WHAT IS EQUIVALENT? A PROBE INTO GDPR ADEQUACY BASED ON EU FUNDAMENTAL RIGHTS

Laura Drechsler

Laura Drechsler, doctoral researcher (FWO aspirant), Brussels Privacy Hub, LSTS, Vrije Universiteit Brussel
Pleinlaan 2, 1050 Brussels, BE
laura.drechsler@vub.be
https://www.vub.ac.be/LSTS/members/drechsler/

Keywords: ***Adequacy, Fundamental Rights, Data Protection, Privacy Shield, Japan Adequacy, GDPR***

Abstract: *In July 2018, the European Parliament questioned the validity of the Privacy Shield, regulating the transfer of personal data to the United States (US). This event shows a persistent lack of clarity regarding the conditions a third country needs to fulfil to be considered adequate from the perspective of the General Data Protection Regulation (GDPR). This paper tries to clarify these conditions by analysing the standard of equivalence that was put forward by the Court of Justice of the European Union (CJEU) in the Schrems case and Opinion 1/15 together with the Charter of Fundamental Rights of the European Union (CFR) and the new provisions on data transfers by the GDPR. Applying the results of this analysis back on the Privacy Shield and the Draft Japan adequacy decision demonstrates that an analysis for adequacy firmly grounded in the CFR is still not being done in practice.*

1. Introduction[1]

In July 2018, the European Parliament (EP) passed a resolution stating that the Privacy Shield,[2] the adequacy decision authorising transfers of personal data to the US, did not protect personal data sufficiently. The EP's criticism was largely driven by revelations surrounding illicit data transfers and processing at Cambridge Analytica and Facebook (both certified under the Privacy Shield).[3] The resolution put forward a deadline for the European Commission (EC) to suspend all transfers under the Shield should its flaws not be fixed until 1 September 2018. Similar remarks were made by the Article 29 Working Party (WP29), who in its opinion on the first annual review, also urged the EC to suspend the Shield if there is no improved compliance of some key provisions by October 2018.[4] At the same time, the freshly adopted draft for an adequacy decision on Japan

[1] This research forms part of the Ph.D. project of the author, for which she receives funding from the FWO (1165319N). The author would like to thank her supervisors Christopher Kuner and Gloria González Fuster (both VUB) for their comments on this research.

[2] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ 2016 L 207/1.

[3] European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield (2018/2645(RSP)), P8_TA-PROV(2018)0315, p. 7.

[4] Article 29 Working Party, *EU – U.S. Privacy Shield – First annual Joint Review* (28 November 2017), p. 4. In October 2018 the second annual review of the Shield took place. The final report does not recommend any immediate suspension (it threatened in case a permanent Ombudsperson is not appointed). See European Commission, *Report on the second annual review of the functioning of the EU-U.S. Privacy Shield* (19 December 2018), pp. 5-6. See further the more detailed staff document, explicitly mentioning the EP resolution as main source: European Commission, *Commission Staff Working Document on the second annual review of the functioning of the EU-U.S. Privacy Shield* (19 December 2018), p. 3.

faced heavy scrutiny by the European Data Protection Board (EDPB), also revealing disagreement with the EC on how to assess adequacy.[5]

The *Schrems* case set forward the condition that a third country must be «*essentially equivalent*» compared to the system of fundamental rights protection within the CFR to be considered adequate.[6] The GDPR,[7] and the CJEU[8] have tried to further clarify this standard of essential equivalence. However, a clear definition has not emerged. This contribution therefore tries to propose a definition for the standard of equivalence for GDPR adequacy decisions and an outline how to ensure that an adequacy assessment is based on the CFR.[9]

2. The adequacy process of the GDPR

Art. 44 GDPR lays down the principle that data transfers can only take place if the GDPR is complied with, meaning that in general the GDPR restricts such transfers, unless its conditions are fulfilled. The goal of these rules is to ensure that the level of protection provided in the GDPR is not undermined.[10] The GDPR offers three venues for transfers, adequacy decisions (Art. 45), appropriate safeguards (Arts. 46 and 47) and derogations (Art. 49).[11] This paper focuses solely on adequacy decisions.

