor and CJEU, *Schrems II* invalidated the EU-US Privacy Shield.
[1120] Most recent example is Adequacy Decision for Japan.
[1121] Schwartz (2019), p. 807.
[1122] Communication from the Commission to the European Parliament and the Council, *Exchanging and Protecting Personal Data in a Globalised World*, COM (2017) 7 final, 10 January 2017, P. 8,
[1123] For a discussion, see Yakovleva, Irion (2016), p. 205.
[1124] Schwartz (2019), p. 806.
[1125] *Ibid*., p. 806-807.
[1126] Kuner (2009), p. 8-9.
[1127] Kuner (2013), p. 66.
[1128] Kuner (2009), p. 8-9. See also Roth (2017), pp. 61-62; Wolf (2014), pp. 242-243.
[1129] Article 29 Working Party, Opinion 4/2002 on the level of protection of personal data in Argentina, WP 63, 3 October 2002, p. 17.

vein, one of the factors that played a role in the assessment and finding of adequacy of New Zealand was the volume of EU's trade with this country.[1130] Concerns regarding the absence of onward transfer restrictions in New Zealand law was addressed by simply pointing out the remote geographical location of the country and low likelihood of such transfers.[1131] The adequacy decision for Israel, despite Israeli intelligence agency practices, is yet another example of a political compromise in the assessment of adequacy.[1132]

The recently invalidated EU-US Privacy Shield (which superseded the EU-US Safe Harbor, invalidated by the CJEU in 2015), was hastily negotiated and concluded in record time: 8 months as opposed to the 'lengthy and troubled negotiations of the Safe Harbor'[1133] and other adequacy decisions.[1134] Political pressure from the US government and powerful transatlantic business stakeholders not only explains the faster pace of the negotiations, but also the fact that this adequacy decision for the US was adopted despite reservations from the Article 29 Working Party (the EDPB's predecessor), the European Parliament and the EDPS.[1135] It therefore comes as no great surprise that just like its predecessor, the Privacy Shield did not survive CJEU scrutiny.[1136]

The adequacy decision for Japan is the most recent example of the same phenomenon. As mentioned in Chapter 4, trade negotiations with Japan played a significant role in granting Japan an adequacy decision, which indeed coincided with the conclusion of the bilateral trade agreement. Japan's adequacy decision contains (besides the Commission's assessment of Japan's regulatory framework) additional rules that Japan agreed to implement specifically in relation to personal data transferred from the EEA, thus creating a double standard for personal data protection within the country.[1137] As rightly mentioned by France in its submission for the 2020 review of the GDPR, the purpose of the adequacy decision is the assessment of an existing framework, not the creation of an

---

[1130] Bygrave (2014), p. 194 referring to Article 29 Working Party, Opinion 11/2011 on the level of protection of personal data in New Zealand, WP 182, 4 April 2011.
[1131] Roth (2017), pp. 60-61.
[1132] Kuner (2013), p. 66.
[1133] House Hearing. (2001), p. 72.
[1134] The EU-US Safe Harbor was invalidated in October 2015, the EU-US Privacy Shield was adopted on 12 July 2016.
[1135] European Parliament Resolution of 26 May 2016 on transatlantic data flows (2016/2727(RSP)); EDPS, Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision, 30 May 2016; Article 29 Working Party, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, WP 238, 13 April 2016.
[1136] Farrell, Newman (2020a) (arguing that 'no one—including the European Union officials who negotiated it—ever thought that the Privacy Shield agreement that succeeded Safe Harbor had much chance of surviving CJEU scrutiny'.) See also Christakis (2020); Kuner (2020d).
[1137] Annex 1 to Adequacy decision for Japan. In its comments to the EU Council on the evaluation of the GDPR France calls this approach an 'ingenious solution,' which, nonetheless, 'should not be considered as a precedent for future adequacy decisions'. Preparation of the Council position on the evaluation and review of the General Data Protection Regulation (GDPR): Comments from Member States, 12756/1/19 REV 1, submission of France, p. 24.

additional layer of rules specifically for the EEA data to rectify gaps in a foreign country's legal system.[1138] Thus, by adding Supplementary Rules to the adequacy decision, the European Commission has, in effect, re-designed the adequacy framework under the GDPR. Furthermore, the adequacy decision for Japan was adopted despite the concerns of the EDPB and the European Parliament regarding, in particular, the compliance of the surveillance measures employed by the Japanese government with the adequacy standard established by the CJEU in *Schrems I*, and relatively mild enforcement mechanisms (compared to those under GDPR) under Japanese law.[1139] Although the 2020 reform of Japan's Act on the Protection of Personal Information brought it closer to the GDPR, it did not alter the provisions on administrative fines.[1140] Not surprisingly, Greenleaf criticised the adequacy decision for Japan, which, in his words, 'discounts' the EU law's adequacy standard on several grounds, most importantly in that (a) the Japanese enforcement regime is not 'essentially equivalent' to that of the EU; (b) consent cannot be a sufficient ground for onward transfers (this issue is further discussed in Section 5.3.2.2 below); and (c) there was a lack of expert involvement in the assessment of the Japanese legal system.[1141]

The adequacy decision mechanism has been, and continues to be, a powerful tool for the EU to export its data protection standards and seek further convergence of other countries' data protection rules on the basis of the EU standards (the above-mentioned 'Brussels Effect'[1142]). The political component, however, has an impact on the robustness of the adequacy decisions to safeguard an 'essentially equivalent' level of protection of personal data transferred outside the EEA. Although none of the adequacy decisions (except those for the US) have yet been challenged at the CJEU, it is questionable whether most of them – given that 10 out of 11 adequacy decisions in force were granted before the 2015 *Schrems I* judgement – would stand the 'essential equivalence' test articulated by the CJEU in *Schrems I* and recently confirmed in *Schrems II* in respect to the access of foreign surveillance authorities to transferred data, and right to effective judicial remedy.[1143] This problem of staticity of adequacy assessments and other limitations of the adequacy framework are discussed below.

[1138] Preparation of the Council position on the evaluation and review of the General Data Protection Regulation (GDPR): Comments from Member States, 12756/1/19 REV 1, submission of France, p. 24.
[1139] EDPB, Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan, 5 December 2018, paras 122, 128, 137ff; European Parliament resolution of 13 December 2018 on the adequacy of the protection of personal data afforded by Japan (2018/2979(RSP), paras 21-25. See also Miadzvetskaya (2019).
[1140] For an overview of amendments, see One Trust Data Guidance (2020b).
[1141] Greenleaf (2018b); see also Greenleaf (2018c), pp. 4-8; Greenleaf (2017b).
[1142] Bradford (2012).
[1143] See Christakis (2020).

5.3.2.2 Limitations of adequacy decisions inherent in legal instruments with extraterritorial application

This Section argues that, as domestic legal instruments with extraterritorial reach,[1144] adequacy decisions suffer from at least three weaknesses. First, they embody an assessment of a third country's legal framework at a particular point in time and do not provide effective dynamic mechanisms for ensuring that the third country will maintain the same level of personal data protection throughout the life of the adequacy decision (the 'snapshot' problem). Second, if a foreign data controller or processor violates the third country's data protection rules when processing a European's personal data, enforcement of such rights abroad is burdensome (the 'heavy burden' problem). Third, adequacy decisions, at best, guarantee that personal data transferred from the EEA are equally protected in the *first country of destination* — the one granted an adequacy decision — but often fail to provide the same level of protection in relation to *onward transfers* of such data to other countries (the 'onward transfer' problem).