Adequacy decisions have to be taken by the EC. They can concern a whole third country, a territory of it, a specified sector within it or an international organisation. The GDPR provides a list of elements the EC has to consider in Art. 45(2) GDPR, which include respect for fundamental rights (Art. 45(2)(a)), independent supervisory authorities (Art. 45(2)(b)), and international commitments to data protection (Art. 45(2)(c)). All 12 adequacy decisions made under the Data Protection Directive (DPD) remain valid until replaced (Art. 45(9)).[12] Rec. 104 states that adequacy means that a third country has «an adequate level of protection essentially equivalent to that ensured within the Union», this standard of equivalence was developed by the CJEU in *Schrems* (see next section).

3. The standard of equivalence as defined by the CJEU in Schrems

The CJEU decision in *Schrems* clarified some aspects about the content of adequacy and put forward the standard of essential equivalence for transfers. The case was based on the complaint of an Austrian law student Maximillian Schrems questioning whether his data with Facebook, where he had created a profile, was protec-

---

5 See Draft Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan. See further European Data Protection Board, *Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan* (5 December 2018).

6 Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650, para. 73.

7 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

8 For example in: Case Opinion 1/15 *Opinion pursuant to Art 218(11) TFEU* [2017] ECLI:EU:C:2017:592.

9 Charter of Fundamental Rights of the European Union, OJ 2010 C 83/389.

10 See Art. 44 GDPR. For a general critique on the concept of «transferring personal data», when in reality there is no defined movement but rather a copying of the data to elsewhere, see; González Fuster, «Un-Mapping Personal Data Transfers», 2 *European Data Protection Law Review* (2016), pp. 161-162; 166. See for an explanation of different policy goals of data transfer regulation: Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013), pp. 101-120.

11 The predecessors of these rules can be found in Arts. 26(1) and (2) DPD. For an overview the GDPR transfer mechanism, see: Voigt and von dem Bussche, *The EU General Data Protection Regulation (GDPR) – A practical guide* (Springer 2017), p. 116-133. See also: Kuner, Article 44, in Kuner, Bygrave and Docksey (eds.), *Draft commentaries on 10 GDPR Articles (from Commentary on the EU General Data Protection Regulation, OUP 2019)* (2018), available at http://works.bepress.com/christopher-kuner/1/.

12 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31. The adequacy decisions concern: Andorra; Argentina; Canada (only for commercial organisations); Faroe Islands; Guernsey; Israel; Isle of Man; Jersey; New Zealand; Switzerland; Uruguay; United States (for the companies enrolled in the Privacy Shield). The adequacy decision for Japan is undergoing ratification. Negotiations are ongoing for an adequacy decision for South Korea.

ted in a way that satisfied EU data protection law. He doubted such protection since his data was likely being transferred to the Facebook headquarters in the US, where considering the Snowdon revelations,[13] unlimited access by US intelligence agencies seemed probable. As the CJEU summarised, Schrems challenged the Safe Harbour Principles,[14] that pronounced the US system adequate for certain transfers.[15]

In its decision, the CJEU declared the Safe Harbour Principles invalid, forcing the EC to undergo a new adequacy process with the US, which resulted in the Privacy Shield. The most important finding the CJEU made on adequacy is that it set a high standard for a third country to reach it, the «standard of essential equivalence»: «*[T]he term ‹adequate level of protection› must be understood 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*».[16] With this, the CJEU arguably puts forward at least three conditions for an adequacy decision:[17] a result-driven assessment, a level of protection of fundamental rights in the third country similar to the CFR and need for a detailed assessment of domestic law and international commitments.

The CJEU proscribes a result-driven assessment by its contradictory statement, that a foreign country does not need identical protection but essential equivalent protection of fundamental rights. As «identical» is often considered a synonym for «equivalent»,[18] «identical» has to be interpreted as referring to identical legislative tools, while «equivalent» must then mean achieving the same result potentially using other means.[19] Such an interpretation is supported by the CJEU assertion that the means for achieving essential equivalence might differ as long as they prove to be effective in practice.[20]

A second step is to define the result that needs to be achieved with said result-driven assessment. According to the CJEU, the result needs to be «*a level of protection of fundamental rights and freedoms (...) essentially equivalent to (...) Directive 95/46 read in light of the Charter*». In this authors opinion, the CJEU is trying to assert, that first, the relevant source for EU fundamental rights is the CFR and secondly, not all fundamental rights of the CFR are relevant for the adequacy assessment, but only those that can be sufficiently linked to EU data protection legislation (then the DPD).[21] The use of the plural for fundamental rights by the CJEU is intentional. It is not «just» the right of data protection or «just» the right of privacy of the CFR that need to be considered, but all fundamental rights that can be linked to data protection.[22]

---

13 For more information on the «Snowdon revelations», see: The Guardian, «NSA Files: Decoded – What the revelations mean for you» (1 November 2013), available at https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1. See also European Commission, *Communication: Rebuilding Trust in EU-US Data Flows* (27 November 2013) and European Commission, *Communication on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU* (27 November 2013).

14 Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ 2000 L 215/7. For a detailed explanation on how Safe Harbour functioned and what its main flaws were, see: Dhont et al., «Safe Harbour Implementation Study» (19 April 2004).

15 *Schrems*, supra, note 6, para. 67.

16 Ibid., para 73.

17 Compare to Kuner, who puts forward 8 conditions that the CJEU establishes in Schrems. See Kuner, «Reality and Illusion in EU Data Transfer Regulation Post Schrems», 18(4) *German Law Journal* (2017), pp. 899-900.

18 At least according to Theasaurus.com. See Thesaurus, «equivalent», available at https://www.thesaurus.com/browse/equivalent?s=t.

19 See a similar conclusion by Kuner in: Kuner, supra, note 17, p. 902.

20 *Schrems*, supra, note 6, para. 74. This interpretation also hints at the CJEU essentially requiring a functional comparative analysis to be conducted for an adequacy decision. For more information on legal functional comparison, see Husa, *A New Introduction to Comparative Law* (Hart Publishing, 2015), p. 118ff.

21 See Brkan, «The Unstoppable Expansion of the EU Fundamental Right to Data Protection», 23(5) *Maastricht Journal of European and Comparative Law* (2016), p. 829.

22 Compare to Kuner, who concludes that the CJEU wanted to highlight that the standard is comprised of the data protection standards set by the CFR. See Kuner, supra, note 17, p. 902.

The final part of the CJEU's conditions for adequacy states that adequacy must be guaranteed by «domestic law or international commitments». This part served as the main argument for the CJEU in *Schrems* to invalidate Safe Harbour.[23] This condition sets forth the requirement to sufficiently look at the domestic law and international commitments of the third country being assessed. Judging from the criticism on Safe Harbour in *Schrems*, it should include a fairly complete listing of relevant legislation including an explanation how they apply in practice. It also includes to a certain extent, an obligation of the third country to report on relevant legislative developments.[24]

4. Assessing GDPR adequacy according to the standard of equivalence

The standard of equivalence established in *Schrems*, does not include details on how such an adequacy assessment should take place. This is partly justified, since it is a result-orientated analysis, an exact procedure for adequacy would only leave little room for different means to achieve the necessary fundamental rights protection.[25] However, since the result of essential equivalence should be a high protection of fundamental rights, those fundamental rights themselves require that the adequacy process includes certain elements. After analysing the GDPR, EU fundamental rights law and *Opinion 1/15*, this author puts forward that the CFR requires the GDPR adequacy assessment to include three elements to anchor it within the EU fundamental rights system: an identification of the fundamental right(s) at stake in an adequacy decision, linking these fundamental rights to data protection with analysis of the additional elements of Art. 8 (meaning Arts. 8(2) and (3) CFR)),[26] and finally an analysis of the adequacy decision as limitation to the previous identified fundamental right.[27] These elements should form the starting point for every GDPR adequacy assessment, from which then additional elements can be explored.