On the first point (*the 'snapshot' problem*), as mentioned above an adequacy decision for a third country (international organisation, territory or sector of industry[1145]) is the result of an assessment of that country's system based on a snapshot of rules at a particular point in time. The GDPR requires that the adequacy decision should provide for a periodic review, at least every four years.[1146] In a fast-paced globalised present-day environment, review of the legal framework once in four years is simply not frequent enough. In addition, the GDPR requires the Commission to monitor developments in third countries and international organisations that could affect the functioning of the adequacy decisions and may, to the extent necessary, repeal, amend or suspend such adequacy decisions.[1147] Although the Data Protection Directive did not contain specific rules on the monitoring and review of adequacy decisions, similar requirements were initially included in the text of adequacy decisions themselves.[1148] These requirements were later expanded to include the monitoring of the developments on foreign authorities' access to personal data in the aftermath of the CJEU *Schrems I* judgement.[1149] There is, however, no information on whether and how, if at all, the Commission actually conducts the monitoring of legal regimes in third countries that have been afforded adequacy. Furthermore, none of the adequacy decisions – except for the invalidated EU-US Privacy Shield, which was the only

[1144] Kuner (2015b), pp. 236, 239 (arguing that although the EU rules for transfers of personal data is not 'extraterritorial in scope within a literal meaning of the term, they do have extraterritorial effect'.)
[1145] For simplicity, this section refers to country only, but implies organisation, territory, and sector of industry.
[1146] Art. 45(3) GDPR.
[1147] Art. 45(4) and (5) GDPR.
[1148] See, e.g., Art. 4 of Adequacy decision for Canada; Art. 4 Adequacy decision for Uruguay.
[1149] European Commission, Implementing Decisions amending Adequacy Decisions after *Schrems I*.

adequacy mechanism reviewed on an annual basis[1150] – have ever been reviewed. Of the 11 adequacy decisions adopted prior to the GDPR, which are currently in force, some have been in force for nearly 20 years (for example, adequacy for Switzerland adopted in 2000, for Canada, in 2001). Neither the 2013 Snowden revelations, followed by European Parliament reports and calls on the Commission to review adequacy decisions for New Zealand and Canada because of these countries participation in the 'Five Eyes' programme, nor the 2015 *Schrems I* judgement, triggered a review of such adequacy decisions by the Commission.[1151] Similarly, the Commission did not take action to remedy the deficiencies of the Safe-Harbor, despite having identified its weaknesses in its 2013 Communications, preceding the Safe Harbor's invalidation by the CJEU in *Schrems I*.[1152] What is more, already back in 2001, just one year after the Safe Harbor framework came into being, a leading US academic proclaimed Safe Harbor 'only a weak, seriously flawed solution for e-commerce'.[1153]

The European Commission announced the first review of all adequacy decisions in 2017.[1154] This review is still ongoing at the time of writing. The publication of the report on the review of adequacy decisions was postponed until after *Schrems II*. The Commission has, however, already indicated that it is discussing 'additional safeguards' with some of the countries and territories 'to address relevant differences in protection'.[1155] It remains to be seen whether this review will result in qualitative improvements of the adequacy decisions.

[1150] The third annual review was completed in October 2019. See Report From the Commission to the European Parliament and the Council *on the Third Annual Review of the Functioning of the EU-U.S. Privacy Shield*, COM(2019) 495 final, 18 October 2017.

[1151] See Committee on Civil Liberties, Justice and Home Affairs, *Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*. No 2013/2188(INI), 21 February 2014; European Parliament Resolution of 12 March 2014 *on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs* 2013/2188(INI)). For a discussion see Roth (2017), p. 64. In the aftermath of *Schrems I* the European Commission amended adequacy decisions in force at that time to include provisions regarding the monitoring of developments in third countries regarding government agencies' access to personal data, the communication between the European Commission and EU member states, and between the European Commission and third countries on the issue. European Commission, Implementing Decisions amending Adequacy Decisions after *Schrems I*.

[1152] See Communication from the European Commission to the European Parliament and the Council, Rebuilding Trust in EU-US Data Flows, COM(2013) 846 final, 27 November 2013, paras. 2 and 3.2; Communication from the European Commission to the European Parliament and the Council *on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*, COM(2013) 847 final, 27 November 2013, paras. 3-5,7-8.

[1153] Reidenberg (2001), p. 719.

[1154] International Association of Privacy Professionals. (2017). See also EDPB, Agenda of the 40th EDPB meeting, 20 October 2020, suggesting that the Adequacy decision for Japan is also being reviewed.

[1155] Communication from the Commission to the European Parliament and the Council, *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.

One way or the other, at this juncture it seems clear that adequacy decisions do not fully factor in developments in the third countries' legal systems, and practice of application after adequacy has been granted. Besides, the EU has little or no control over the way personal data transferred from the EEA is processed abroad. One of the reasons why the review of adequacy decisions has not been an effective mechanism, is that, as discussed above, granting and maintaining an adequacy decision is not purely a legal matter, but largely a political act, especially when the EU's trade interests are at stake. Another reason is the design of the adequacy decision as a unilateral assessment by the EU. To constantly monitor developments in all countries that have been granted adequacy, especially in relation to the practice of application of the legal framework governing the processing of personal data, would require a substantial investment and granular expertise from the European Commission. In turn, third countries do not have any notification obligations regarding the changes of rules or practices related to personal data protection and national security programs, which makes the discovery of such changes burdensome for the EU. Even at the stage of negotiations, as the practice of negotiating the adequacy decision with Japan has shown, the Commission may not commission independent expert opinions on the third country's legal system and instead relies solely on the statements of the foreign government.[1156]

On the second point (*the 'heavy burden' problem*), seeking judicial or administrative redress abroad under the rules of a foreign legal system may incur prohibitive costs for individuals.[1157] This is even assuming that the level of personal data protection guaranteed in a third country, including the level of administrative fines, does comply with the standard of 'essential equivalence'. In the case of Japan, which as discussed above, has created a higher level of protection of personal data from the EEA as compared to Japanese citizens' data, enforcement of those higher protections may also be more difficult as there will be scarce domestic practice on which Supplementary rules (applicable only to personal data transferred from the EEA) can be grounded. Similarly, even when the GDPR applies to the processing of personal data abroad (e.g. under Article 3(2) GDPR)[1158] and grants EU member state courts jurisdiction over the issue – for example, in relation to damage compensation under article 79(2) GDPR – the costs of enforcing such a decision against a foreign controller in a third country are likely to be much higher than the amount of damages the individual may obtain. In addition, the harm caused to individuals as a result of violation of their fundamental rights cannot be fully undone. Lack of enforceability

[1156] Greenleaf (2018b), p. 9.
[1157] Kuner (2009), pp. 8-9.
[1158] As discussed in Section 2.2.1.2, the question on the relationship between Chapter V GDPR rules on transfers of personal data and extraterritorial application of the GDPR under Art. 3(2) GDPR remains an open question.

however, significantly reduces the effectiveness of data protection rules, as Section 5.3.3 below discusses in more detail.

On the third point (*the 'onward transfer' problem*), assessment of the rules for onward transfers of personal data from country A (which is undergoing the adequacy assessment) to country B (which does not have adequacy) is one of the factors in the adequacy assessment under Article 45(2)(a) of the GDPR. This means that, in order to preserve continuity of personal data protection and prevent circumvention of the EU data protection framework, the mechanism for transfers of personal data under country A's legal framework should be 'essentially equivalent' to that of the EU. Although most countries' legislation provides for some form of restrictions on international transfers of personal data, those restrictions are typically milder than those under the GDPR.[1159] Onward transfer mechanisms in existing adequacy decisions adopted by the Commission, which aim to compensate for the absence of restrictions on transfers of personal data from countries granted adequacy, provide for a lower level of protection to personal data transferred from country A (that has been granted adequacy) to countries B, C, and D (that have not been granted adequacy) than the level of protection that would have been granted to this data if it was transferred to countries B, C, and D directly from the EEA. In other words, onward transfer mechanisms under the adequacy decision could allow circumvention of the EU's high level of personal data protection and restrictions on transfers of personal data to third countries that have not been granted adequacy. Another challenge in this context is that the rules for onward transfers of personal data included in the adequacy decisions only apply to data obtained from the EEA and not to any other data processed in country A. Different legal regimes applicable to different data sets within the same country make monitoring of compliance difficult and therefore diminish the effectiveness of restrictions on onward transfers. This makes rules on onward transfers under adequacy decisions the Achilles' heel of the adequacy mechanism. Furthermore, and relatedly, just as there is no effective mechanism to monitor the rules in countries afforded adequacy, the EU framework does not have any monitoring mechanisms for the onward transfer rules.[1160]

To illustrate the point, the discussion below looks at specific provisions on onward transfer mechanisms under the adequacy decisions for Canada and Japan. There are two

---

[1159] Greenleaf (2017a). For an overview of restrictions see Ferracane (2017), pp. 10-27.

[1160] The same argument was made by France in its submission to the Council of the European Union. Preparation of the Council position on the evaluation and review of the General Data Protection Regulation (GDPR): Comments from Member States, 12756/1/19 REV 1, submission of France, p. 24 ('the existence of a precise and effective mechanism for monitoring these rules, in particular in regard to subsequent transfers of the European data transmitted, must be a sine qua non for the adoption of an adequacy decision, and must be regularly assessed by the European authorities'.) The importance of such monitoring is also highlighted by the EDPB. EDPB, Contribution of the EDPB to the evaluation of the GDPR under Article 97, Adopted on 18 February 2020, p. 6.

reasons for selecting these specific adequacy decisions. First, these countries are important trading partners of the EU, with which the EU has recently concluded a trade agreement.[1161] Second, Japan's decision is the most recent adequacy decision adopted by the EU and the only one so far adopted under the GDPR. In other words, it is the most up-to-date adequacy decision. In contrast, the adequacy decision for Canada is one of the oldest, adopted in 2001. Bringing both of them into analysis demonstrates the evolution in adequacy decisions over the last 20 years.