In this context, it is important to note that the WP29 has put forward its own guidelines on how to assess adequacy (since then confirmed by the EDPB) and essential guarantees for access by the public sector in a third country.[28] In its opinion on the draft adequacy decision for Japan, the EDPB follows these documents for its assessment.[29] While the guidance of the WP29 includes useful (additional) elements that should be considered, it is this authors opinion that it prescribes a too rigid list of factors to fulfil the *Schrems* requirement of «equivalent» but not «identical», while at the same time not being rooted firmly enough in the different fundamental rights protected in the CFR and the EU data protection instruments (which, as will be explained shortly, are more than data protection and privacy). Hence, the proposed approach will differ in its starting point from the one put forward by the WP29/EDPB.

---

23 *Schrems*, supra, note 6, para 97.

24 Ibid., para 96. See further: European Data Protection Supervisor, *Opinion 4/2016. Opinion on the EU-U.S. Privacy Shield draft adequacy decision* (30 May 2016), p. 11. Article 29 Working Party, *Opinion 01/2016 on the EU U.S. Privacy Shield draft adequacy decision* (13 April 2016), p. 2. For Kuner such an obligation is linked to an admittance by the CJEU, that it might need to review foreign legal standards in such cases. See: Kuner, «International agreements, data protection and EU fundamental rights on the international stage: Opinion 1/15, *EU-Canada PNR*», 55(3) *Common Market Law Review* (2018), 880. See also the criticism of the EC in its first annual review of the Shield, that the US failed to alert it to relevant new legislative actions. European Commission, *Report on the first annual review of the functioning of the EU-U.S. Privacy Shield* (18 October 2017), p. 7.

25 This would run counter to *Schrems*, where it is explicitly stated that the means of protection do not need to be identical to the ones in the EU. See *Schrems*, supra note 6, para. 74.

26 These elements are the principles of fairness, legitimate processing and purpose limitation, the data subject rights of access and rectification (Art. 8(2) CFR) and the need for an independent supervision (Art. 8(3) CFR).

27 As was done in *Opinion 1/15*, see: *Opinion 1/15*, supra, note 8, para. 124.

28 See Article 29 Working Party, *Adequacy Referential* (updated), (2017). 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),* (2016). European Data Protection Board, *Endorsement 1/2018*, (25 May 2018), at (15).

29 EDPB, Opinion 28/2018, supra, note 5, p. 5.

The first element required by EU fundamental rights law of a GDPR adequacy assessment is an identification which fundamental rights are protected within it. As indicated, the GDPR transfer provisions do not serve only the fundamental rights of privacy and data protection.[30] The CJEU, when defining the standard of equivalence in *Schrems*, did not limit it to the fundamental rights of Arts. 7 and 8 CFR by listing only them.[31] Both *Schrems* and *Opinion 1/15* considered more fundamental rights in addition, namely the right to an effective remedy and to non-discrimination.[32] Within the GDPR, such an approach is supported by Art. 45(2)(a), which prescribes «respect for human rights and fundamental freedoms», as an element to take into account for an adequacy assessment, also not limiting the analysis to privacy and data protection. The identification of the fundamental rights to consider can differ depending on the EU data protection instrument forming the basis of the adequacy decision. For the GDPR, the following rights can be identified in addition to Arts. 7 and 8 CFR: effective judicial remedy,[33] freedom of expression,[34] and non-discrimination.[35]

Secondly, the additional elements of Arts. 8(2) and (3) CFR have to be assessed as they provide the core elements of EU data protection. Considering that *Schrems* includes in essential equivalence only those fundamental rights expressed in the DPD, all fundamental rights identified must sufficiently be linked to data protection, hence aid these core elements. It is argued by the author that the assessment is therefore always whether X identified fundamental right in connection with Arts. 8(2) and (3) CFR is sufficiently achieved in the third country, thus specifying identified rights for a data protection context. Arguably, this would make Arts. 8(2) and (3) fundamental rights that (probably always) come into effect only in combination with other fundamental rights.[36]

As an argument for this interpretation, one can consider the way the CJEU treated the data subject rights of access and rectification in *Schrems*. Both of those data subject rights are listed in Art. 8(2) CFR and hence core EU data protection elements. The CJEU however found that a non-existence of those rights constituted a breach of the essence of Art. 47 CFR (right to an effective remedy).[37] It would have been more logical if that finding was a breach of Art. 47 in connection with Art. 8(2) CFR, since if the non-existence of those two core elements of Art. 8(2) is not a breach of Art. 8(2), what is? Additionally, this would have linked Art. 47 more concretely to the data protection context. A further argument for this interpretation can be found in *Opinion 1/15*, where the CJEU after having analysed a potential limitation of Arts. 7 and 8 CFR, makes two additional analysis before its conclusions, namely which rights where available for air passengers, including the right of access and rectification but also judicial redress (Art. 8(2) in conjunction with Art. 47 CFR) and on

---

30 See in this regard, rec. 1 of the EP Resolution of 5 July 2018, supra, note 2, which lists Arts. 6, 7, 8, 11, 16, 47 and 52 CFR as rights to be considered. As González Fuster explains, the original French idea of data protection was as a means to protect all fundamental rights from the risks of new technologies, especially those posed by computers. See González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014), p. 63.

31 *Schrems*, supra, note 6, para. 73. See also the Opinion of Advocate General Bot, in Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:627, para. 140, who sees adequacy as a tool for a high level of protection of privacy (though he mentions other fundamental rights later).

32 *Schrems*, supra, note 6, para. 95. *Opinion 1/15*, supra, note 8, para 165.

33 See Arts. 77-79 GDPR granting the data subject remedies against and with supervisory authorities, as well as judicial remedies. See further Art. 47 CFR. See also *Schrems*, supra, note 6, para. 95.

34 See Art. 85 GDPR, guiding the balancing between freedom of expression. See further Art. 11 CFR. See also Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* [2016] ECLI:EU:C:2016:970, para. 102. Case C-73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008] ECLI:EU:C:2008:727.

35 See further Art. 22 GDPR, trying to protect from discriminatory risks in the context of automated decision-making by introducing safeguards. See further Art. 21 CFR. See also *Opinion 1/15*, supra, note 8, para. 165.

36 This can be compared to Arts. 13 and 14 ECHR, which only come into effect if another Convention right is violation. See: «European Convention on Human Rights, as amended by Protocol Nos. 11 and 14, supplemented by Protocols Nos. 1, 4, 6, 7, 12 and 13» [1950], ETS 5.

37 *Schrems,* supra, note 6, para 95.

the independence of supervision by the Canadian authorities (Art. 8(3) in connection with Arts. 8(1) and 7).[38] These additional assessments are part of the whole assessment for compatibility with the fundamental rights of Arts. 7 and 8 CFR, as only afterwards does the CJEU make its final conclusion.

Hence, the existence of the data subject rights of access and rectification, legitimate grounds for processing, and purpose limitation (Art. 8(2)) and the existence of independent institutional supervision (Art. 8(3)) are to be assessed in connection with each identified fundamental right to link them to the data protection context as necessary under the standard of equivalence. For fundamental rights other than data protection or privacy, this assessment might be limited to asking whether for example in a journalistic context (freedom of expression), the rights of access and rectification are made possible as far as feasible. Regarding the supervisory authority, the assessment could be whether the mandate and competence of the authority is sufficiently broad to also deal with issues of freedom of expression or non-discrimination.