Onward transfers of personal data from Japan to third countries are regulated in the 'Supplementary Rules' included in Annex 1 of the adequacy decision for Japan. These rules oblige Japanese businesses 'to ensure (e.g. by technical ("tagging") or organisational means (storing in a dedicated database)) that they can identify personal data transferred from the EEA throughout their "life cycle."'[1162] Recital 75 of the adequacy decision requires that further recipients of EEA data outside Japan are subject to rules ensuring a '*similar'* level of protection to that of the Japanese legal order. The 'similar' as opposed to 'essentially equivalent' standard suggests that the adequacy decision sets a lower threshold for the legal framework in a country of onward transfer to meet, than that threshold applicable to countries of destination where personal data is transferred directly from the EEA.

The adequacy decision for Japan, including the Supplementary Rules, provides for three principal options for onward transfers of EEA data from Japan. The first option allows onward transfers based on an individual's consent.[1163] Supplementary Rule 4 specifies that 'consent' means that the individual has been 'provided information on the circumstances surrounding the transfer necessary for the principal[1164] to make a decision on his/her consent'. According to Recital 76 of the adequacy decision, this provision ensures that 'such consent will be particularly well informed' and will allow [individuals] to assess the risk for the privacy involved in the transfer.' Greenleaf, however, rightly argues that Japanese consent requirements are lower than those under the GDPR.[1165] The second and third options allow an onward transfer of personal data from Japan without such consent if (a) the country of destination of the onward transfer has been recognised by the Japanese data protection authority as providing a level of protection of personal data 'equivalent' *to that of Japan;* or (b) if the data exporter from Japan and importer in a third country have together implemented binding arrangements that guarantee an *equivalent*

[1161] CETA with Canada and JEFTA with Japan.
[1162] Recital 15 Adequacy Decision for Japan.
[1163] Recital 76 Adequacy Decision for Japan, Supplementary rule 4.
[1164] In terms of the GDPR, 'principal' means 'data subject'.
[1165] Greenleaf (2018b), p. 8.

level of data protection to that in Japan by means of a contract, other forms of binding agreements or binding arrangements within a corporate group.[1166]

The adequacy decision for Canada simply does not address at all the issue of onward transfers of personal data.[1167] Under Canadian federal law (the Personal Information Protection and Electronic Documents Act (PIPEDA)), transfers of personal data outside Canada are regulated by the principle of accountability. The 2009 Guidance by the Office of the Privacy Commissioner (OPC) of Canada explains that a transfer of personal data to a third party for the purposes of processing (including when such party is outside Canada) does not constitute disclosure of such personal data; therefore additional consent is not required for such a transfer.[1168] It stipulates that such transfers are subject to the accountability of the Canadian organisation transferring personal data outside Canada, which means that such an organisation remains responsible for protecting personal data under its control. The primary means of compliance with this principle is through contractual arrangements to ensure that the third party will provide a *comparable* (not 'essentially equivalent' as required by the GDPR) level of personal data protection. [1169] The Canadian OPC also requires organisations to assess the risks and benefits of transferring personal data outside Canada, and recommends applying higher standards of protection to sensitive data, such as financial data, and to refrain from such transfers when the risks are too high (e.g. due to the 'uncertain nature of the foreign regime').[1170] In its opinion on the adequacy of PIPEDA, the Article 29 Working Party noted that such contractual or other binding provisions are able to provide a comparable level of data protection.[1171] After a public consultation concluded in September 2019, the OPC decided that the 2009 Guidelines should remain 'unchanged under the current law'.[1172] At the same

---

[1166]The adequacy decision explicitly states that APEC Cross-Border Privacy Rules cannot be used as a mechanism for onward transfers of EEA personal data from Japan. Recital 79.

[1167] Kuner (2009), p. 5 ('It is also striking that in its own adequacy decisions, the European Commission does not always require that third countries found adequate themselves prohibit the transfer of personal data to non-adequate countries. For example, the Canadian Personal Information Protection and Electronic Documents Act (PIPED Act (PIPEDA)) has been found adequate, even though the Act itself contains no such prohibition'.)

[1168] Office of the Privacy Commissioner of Canada, Guidelines for Processing Personal Data Across Borders, January 2009.

[1169] Principle 1 of the CSA Model Code for the Protection of Personal Information, Schedule 1 of PIPEDA. states:

> An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

[1170] Office of the Privacy Commissioner of Canada, Guidelines for Processing Personal Data Across Borders, January 2009.

[1171] Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act, WP 39, 26 January 2001, p. 6.

[1172] Office of the Privacy Commissioner of Canada, Commissioner concludes consultation on transfers for processing, 23 September 2019.

time, the Privacy Commissioner acknowledged that the 'PIPEDA's accountability principle is not always effective in protecting Canadians in the context of international transfers' and requires reform.[1173] Similar to the situation with Japan's adequacy decision, this shows that the standard required for onward transfers is lower than that required by the GDPR for transfers of personal data outside the EEA.

To sum up, the most recent adequacy decision for Japan devotes significantly more attention to the question of onward transfers of personal data than the earlier adequacy decision for Canada. Analysis of the onward transfer mechanisms in the adequacy decision for Japan shows, however, that the range of onward transfer mechanisms is narrower than the range of mechanisms for transfers of personal data available under Chapter V of the GDPR and is limited solely to contractual arrangements or binding arrangements within a group and individual consent. Despite the fact that the choice of onward transfer mechanisms is restricted, in substance their application is unlikely to meet the standard of 'essential equivalence' to the EU framework, and, therefore, the strict necessity and proportionality tests for derogation from these fundamental rights under Article 52(1) of the Charter.

In relation to consent, for example, Greenleaf convincingly argues that it cannot serve as a sufficient basis for onward transfers of personal data for at least three reasons.[1174] First, the Supplementary Rules annexed to the adequacy decision for Japan do not require, when obtaining consent, individuals to be informed that their data will be subject to an onward transfer to a country with a lower level of data protection.[1175] Second, as already mentioned above, the standard for actually obtaining consent under Japanese law is lower than that under the GDPR.[1176] The third, and more systemic, issue is that, under the GDPR, consent is a specific derogation that is inappropriate for systematic transfers of personal data. The fact that it can be used as a legal ground for systematic onward transfers of personal data from Japan is inconsistent with the logic of the GDPR, where under Article 49 GDPR, as interpreted by the EDPB, consent can be used only for non-repetitive and occasional transfers.[1177] This thesis contends that it is precisely because of the fact that specific derogations, such as consent, are not intended for systematic transfers, that the

[1173] 2018-2019 Annual Report to Parliament on the Privacy Act and the Personal Information Protection and Electronic Documents Act. Data protection law reforms have been announced in December 2019 by Canada's Prime Minister Trudeau. See Hunt (2019).
[1174] Greenleaf (2018b), p. 8.
[1175] *Ibid.* ('Supplementary Rule (4) requires that the individuals concerned shall be "provided information on the circumstances surrounding the transfer necessary for the principal to make a decision on his/her consent". However, there is no obligation to tell the person that their data will be transferred to a country with very weak privacy laws such as the US'. Internal footnotes omitted).
[1176] *Ibid.*
[1177] EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018.

CJEU in *Schrems II* did not impose the 'essential equivalence' standard on transfers using such derogations. As the Article 29 Working Party noted in the 2014 Opinion on data protection in Québec, 'consent should not be promoted as the general legal basis for onward transfers as the recipient then does not commit to take any action to ensure an adequate level of protection; this situation should thus remain an exception.'[1178] In essence, by allowing regular transfers on the basis of consent, the adequacy decision for Japan allows the circumvention of the GDPR rules restricting transfers of personal data on the basis of consent. This places Japanese companies in a more favourable position than those from third countries that have not been afforded adequacy, as unlike Japanese companies, those companies cannot rely on consent for systematic transfers of personal data from the EEA.

In respect of using contractual arrangements and binding agreements within the group as mechanisms for onward transfers, there are at least two potential problems. The first is that, unlike the SCCs and the BCRs in the GDPR framework, there are no specific requirements that such contractual and intra-group arrangements must incorporate. Recall that the model SCCs in the EU are approved by the Commission and must be incorporated verbatim in the contract. As confirmed by the CJEU in *Schrems II*, these provide for 'effective mechanisms' for protection of personal data, but only to the extent that transfers are suspended or prohibited when the recipient of data is unable to comply with those clauses.[1179] In addition, the GDPR provides for extensive requirements as to the content of the BCRs, further elaborated in the EDPB guidance.[1180] Furthermore, the compliance of BCRs with the GDPR is ultimately certified by the EDPB, which approves BCRs before they take effect.[1181] The absence of similar requirements in relation to contractual and intra-group arrangements used for onward transfers of personal data from Japan and Canada is likely to lead to a lower level of data protection as compared to that under the SCCs and the BCRs. The second problem, as discussed in Section 5.3.1 above, is that appropriate safeguards like the SCCs and the BCRs can be used as mechanisms for systematic transfers of personal data to third countries that have not been afforded adequacy only subject to prior comprehensive case-by-case assessment by data exporters of such third country's legal framework. Relying on the logic of the EU framework for transfers of personal data as interpreted by the CJEU in *Schrems II*, and in light of the aims pursued by the EU

[1178] Article 29 Working Party, Opinion 7/2014 on the protection of personal data in Quebec, WP 219, 4 June 2014, p. 10.
[1179] CJEU, *Schrems II*, para. 148.
[1180] Art. 47(2) GDPR; Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev.01, 6 February 2018; Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 257 rev.01, 6 February 2018.
[1181] Art. 47(1) GDPR.

framework for transfers of personal data, the same assessment must be conducted whenever contractual or intragroup arrangements are used for onward transfers of personal data. This requirement could indeed be one of the outcomes of the above-mentioned ongoing review of adequacy decisions by the European Commission. The adequacy decision for Japan, however, is not covered by such review. Until this deficiency is rectified through amendment by the Commission, or interpretation in the light of *Schrems II* by the EDPB or domestic courts, this adequacy decision is unlikely to yield an essentially equivalent protection of personal data in the context of onward transfers.

A further complicating factor is, as already mentioned, that since 2018 both Japan and Canada have been subject to an obligation to ensure free cross-border data flows between the parties to the CPTPP, most of which do not have an adequacy decision from the EU.[1182] The USMCA contains a similar provision.[1183] Unlike Canada, the US and Mexico do not have an adequacy decision from the EU. These international trade obligations put additional pressure on the mechanisms of onward transfers under the adequacy decisions. Given that the EU is refraining from including such obligations in its own trade agreements, countries, such as Japan and Canada, to which EU personal data can be transferred without restrictions, can become – in a multinational company's setting - a transit point for data transfers to other countries not afforded adequacy, thus circumventing the EU framework for cross-border transfers of personal data.

5.3.3 Limited scalability of EU framework for transfers of personal data

Against the backdrop of the broad understanding of the notion of 'personal data' in the EU, this Section argues that the EU regime for transfers of personal data outside the EEA in Chapter V GDPR lacks granularity in the sense that the same rules apply irrespective of the context, volume and type of data transferred and other parameters of data transfers. In a world where massive volumes of personal data are transferred every second, it is unrealistic to expect that the stringent EU framework under Chapter V of the GDPR will be observed in all those transfers. Even more unrealistic is it to believe that the EU DPAs endowed with the powers to enforce this compliance can have the capacity to monitor such compliance and enforce against non-compliance in order to produce an effective level of deterrence to violate such rules. As a result, there is a mismatch between the *legal framework* and the *reality* of data transfers in the digitalised world.

[1182] Art. 14.11(2) CPTPP.
[1183] Art. 19.11 USMCA.

EU law maintains a distinction between personal data and non-personal data, which are governed by two different legal frameworks.[1184] In the digital environment, where almost any data can be linked to an identifier, the distinction between what constitutes personal data and what remains non-personal data – and therefore not subject to the scrutiny of stringent data protection rules – is often difficult to make.[1185] While cross-border transfers of personal data are subject to a 'border control'[1186] regime as discussed above, transfers of non-personal data outside the EEA are not subject to restrictions on transfers under the GDPR.[1187] As a result, there is misalignment between reality, where it is hard to draw a distinction between personal and non-personal data, and the legal framework, which qualifies data as either personal and non-personal.

Schwartz and Solove succinctly summarise four main problems with this distinction. First, almost any data online can be qualified as personal data. The 'built-in identifiability' in cyberspace makes anonymity online a 'myth', as all online data can be linked to some identifier.[1188] Second, non-personal information can be transformed into personal data over time. Third, the distinction between personal and non-personal data has a dynamic nature, as the line between the two depends on technological developments. Fourth and finally, the borderline between personal and non-personal data is not firm, but rather contextual, as many kinds of data are not non-identifiable or identifiable in the abstract.[1189]

[1184] Koops (2014), p. 257 ('EU data protection law applies an all-or-nothing approach: data is either personal data (triggering the whole regime), or it is not (triggering nothing), but it cannot be something in between or something else'.) While processing of personal data is regulated by the GDPR, non-personal data is governed by Regulation on Non-Personal Data.

[1185] Recital 9 Regulation on Non-Personal Data. For a discussion, see Tene, Polonetsky (2013); Kondor, Hashemian, De Montjoye, Ratti (2018); Schwartz, Solove (2011); Purtova (2018), p. 78; Ohm (2010), p. 1706 (warning about the problems of re-identification of personal data and stressing that even truly anonymised personal data at some point in time may be re-identified.)

[1186] Svantesson (2011), p. 184; LeSieur (2012), pp. 101, 103–04.

[1187] Regulation on Non-Personal Data does not provide for any restrictions on cross-border transfers of non-personal data outside the EEA. See also Art. 11(1) the Proposal for a Directive of The European Parliament And Of The Council on the re-use of public sector information (recast). COM/2018/234 final - 2018/0111 (COD). ('Any applicable conditions for the re-use of documents shall be non-discriminatory for comparable categories of re-use, including for cross-border re-use'.) See also Collington (2019); Irion, Williams (2019), p. 31.

[1188] See also Ohm (2010), p. 1706 (warning about the problems of re-identification of personal data and stressing that even truly anonymised personal data at some point in time may be re-identified.)

[1189] Schwartz, Solove (2011), pp. 1836 – 1848. Stating that

> [f]irst, many people believe in an 'anonymity myth,'-that is, a belief that individuals remain anonymous if they have not formally used their name. This belief is especially prevalent for cyberspace activity. Yet, the growth of static IP addresses and other developments creates some built-in identifiability when one enters cyberspace. Second, information that is initially non- PII can be transformed into PII. Third, technology itself is constantly evolving, which means that the line between PII and non-PII is not fixed but rather depends upon changing technological developments. Fourth, the ability to distinguish PII from non-PII is frequently contextual. Many kinds of information are not inherently non- identifiable, or identifiable as an abstract matter.

The EU Regulation on Non-Personal Data illustrates a number of those points. It specifically mentions that examples of non-personal data include 'aggregate and anonymised datasets used for big data analytics, data on precision farming that can help to monitor and optimise the use of pesticides and water, or data on maintenance needs for industrial machines'.[1190] The Regulation, however, also notes that '[i]f technological developments make it possible to turn anonymised data into personal data, such data are to be treated as personal data, and [the GDPR] is to apply accordingly'.[1191] Although the very existence of this Regulation is grounded on the possibility of separating the notions of personal and non-personal data, the Regulation itself suggests that such distinction is not clear-cut and requires constant re-assessment.

Maintaining this distinction between personal and non-personal data in a situation where almost any data element can be qualified as personal at a specific point in time can also be very costly.[1192] The transition of data from non-personal to personal leads to higher compliance costs and the risks of multimillion Euro fines.[1193] As a result, the problems of distinguishing personal and non-personal data exemplify a tendency of any data potentially becoming personal in the future and being treated as personal.[1194] The upshot of this is that the GDPR has become applicable to virtually any operations with data, which, in the words of Purtova, makes it 'the law of everything'.[1195] Viewing this tendency critically, Koops argues that broadening the notion of personal data leads to an 'artificial framing of data-processing problems in terms of personal data'.[1196] These authors predict that the

---

[1190] Recital 9 Regulation on Non-Personal Data.
[1191] *Ibid*.
[1192] A 2019 OECD study shows that businesses across sectors overwhelmingly report that separating personal from non-personal data is likely to be costly or very costly. Casalini, López González (2019), p. 33 and figure 6 ('The extent to which firms can identify and split personal from non-personal data was also identified as an issue for firms. Respondents to the business questionnaire overwhelmingly reported that separating data was likely to be costly or very costly, a response consistent across most sectors')
[1193] Art.83(4)-(5) GDPR.
[1194] Ohm (2010), p. 1742. ('No matter how effectively regulators follow the latest re-identification research, folding newly identified data fields into new laws and regulations, researchers will always find more data field types they have not yet covered. The list of potential PII categories will never stop growing until it includes everything'. Internal footnotes omitted); Purtova (2018), p. 41 arguing that 'literally any data can be plausibly argued to be personal'.
[1195] Purtova (2018), p. 41.
[1196] Koops (2014), p. 258 (arguing that in the EU all data processing 'is seen through the lens of personal data, in the frame of data protection law', which requires 'stretching the concept of personal data (sometimes to the point of breaking, or perhaps rather of becoming void of meaning), or stretching the regulatory problem so that it becomes a problem of processing personal data'. He also argues that 'the second problem of relying on law in the books is the expansion of data protection legislation to include almost all types of data processing, leading to an artificial framing of data-processing problems in terms of personal data'.) See also Granger, Irion (2018), p. 16 (highlighting 'a recent tendency to overcharge EU data protection law with expectations that it would come to terms with the much more complex challenges of algorithmic decision-making and artificial intelligence'.) But see Dalla Corte (2019) (proposing a 'nuanced epistemological approach' to interpretation of the notion of 'personal data' in order to avoid overly extensive interpretation of this notion.)