Finally, once the fundamental rights at stake have been identified and linked to data protection, the data transfer authorised by the potential adequacy decision, must be considered an interference with those fundamental rights. Since *Opinion 1/15*, it is clear that transferring personal data is always an interference with fundamental rights.[39] While the CJEU only mentions Art. 7 CFR in *Opinion 1/15*, this can arguably extended to all fundamental rights protected within EU data protection legislation, as they all can be potentially undermined by a transfer of the personal data to a third country. As the adequacy decision is hence an interference (limitation) to EU fundamental rights, Art. 52(1) CFR, setting forward justifications of such a limitation, applies and needs to be assessed separately for each identified fundamental right. This requires an assessment if the essence of the identified right has been breached, whether the limitation comes in the form of law and serves objectives of general interest recognised by the EU, and whether the interference is proportional to these objectives.

5. Conclusions for transatlantic data transfers and transfers to Japan

After having proposed a definition for the standard of equivalence and outlined the starting point of an adequacy assessment, this section will shortly apply them to the Privacy Shield and the draft adequacy decision regarding Japan.

Regarding the identification of fundamental rights at stake, the Privacy Shield explicitly mentions Arts. 7 and 8 CFR,[40] while the draft Japan adequacy decision mentions no specific CFR provisions, but notes that «substance of privacy rights» is relevant for adequacy.[41] Both decisions show that the EC did not consider essential equivalence as including all fundamental rights. This can also be concluded from the fact, that in both decisions a provision to protect non-discrimination is lacking. *Opinion 1/15* states that the right to non-discrimination within a data protection context, would require a comparable provision to Art. 22 GDPR (protection from discriminatory automated decisions).[42] As is pointed out by the EDPS, WP29 and EDPB, no such provision is to be found in the Shield or the draft Japan adequacy decision.[43]

---

38 *Opinion 1/15*, supra, note 8, «The individual rights of air passengers», paras. 218-227; «Oversight of PNR data protection safeguards», paras. 228-231.

39 Ibid., supra, note 8, para. 124.

40 Rec. 3 Privacy Shield, supra, note 2. Compare to the Safe Harbour Principles, which only mentioned privacy: Safe Harbour Principles, supra, note 14, Annex I, p. 10.

41 Draft Japan adequacy decision, supra, note 5, rec. 3.

42 See *Opinion 1/15*, supra, note 8, para. 165.

43 See WP29, Opinion 01/2016, supra, note 24, p. 3. See also: EDPS, Opinion 4/2016, supra, note 24, pp. 9-10. The EC admitted that this might be a potential issue for the Shield and promised a study on the issues of automatic decision-making in its 1st annual review of the Shield. See: EC, Report 2017, supra, note 24, p. 6. For Japan see: EDPB, Opinion 28/2018, supra, note 5, pp. 21-22. Interestingly, while the EC was originally concerned about this absence, it includes in its 2nd review of the Shield, that there was no real risk, since hardly any automated decisions are being made on basis of EU data transferred under the Shield. See EC, Working Document 2018, supra, note 4, pp. 19-22.

Turning to the second element, fulfilment of the additional requirements of Arts. 8(2) and 8(3) CFR in conjunction with the fundamental right at issue to link them to a data protection context, the EDPS notes for the Shield an issue with independent oversight (Art. 8(3)) of intelligence bodies, as non-US citizens have a different protection than US citizens. This could be seen as an issue of Art. 7 in conjunction with Art. 8(3) CFR. In a similar vein, the WP29 doubts the independence of the Ombudsperson for intelligence activities, suggesting another necessary analysis of Arts. 7 and 8(3) combined.[44] In addition, the EDPS criticises a lack of analysis regarding the effective exercise of data subject rights in a non-surveillance context, leading to a potential issue with Art. 47 in conjunction with Art. 8(2).[45] Similar concerns (though to a lesser extent) with oversight and effective remedies are noted by the EDPB for Japan.[46] While these examples should not suggest any in-depth assessment into these claims, they can demonstrate that even though the EU data protection institutions do not explicitly state that they are assessing adequacy decisions for the elements of Arts. 8(2) and (3), they arguably do so in practice.