application of the GDPR's 'highly intensive and non-scalable regime' to virtually any data processing will devoid this data protection framework of any meaning,[1197] by leading to paper compliance and selective enforcement.[1198] In the same vein, Helen Dixon, the head of the Irish DPA – which is in charge of supervising the European data processing operations of a number of big tech companies – acknowledged in a media interview that '[o]ne of the problems with GDPR is that it has become the law of everything, and that it's drawing data protection authorities, who are not elected officials, into making an awful lot of decisions that impact societies and individuals, which go well beyond data processing.'[1199] As Bygrave noted in connection to this, the 'general discourse on data protection has become extremely GDPR-centric' in that 'the [GDPR] has effectively created a vortex that sucks policy discussion into its fold'.[1200]

The point about the broad definition of personal data is not made here with a view to criticise the breadth of this definition in the GDPR, as there are good normative reasons to support a broad definition of this notion.[1201] Given that the rights to privacy and the protection of personal data are protected as fundamental rights, maintaining a broad concept of 'personal data' is essential to ensure a high level of protection of these fundamental rights.[1202] Rather, this is meant here as a critique of the way in which EU institutions *use* the broad definition of personal data in their discourse to expand their competence through framing the issues beyond data protection as GDPR issues, as their competence to legislate on data protection is 'clear-cut'.[1203] Furthermore, to be clear, this thesis also does not propose to eliminate a legal distinction between personal and non-personal data and, as Purtova has suggested, to treat *all* data as personal,[1204] as this would water down the legal data governance framework even further. The thesis does, however, call for a reform of data protection rules on transfers of personal data to make them more scalable and, therefore, more effective in practice.

[1197] Purtova (2018), p. 75 ('a highly intensive and non-scalable regime of rights and obligations created by the GDPR will not simply be difficult but impossible to maintain in a meaningful way'.)
[1198] *Ibid.*, pp. 77-78 ('Facing the threat of effective and deterring sanctions, the controllers, instead of engaging in a meaningful assessment of fairness and necessity, will be pushed to create the formal appearance of compliance by using "compliance surrogates", such as compliance roadmaps, "accountability tools," trust marks and certification schemes'.); *Ibid*., p. 78 ('Alternatively, or in addition, enforcement of the data protection rights and obligations will likely become selective, determined by priority lists and short- cuts that the data protection authorities would develop to cope with the workload, including the "compliance surrogates". Selective enforcement and the pretence of compliance will reinforce each other, ridiculing data protection law, and depriving its protection of meaning'.)
[1199] Tene (2020a).
[1200] Bygrave (2020).
[1201] See, e.g., Demetzou (2020), p. 131.
[1202] Purtova (2018), p. 78; Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP 136, 20 June 2007.
[1203] Tene (2020a).
[1204] Purtova (2018), pp. 79-80.

To some extent, the GDPR has already made steps towards greater scalability by implementing a risk-based approach to data protection. In particular, the GDPR contains stricter rules for the processing of special categories of personal data, such as personal data relating to health, race or sexual orientation.[1205] Data about criminal convictions, the content of electronic communications, and financial and location data have also been recognised as sensitive by the Article 29 Working Party and its successor, the EDPB, due to the higher risks of processing these types of data for individual rights. They are therefore, subject to a higher level of protection than personal data falling into what one might call the general category.[1206] In addition, in several contexts (for example, in the balancing between the legitimate interest of the data controller as the legal ground for processing personal data with the risk to the fundamental rights of data subjects, data breach notification, accountability of data controller), the GDPR allows data controllers to calibrate their obligations in accordance with the risk that certain processing of personal data may pose to the fundamental rights of individuals.[1207] Furthermore, the GDPR has codified a notion of *pseudonymised data*.[1208] Recital 28 of the preamble to the GDPR explicitly states that the 'application of pseudonymisation to personal data can reduce the risks to the data subjects concerned'. As noted by various experts in the field and European Data Protection authorities, the GDPR already provides for more lenient rules for pseudonymised data when it comes to the rights of individuals, data breach notification requirement and the possibilities of using the data for purposes other than that for which it was originally collected.[1209]

None of these flexibilities, however, are taken into account in the GDPR's framework for transfers of personal data *outside the EEA* in Chapter V. Therefore, the criticism of non-scalability, lack of nuance and a catch-all method fully applies to this set of rules. Moreover, as compared to the substantive data protection framework, which, to some extent has embraced a risk-based approach, the provisions on data transfers do not differentiate between different degrees of risks to fundamental rights that transfers of personal data may entail for individuals. Given the expansive scope of information that may constitute personal data, this 'one-size-fits-all' approach to cross-border transfers is

[1205] Art. 9 GDPR.
[1206] Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA), WP 248rev.01, 4 October 2017.
[1207] Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, 9 April 2014. At the time of writing, the EDPB is working on the new guidelines on the topic.
[1208] Art. 4(5) GDPR.
[1209] Recitals 29, 50 and 156, Arts. 6(4), 11(1), 12(2), 14(5)(b) GDPR; Article 29 Working Party Guidelines on transparency under Regulation 2016/679, WP260 rev.1, 11 April 2018, p. 31; Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, WP250rev.01, 6 February 2018, pp. 15-16, 21; De Brauw Blackstone Westbroek (2018); McCreanor (2018); Maldoff (2016).

not sustainable in the long run as it applies to growing datasets including 'Big Data' corpora systematically crossing EEA borders. Under these circumstances, it is hardly realistic to expect that the same level of 'effective and complete' protection of all personal data transferred internationally can be achieved in practice. Requiring the same level of compliance with a strict regime for transfers of personal data for such a broad scope of data is simply inoperable. Kuner thus seems to be correct when he argues that '[t]he definition of transborder data flows is so broad that it can cover most acts of data processing on the Internet, and no national regulation could ever be consistently enforced with regard to such a vast amount of data processing on a global scale.'[1210] It is therefore entirely unsurprising that enforcement of the rules on cross-border data flows has so far been ineffective.[1211] Throughout the lifetime of the EU data protection framework, the only significant enforcement actions came from the CJEU, which, as discussed above, invalidated adequacy decisions issued by the European Commission for the US.[1212] Just as there was 'very little enforcement related to the *Schrems [I]* judgement',[1213] *Schrems II* is unlikely to lead to a surge of enforcement actions in the context of data transfers.[1214] Apart from a few enforcement actions triggered by the CJEU, there have not been, until recently, any known enforcement cases for violations of rules on transfers of personal data. It was only in June 2020 that the EDPB initiated the first major enforcement action to date by establishing a taskforce to coordinate potential enforcement actions across Europe against TikTok, which covers, in particular, the company's practices of transferring personal data to third countries.[1215]

The risk of enforcement is one of the major drivers behind companies' compliance with data protection rules. Thus, a lack of enforcement reduces the risks of non-compliance with the cross-border transfer rules, making them even less effective in performing their

---

[1210] Kuner (2013), pp. 154-155. See also Koops (2014), p. 259:

> The regulatory disconnection of data protection law, with risks being enlarged rather than diminished through stretching the scope of data protection law to embrace new regulatory issues, together with a narrow focus on command-and-control law, demonstrate a fallacy of regulators to believe that every problem related to Internet data flows can be regulated by data protection law in the books. It does not work, as any realist looking at 21st century data processing practices will acknowledge.

[1211] Kuner (2013), p. 144. ('The levels of compliance and enforcement of transborder data flow regulation are important indicators of its effectiveness. A lack of enforcement, or inconsistent enforcement, may reduce respect for a particular rule, and for a regulatory system in general'.)

[1212] CJEU, *Schrems I* and *Schrems II*.

[1213] Kuner (2017), p. 885.

[1214] Referring to the inaction on the part of the DPAs, Max Schrems, the activist behind the legal action that led to the CJEU *Schrems II* judgement has already filed 101 complaints with DPAs across Europe to pressurise the authorities to take action. Noyb (2020a). Some authorities, however (e.g. the Finnish DPA) have initiated several inquiries following the request. See Clark (2020).

[1215] EDPB, Press Release, Thirty-first Plenary session: Establishment of a taskforce on TikTok, Response to MEPs on use of Clearview AI by law enforcement authorities, Response to ENISA Advisory Group, Response to Open Letter NYOB, 10 June 2020.

function of preventing the circumvention of the EU's high level of personal data and privacy protection.

5.4 Directions of thought on how to improve the EU framework for transfers of personal data outside the EEA

A reform of the GDPR's framework for transfers of personal data outside the EEA is necessary to address its weaknesses, as identified in the previous Section. This Section suggests and elaborates upon three possible lines of thought on how to improve the framework. It should be acknowledged that a fully-fledged reform proposal cannot be developed within the boundaries of this work for a few reasons, among them the fact that the aim of this thesis is to situate the need for reform in the context of international trade law and the EU's approach to existing and future trade commitments. A comprehensive reform of the GDPR would require an interdisciplinary effort based on a host of both domestic and international factors, an endeavour which goes well beyond the scope of this thesis. Hence, this Section's objective is to inform and suggest reform paths, but not to offer an *exhaustive* overview of opportunities for reform of the GDPR's Chapter V.

The three proposed paths or lines of thought that this Section considers are as follows. The first, and the most moderate, is to improve *specific elements* of the mechanisms for transfers of personal data already present in Chapter V of the GDPR but without changing the design and composition of the framework. The second, intermediate, path incorporates the first but goes a step further by suggesting adding several new elements to the extant framework based on key recent developments in EU data protection law and technology. The third, and the most radical, path is a complete redesign of GDPR Chapter V's framework, for example by re-anchoring it on a risk-based approach, with elements proposed as a part of the second line of thought. The three paths roughly correspond to short, medium, and long term strategies for the reform of Chapter V of the GDPR.

Before moving on to the discussion of each path, two remarks are in order. First, recall, that while some form of restrictions on transfers of personal data form part of the essence of the fundamental rights to privacy and the protection of personal data, their specific design – with some specific exceptions[1216] – is subject to balancing with the aim

[1216] Based on the current CJEU case law, the elements of the design of the framework for transfers of personal data, which constitute a part of the essence of the fundamental rights to privacy and the protection of personal data, include: a) restrictions on generalised access to the content of electronic communications; b) compliance with the purpose limitation principle, the rules designed to ensure, inter alia, the security, confidentiality and integrity of the data, and to protect them against unlawful access and processing; c) limitations on the retention of the content of communications; d) rules that provide for some possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data. For a discussion see Section 5.2.3.2.

of ensuring 'essentially equivalent' protection of personal data. This balancing must be conducted on the basis of the principles of strict necessity and proportionality (Article 52(1) of the Charter), which, as Section 5.2.2 above explained, underlie the 'essential equivalence' standard. Second, the concept of 'essential equivalence' itself does not constitute the essence of the fundamental rights to privacy and the protection of personal data under the Charter. It does, however, constitute a part of the constitutional meaning of the above-mentioned fundamental rights and is not merely an interpretation of the secondary EU data protection law concept of 'adequacy'.

5.4.1 Improving the operation of the current framework

This line of thought considers a number of improvements to existing mechanisms for transfers of personal data, in particular adequacy and the SCCs. It also recommends the operationalisation of the codes of conduct and certification mechanisms, which are envisaged as data transfer mechanisms in the GDPR but have not yet been implemented in practice. Although this line of thought does not resolve some of the conceptual drawbacks of the framework of Chapter V, its modesty makes it easier to implement, at least in the short term. Furthermore, it could yield an incremental improvement through fairly minor changes to the GDPR and CJEU jurisprudence without having to redesign the framework for transfers of personal data at its core, which seems a much longer-term exercise.

To address the proneness of adequacy decisions to political influence, the EU could adopt a transparent procedure governing such assessments. According to Kuner, the European Commission already has internal guidelines for evaluating adequacy, though they have never been published.[1217] A renewed procedure could, in particular, regulate the process of the selection of countries (or application by countries themselves) in relation to which the adequacy assessment is to be conducted and the detailed procedure for an adequacy assessment, including the due involvement of all stakeholders (such as the EDPB and European Parliament), the time frame for the whole process as well as for each step of the assessment. All this would ensure, among other things, that stakeholders have sufficient time and opportunity to review the assessment.[1218] The Commission could be required to respond and substantiate its deviation from the recommendations or opinion of stakeholders, and to involve experts in the assessment, so as to exclude situations where the review of the foreign legal system is conducted by the European Commission's employees on the basis essentially consisting of submissions by the foreign government.

[1217] Kuner (2017), p. 901.
[1218] EDPB, Contribution of the EDPB to the evaluation of the GDPR under Article 97, Adopted on 18 February 2020, pp. 4-6 (noting that the EDPB should have sufficient time to review adequacy decisions.)

Such a procedure could be adopted by a Commission's Implementing Regulation, which, however, would require including a relevant enabling provision in the GDPR.

To enhance ongoing monitoring of the foreign legal framework, and in order to mitigate the fact that an adequacy assessment (and its review once in four years) constitutes a snapshot of the foreign legal framework at a particular point in time, adequacy decisions could transition from a unilateral instrument to a reciprocal agreement, under which the foreign country would undertake certain obligations. For example, such an agreement could include a mechanism of notifications by the foreign government of any changes to legislation taken into account during the adequacy assessment, and provide for negative consequences for non-notification, if discovered during the periodic review. This change would not require any amendments to the GDPR.[1219]

The onward transfer mechanisms should, as much as possible, mirror the appropriate safeguards provided for in the GDPR and as interpreted by the CJEU in *Schrems II*. This is necessary in order to avoid discrimination between transfers of personal data on the basis of appropriate safeguards to countries not afforded adequacy from the EEA (under Article 46 GDPR) and *onward transfers* of personal data from a country that has been afforded adequacy, to another country that has not been afforded adequacy. In particular, consent should not be generally allowed as a legal ground for systematic onward transfers (as discussed above, consent serves as one of the grounds for onward transfers in the EU adequacy decision for Japan). In addition, contractual mechanisms used for onward transfers should incorporate the SCCs approved by the European Commission; their wording should not be left to the discretion of the parties.

In relation to the SCCs, as Kuner argued, controller-to-controller SCCs could be improved by putting a greater emphasis on the practically enforceable redress mechanisms and dropping the obligations that are difficult to enforce in practice.[1220] In particular, Kuner has proposed to reform the 2004 SCCs by eliminating or shifting some of the data importer's obligations to the data exporter because they are difficult to enforce outside the EU.[1221] To enhance the effectiveness of the SCCs, the European DPAs should also enhance their enforcement efforts on this issue, for example, through conducting industry scans and

[1219] The most recent (and thus far the only) adequacy decision under the GDPR –Adequacy decision for Japan – contains Supplementary Rules, which Japan undertook in order to compensate for the deficiency of its legal framework for protection of personal data as compared to that of the EU. Similarly, the two adequacy decisions for the US – the invalidated EU-US Safe Harbor and the EU-US Privacy Shield – contain representations by the US Government in relation to the protection of personal data.
[1220] Kuner (2009), pp. 8-9. See also Kuner (2011), p. 26.
[1221] Kuner (2009), pp. 8-9.

requests for information, while prioritising the transfers that that carry the greatest risks for individuals.[1222]

The issue of foreign governments' access to personal data transferred from the EEA is a highly politically contentious one. It also cuts across an intricate relationship between the EU legislature and the CJEU, as it was the CJEU that introduced this issue to the EU framework for transfers of personal data in the first place. Although in the long term, as this thesis argues in Section 5.3.1 of this Chapter, this topic should be addressed by the EU at the international level, in the short term, the DPAs should issue comprehensive guidance on the assessment of the 'essential equivalence' of foreign legal frameworks for the purposes of relying on Article 46 for personal data transfers and formulate additional safeguards that companies could use to mitigate the lack of 'essential equivalence'. This is essential in order to avoid a surge of private enforcement in this area, which would lead to the fragmentation of approaches across the EU, at least, in the short and medium term. The EDPB could also spearhead a platform with reliable resources necessary to assess the 'essential equivalence' of third countries' frameworks, prioritising those where personal data is transferred most from the EEA.[1223]

5.4.2 Greater scalability

A second, intermediate line of thought suggests adjustments to the GDPR's framework for transfers of personal data *complementing* those encompassed by the first line of thought discussed in the previous Section. It would require a more substantial revision of the GDPR and, therefore, could realistically be addressed only in the medium term. For example, it could be introduced as a result of the next review of the GDPR's Chapter V under Article 97 of the GDPR, which is scheduled for 2024.