The final element, whether the interference these adequacy decisions pose to fundamental rights, can be justified under Art. 52(1) CFR, requires a complex analysis that cannot be made in the limited confines of this paper. Instead the most forceful of the limitation elements shall be shortly highlighted – a potential breach of essence of a fundamental right. If such a breach is found a justification of the limitation of a fundamental right is not possible, hence the assessment can conclude.[47] Regarding the essence of a fundamental right, *Schrems* is one of the two CJEU cases actually finding a breach (really breaches) of essence,[48] namely of Art. 7 through the access to content of electronic communications with a lack of safeguards, and of Art. 47 by giving no legal remedies for access or rectification to the data subject.[49] Both of those issues seem insufficiently addressed within the Shield. As the EP points out, access by US intelligence services continues to take place and supervision is unclear and/or lacks the personnel,[50] suggesting still a breach of essence of Art. 7 CFR, especially in light of the recent judgment of the European Court of Human Rights (ECtHR) in *Big Brother*.[51] Regarding the essence breach of Art. 47 CFR, while the Shield provides more remedies, a full equivalence with GDPR data subject rights seems to be lacking. The right of access for example, seems to be restricted to information stored within a company.[52] For the Japan adequacy decision, the EDPB considers that access by public authorities for national security purposes is theoretically restricted and there exist oversight mechanism with individual redress opportunities, however, it is not clear how those work and are effective in practice. In any case, comparing the situation to the one in *Schrems*, there seems to be enough theoretical possibilities to argue that no breach of essence has occurred, though the interference might still not be justified under Art. 52(1) CFR.[53]

6. Final remarks

As a conclusion, this author puts forward that the standard of equivalence for EU adequacy decisions needs to be firmer linked to the fundamental rights of the CFR. So far, the EC has tried to assess adequacy without a

44 EDPS, Opinion 4/2016, supra, note 24, p. 8. WP29, Opinion 01/2016, supra, note 24, p. 4. The EC also found issues with the Ombudsperson, but of a different nature, criticizing, that such a person has not been permanently appointed yet, see: EC, Report 2017, supra, note 24, p. 4. This remains an issue, see EC, Report 2018, supra, note 4, pp. 5-6.

45 See EDPS, Opinion 4/2016, supra, note 24, p. 11.

46 See EDPB, Opinion 28/2018, supra, note 5, pp. 22-24.

47 Brkan, «The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core», 14(2) *European Constitutional Law Review* (2018), p. 333.

48 Ibid., p. 337.

49 *Schrems*, supra, note 6, para. 94-95.

50 EP Resolution of 5 July 2018, supra, note 3, at (20)-(30). See also WP29, First annual joint review, supra, note 4, pp. 14-17.

51 *Big Brother Watch and others v. The United Kingdom* App nos. 58170/13, 62322/14 and 24960/15 (ECtHR, 13 September 2018).

52 WP29, First annual joint review, supra, note 5, p. 8.

53 Compare a similar conclusion in *Opinion 1/15*, supra, note 8, para. 151.

clear basis in EU fundamental rights law.[54] Transatlantic transfers show that an assessment of data transfers as a limitation to fundamental rights is lacking. Merely reworking Safe Harbour, as the EC did with the Privacy Shield,[55] cannot lead to a result that ensures essential equivalence. Judging from the latest draft adequacy decision concerning Japan, an in-depth analysis regarding fundamental rights is still not being conducted. As a solution, the author proposes an assessment anchored in the test for a limitation of a fundamental rights laid down by the CJEU and in the CFR that would be capable of producing results of essential equivalence.

[54] Compare: Article 29 Working Party, *Adequacy Referential* (updated), (2017); European Commission, *Communication: Transatlantic Data Flows: Restoring Trust through Strong Safeguards* (29 February 2016); and *Opinion 1/15*, supra, note 8.

[55] This argument is put forward for example by the EDPS, see: EDPS, *Opinion 4/2016*, supra, note 24, p. 6.