The two principle adjustments that could be introduced into Chapter V of the GDPR are (a) the introduction of the more lenient rules for transfers of pseudonymised data as long as such data does not include sensitive data;[1224] and (b) a codification of the legal significance of technological means for protection of personal data, including as a means of ensuring that pseudonymised data will not be re-identified after the transfer. In his 2014 article, Koops suggested that pseudonymised data could become a 'useful in-between

[1222] See Kuner (2011), p. 27.
[1223] A private crowd-sourced initiative has been recently launched by Christopher Schmidt. Although this resource provides useful insights, it does not guarantee accuracy of the information and that the EDPB will take this information in to account in conducting their assessment during a possible enforcement action. EUROPEAN ESSENTIAL GUARANTEES GUIDE, https://www.essentialguarantees.com/
[1224] Just like pseudonymised personal data remains personal, pseudonymised sensitive data remains sensitive data. This means that processing pseudonymised sensitive data still involves a higher risk than processing pseudonymised 'ordinary' personal data.

category' between personal and non-personal data.[1225] He proposed, accordingly, the creation of a special legal regime for pseudonymised data that would be 'milder' than the regime for personal data but stricter than for non-personal data.[1226] Kuner proposed relaxing restrictions on cross-border transfers of pseudonymised and encrypted data under appropriate circumstances,[1227] and data in transit.[1228] Similarly, but in more general form, Schwartz and Solove have suggested calibrating the intensity of the data protection regime depending on the risk of identification of individuals, based on three categories of personal information (or data): (a) identified, (b) identifiable, or (c) non-identifiable.[1229] As one of the advantages of their proposed approach, Schwartz and Solove name the incentives to companies to invest resources in maintaining data in the less identifiable form. In contrast, in the current EU regime that treats identifiable and identified data as equal, such incentive is absent.[1230] Most recently, some data protection authorities and scholars proposed to use encryption, pseudonymisation and other privacy enhancing technologies as one of the additional safeguards that data exporters can implement while transferring personal data to countries that do not ensure an adequate level of data protection based on the SCCs.[1231]

Since the adoption of the GDPR, pseudonymised data, defined in article 4(5) GDPR, gained more prominence in the EU data protection framework. Recital 28 of the preamble to the GDPR explicitly states that the 'application of pseudonymisation to personal data can reduce the risks to the data subjects concerned'. As noted by various experts in the field and European DPAs, the GDPR already provides for more lenient rules for pseudonymised data, when it comes to the rights of individuals, data breach notification requirements, and the possibilities of using the data for purposes other than that for which it was originally

---

[1225] Koops (2014), p. 257, fn. 40. At the same time, Koops criticises the definition of 'pseudonymised data' in the (then draft) GDPR. That wording, however, has not changed in the final version of the GDPR.
[1226] *Ibid*., p. 257 ('… not all identifiers function in the same way, and it makes sense to differentiate in the legal regimes for different types of identifiers'.)
[1227] Kuner (2013), pp. 97, 99.

> Pseudonymization is used on a wide scale in some important areas (eg, in clinical trials of pharmaceutical products), and can be regarded as a form of encryption, since it allows identification of an individual only under limited conditions and by certain parties; it should be encouraged by relaxing restrictions on transborder data flows under appropriate circumstances. … [G]reater use should be made of technology in the context of transborder data flow regulation, such as by the creation of 'safe harbours' to ease regulatory approval of transborder flows of encrypted data.

See also Hon, Millard (2012), p. 27.
[1228] Kuner (2013), p. 175.
[1229] Schwartz, Solove (2011), p. 1877. See also Schwartz, Solove (2014), p. 905.
[1230] Schwartz, Solove (2011), p. 1883. In particular Schwartz and Solove quote Article 29 Working Party Guidance for ISPs and search engine operators, where the Working Party introduced an 'absolutely certainty test' requiring companies to treat data as personal unless they can demonstrate 'with absolute certainty that the data correspond to users that cannot be identified'. See Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP 136, 20 June 2007, p. 17; Article 29 Working Party, Opinion 1/2008 on data protection issues related to search engines, WP 148, 4 April 2008, p. 8.
[1231] See e.g. One Trust Data Guidance (2020a); Christakis (2020).

collected.[1232] Relaxation of these data protection principles, two of which are explicitly mentioned in Article 8 of the EU Charter, in relation to pseudonymised data, suggests that a lighter touch regulatory approach to transfers of such data outside the EEA could be compliant with the EU Charter and the GDPR. In particular circumstances, such as scientific or academic research, where societal benefits of data processing are high and risks of interference with fundamental rights could be minimised through various technological means, such as differential privacy and ethical safeguards of the profession, the transfer of pseudonymised data could be allowed without restrictions. Such a possibility would be welcome, for example, in global health crises such as the one triggered by the COVID-19 pandemic in 2020.[1233] It should, however, also be acknowledged that pseudonymisation is effectively a security measure which reduces the risks associated with personal data processing. The way in which this measure should be taken into account in designing more flexible rules for transfers of personal data outside the EEA requires further research.

In relation to the role of technology in governing information flows, Reidenberg in his seminal 1998 article 'Lex Informatica', showed that 'for network environments and the Information Society … law and government regulation are not the only source of rule-making. … The creation and implementation of information policy are embedded in network designs and standards as well as in system configurations.'[1234] He argued that Lex Informatica – 'the set of rules for information flows imposed by technology and communication networks' – had an equally important role to play, along with the law, in governing information flows online.[1235] Similarly, Kuner argued more recently that 'technology could play a greater role in transborder data flow regulation'; in particular, through the principle of 'privacy by design' (which is now codified in the GDPR), it could explicitly include a possibility to regulate cross-border data flows in part by technological solutions.[1236] He also noted that companies already routinely configure their international IT systems to regulate cross-border flows of data and access rights in their IT networks.[1237]

[1232] Recitals 29, 50 and 156, Arts. 6(4), 11(1), 12(2), 14(5)(b) GDPR; Article 29 Working Party Guidelines on transparency under Regulation 2016/679, WP260 rev.1, 11 April 2018, p. 31; Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, WP250rev.01, 6 February 2018, pp. 15-16, 21; De Brauw Blackstone Westbroek (2018); McCreanor (2018); Maldoff (2016).
[1233] For a discussion, see Kuner (2020a). Although Kuner does conclude that the current framework is flexible enough for the times of pandemic, he also emphasises its limitations.
[1234] Reidenberg (1998), pp. 554-555.
[1235] *Ibid.*, pp. 555, 562-565, 568-576. Similar arguments also made by Lessig. See Lessig (1999).
[1236] Kuner (2013), p. 96. ('But technology could play a greater role in transborder data flow regulation than is now the case. ... Data controllers routinely configure information technology systems so as to regulate the transborder flow of data, and it is not uncommon for an international company to structure its IT system so that certain types of data may not be accessed by its employees outside a specific country or region'.)
[1237] *Ibid.*

Gürses and van Hoboken suggest that the question of information flows should be tackled at the level of the design and production of functionality, where some of the individual harms due to reidentification of data can be mitigated though privacy technologies, such as differential or pan-privacy.[1238] In addition, those authors note that certain privacy intrusive practices adopted by service providers can be leveraged by 'automated privacy support that allows users to evaluate which information flows they want to engage in and how they can control these when they use services.'[1239]

It should, of course, be acknowledged that technology is not a panacea to correct inefficiencies of the legal framework in governing transfers of personal data, but it could provide an effective complementary regime to mitigate those inefficiencies.[1240] In his 2009 OECD study, Schwartz demonstrated based on several case studies that cross-border transfers of data are 'not a finite event' and 'occur in a multi-directional fashion throughout the globe, and involve more companies and entities in the processing activities'.[1241] In other words, they 'occur as part of a networked series of processes made to deliver a business result.'[1242] The implication of this transformation is that regulating cross-border transfers of personal data based on the outdated views of information flows as point-to-point transfers is increasingly challenging, and is perhaps missing the forest for the trees. Technological tools in combination with data privacy industry standards could be more effective in tracing cross-border data flows and ensure that the legal regime for protection of personal data is not circumvented. The EU has already to some extent resorted to technological means in governing cross-border data flows in its adequacy decision for Japan. Because the adequacy decision creates – through Supplementary Rules – a higher level of data protection for data from the EEA in contrast to Japanese data, the Supplementary Rules require that Japanese business operators must 'ensure (e.g. by

---

[1238] Gürses, van Hoboken (2018), p. 597:

> If every form of digital functionality has the potential to be transformed into a data intensive machine learning product, the application of principles such as data minimization, purpose specification and policies that enforce some sort of control over data on the side of end-users is going to be challenging. At the same time, much of service capture creates prime opportunities to apply privacy technologies such as differential or pan privacy. The application of these techniques could protect users from individual harms due to reidentification of data.

[1239] Gürses, van Hoboken (2018), p. 597.

[1240] Kuner (2013), p. 99 ('The use of technology to regulate transborder data flows is not a panacea. Technological or 'code-based' solutions to regulatory problems can raise questions about democratic legitimacy and discrimination; for example, States can adopt national technical standards to disadvantage foreign providers, or mandate the use of domestic products. Procedures would thus have to be developed to ensure accountability and transparency in the implementation of technological solutions'.) See also Lessig (1999), at 138.

[1241] Schwartz (2009), pp. 12, 36.

[1242] *Ibid.*, Schwartz, p. 16.

technical ("tagging") or organisational means (storing in a dedicated database)) that they can identify such personal data throughout its "life cycle"'.[1243]

Implementing these ideas in Chapter V of the GDPR would add more scalability to the regime for transfers of personal data, facilitate and enhance enforcement of compliance with the framework.

5.4.3 Redesign

In the longer term, addressing all the weaknesses of the GDPR's Chapter V framework for transfers of personal data outside the EEA identified in Section 5.3 may require a much more thorough redesign. This redesign could grow organically out of improvements to the GDPR proposed as a part of the second line of thought. One way of doing so would be to replace the current one-size-fits-all approach, in which different mechanisms for transfers of personal data do not take into account the context and the parameters of the transfer, with rules designed on a *risk-based approach*.[1244] Ironically perhaps, such an approach to rules on transfers of personal data outside the EEA would fit much better into the logic of the GDPR, part of which already reflects a risk-based approach.[1245] In particular, this is the case in relation to some data protection elements explicitly or implicitly envisaged in Article 8 of the Charter, such as the legitimate interest that can be used as a legal ground for processing of personal data,[1246] the stricter rules for processing special categories of personal data,[1247] the principle of accountability,[1248] the provisions on records of processing activities,[1249] the data breach notification requirement,[1250]provisions on security of processing,[1251] the obligation of prior consultation with a data protection authority,[1252] and finally in the data protection impact assessment

[1243] Para. 15 Adequacy Decision for Japan.
[1244] For a discussion on the role of the concept of risk in the GDPR, see, e.g., Demetzou (2020).
[1245] It is, however, worth keeping in mind that the implementation of the risk-based approach in the GDPR is incomplete and is, arguably, in tension with the rights of the data subject envisaged in Chapter III GDPR. See, e.g., Quelle (2017b), pp. 20-21.
[1246] In its pre-GDPR but post EU Charter Opinion, Article 29 Working Party explicitly suggests to use the terminology and methodology of traditional risk assessment as a helpful tool to assess the impact of data processing on the individual. Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, 9 April 2014, pp. 37-38. Similarly, in its GDPR guidance on the application of legitimate interest, the UK Information Commissioner's Office (ICO) equates the legitimate interest assessment with a light-touch risk assessment based on the specific context and circumstances. INFORMATION COMMISSIONER'S OFFICE, *Legitimate interests*, https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests-1-0.pdf
[1247] Recital 51, Art. 9 GDPR.
[1248] Recitals 74-77, Arts. 24 GDPR.
[1249] Recital 82, Art. 30(5) GDPR.
[1250] Recitals 85 – 88, Arts 33-34 GDPR.
[1251] Recital 83, Art. 32 GDPR.
[1252] Recitals 94-96, Art. 36 GDPR.

process.[1253] This strongly suggests that a risk-based approach to data transfers would also feasible, and indeed arguably preferable.[1254]

In light of the *function* of the framework for restrictions on transfers of personal data based on the EU Charter, as discussed in the previous Sections of this Chapter, the main risk that the redesigned framework should address is the circumvention of the EU data protection regime when personal data are transferred abroad.[1255] In fundamental rights terms, this can be reformulated as the risk that transfers of personal data outside the EEA can interfere with the fundamental rights to privacy and the protection of personal data more than is strictly necessary and proportionate to pursue a legitimate public policy objective.

In an effort to improve Chapter V, safeguards required for transfers of personal data could be differentiated in the GDPR depending on the remoteness of link between personal data and individuals to which it relates or, in other words, the risk of reidentification (which can serve as a proxy for the risk to a particular individual from a data transfer, including where data is accessed by foreign surveillance authorities) and threat of harm.[1256] One could, for instance, use Ohm's non-exhaustive list of five factors for assessing the risk of privacy harms in general, and apply it to harms associated with transfers of personal data:[1257]

(1) data-handling techniques (risk of re-identification can be labelled as high, medium or low based on a rough relative ordering of different techniques that could potentially be developed by computer scientists[1258]);
(2) private versus public release (the level of protection of publicly released data should be higher than that of data shared between trusted parties due to higher privacy risks inherent in public release of data for privacy[1259]);
(3) quantity (larger volumes of data sets are more susceptible to reidentification through matching different data sets[1260]);

[1253] Recitals 84, 89, 90-93, 95, Art. 35 GDPR.
[1254] There is, however, some critique of this approach. See, in particular Quelle (2018); Quelle (2015); Quelle (2017b).
[1255] Kuner (2018), p. 872. See also Kuner (2013), pp. 107–113.
[1256] For a discussion on this approach to regulating privacy in general, see Ohm (2010), pp. 1761, 1764. Schwartz and Solove are critical of this approach as it requires ex ante cost-benefit assessment of information flows, which, in their view, is not only speculative in nature but may also amount to rejecting potentially beneficial collections and use of large data sets. Schwartz, Solove (2011) pp. 1868-1869.
[1257] Ohm (2010), pp. 1765-1768.
[1258] *Ibid*., p. 1765.
[1259] *Ibid*., p. 1766.
[1260] *Ibid*., pp. 1766-1767.

(4) motive (the legal constraints on sharing data, the motives of owners of data sets to share them as well as the economic incentives for reidentification also have an impact on the risk of reidentification.[1261]); and
(5) trust (society's trust in people and institutions in privacy regulatory framework[1262]).

In line with the first of those five factors, and incorporating the proposals made as a part of the second line of thought above, more lenient transfer rules could be designed for data that only has a remote link with individuals, such as pseudonymised data, when such data are transferred without additional information necessary to link the data to particular individuals. By definition, pseudonymised data cannot be attributed to a specific individual without the use of additional information, *provided* such information is kept separately and adequately protected.[1263] Beyond this, differentiation between the intensity of restrictions on transfers should not be solely or mostly based on the distinctions between different categories of data (such as sensitive data), because such distinctions are often highly contextual,[1264] which makes differentiation between such categories difficult in practice.[1265]

Several authors have emphasized that the data protection framework in general, and the framework for transfers of personal data in particular, should be focused on *harm* or effects on individuals of data processing (or data transfers).[1266] The risk of harm can also be captured by a risk-based approach. Kuner suggests, in relation to regulation of cross-border data flows, that focusing on the situations where cross-border data flows cause harm to individuals could be one way to improve the level of data protection compliance and enforcement.[1267] He also notes, however, that under EU law and the European Convention on Human Rights it is unclear how to define 'harm' in the context of cross-border data flows.[1268] Purtova argues that focusing on harm is generally in line with the case law of the CJEU.[1269]

Another factor that could be useful in designing an improved framework for cross border transfers of personal data based on risk-based approach is the *sector* in which the transfer of personal data occurs. For example, as one of the measures to increase availability of data for businesses, the European Commission has recently proposed to

[1261] *Ibid*., p. 1767.
[1262] *Ibid*., p. 1767.
[1263] Art. 4(5) GDPR.
[1264] Koops (2014), p. 260; Moerel (2020).
[1265] Purtova (2018), pp. 79, 80.
[1266] Koops (2014), p. 260; Kuner (2013), pp. 147-148; Purtova (2018), pp. 79, 80. For an overview of privacy harms, see e.g., Solove (2006).
[1267] Kuner (2013), pp. 147-148.
[1268] *Ibid*.
[1269] Purtova (2018), p. 62.

develop sectoral data spaces within the EU in strategic areas, such as manufacturing, agriculture, health and mobility.[1270] This approach could also be usefully explored for transfers of personal data outside the EEA.

5.5 Conclusion

This Chapter has demonstrated that the framework for transfers of personal data outside the EEA in Chapter V of the GDPR represents only *one* possible design of such a framework in the light of the EU Charter requirements. Only the presence of *some* restrictions and a few aspects of such restrictions constitute the essence of the fundamental rights to privacy, the protection of personal data and the right to judicial remedy (in the context of the first two rights) and, therefore, cannot be altered by EU secondary law. Other elements of such a framework can be determined by the EU secondary legislator on the basis of strict necessity and proportionality assessment, with the aim of ensuring its constitutional function, which is to prevent circumvention of the high level of personal data protection in the EU. Section 5.3 of this Chapter has shed light on several weaknesses of the current framework's elements and overall design, and argued that due to economic, political, geopolitical and legal changes, this framework is no longer actually fit for its constitutional purpose. To ameliorate these weaknesses within the boundaries set by the EU Charter, this Chapter has proposed three paths to how to improve this framework, corresponding to a short, medium,-and long term strategy for the EU.

[1270] 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, A European Strategy for Data, COM(2020) 66 final, 19 February 2020, p.6.