A *certain* standard of protection for international transfers of personal data under the GDPR

Zuzanna Gulczyńska

Introduction

The General Data Protection Regulation[1] ('GDPR') uses not less than six different expressions to describe the standard(s) of protection required for international transfers of data, *i.e.* the transfers of personal data to third countries or international organizations.[2] The one that recurs most often is the *adequate* level of protection requirement.[3] However, in provisions other than Article 45 GDPR (governing international transfers on the basis of the Commission's adequacy decisions), also notions such as *appropriate* safeguards,[4] *appropriate* level of protection[5] and *suitable* safeguards[6] appear. Recital 104 GDPR, in its turn, refers to *essentially equivalent* level of protection. On top of that, Article 44 GDPR on the general principle for transfers, specifies that '[a]ll provisions in [Chapter V GDPR on transfers of personal data to third countries or international organization] shall be applied in order to ensure that *the level of protection of natural persons guaranteed by this Regulation* is *not undermined'*.[7]

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119 ('GDPR').
[2] Governed by Chapter V GDPR.
[3] See in particular Recitals 103, 104, 107, 168, 169 and Art. 45 GDPR.
[4] See in particular Recitals 102, 107, 108, 110 and Art. 13(1)(f), 14(1)(f), 15(2), 40, 41(4), 42(2), 46, 50 GDPR. See also the referral to the concept of appropriate safeguards in the context of other – non-related to transfers – provisions: Recital 50, 56, 62, 156, 157 and Art. 6(4)(e), 9(2)(d), 10, 58(4), 87, 89 GDPR.
[5] See Recital 102 GDPR.
[6] See in particular Recital 113 and Art.13(1)(f), 14(1)(f), 30(1)(e), 30(2)(c), 49 GDPR. See also the referral to the concept of suitable safeguards in the context of other – non-related to transfers – provisions: Recitals 52, 71 GDPR.
[7] Emphasis added. It is worth noting that there are some discrepancies amongst different language versions of the GDPR, *e.g.*, whereas the French version also distinguishes 6 notions to describe the level of protection required for international transfers of data, they do not align with the English terms. The analysis of all language versions of the GDPR exceeds the scope of the present contribution, but some flagrant discrepancies existing between various language versions of the Regulation will be indicated where relevant.

The maze of different concepts referring to the standard(s) of protection required for international transfers of data has been addressed by the Court of Justice of the European Union ('CJEU' or 'Court') in three cases: *Schrems I*,[8] *Schrems II*,[9] as well as *Opinion 1/15*.[10] Amongst these cases, the recent *Schrems II* judgment is particularly important, as it is the first one that directly addressed the question of the standard of protection required for international transfers of data under the GDPR. Indeed, *Schrems I* was issued in the context of the Data Protection Directive ('DPD')[11] but the GDPR expanded the legal bases for transfers[12] and – as pointed out in the previous paragraph – included several different notions relating to the standard(s) required for each of them. In *Schrems II,* the Court shed light on the relationship between these different bases and notions and considered that the same level of protection – *i.e.*, the level of protection essentially equivalent to the one guaranteed by the GDPR[13] – is required 'irrespective of the provision of [Chapter V GDPR] on the basis of which a transfer of personal data to a third country is carried out'.[14]

The Court's finding evokes mixed feelings. On the one hand, it pronounces loud and clear that there is one standard of protection that all international transfers must meet, thereby presumably introducing a simple and clear answer to the questions unanswered by *Schrems I*.[15]

---

[8] *Schrems v. Data Protection Commissioner,* Case C-362/14, [2015] EU:C:2015:650 ('*Schrems I*').
[9] *Data Protection Commissioner* v. *Facebook Ireland and Schrems,* Case C-311/18, [2020] EU:C:2020:559 ('*Schrems II*').
[10] *EU-Canada PNR Agreement,* Opinion 1/15, [2017] EU:C:2017:592 ('*Opinion 1/15*'). Even though *Opinion 1/15* concerned transfers of personal data based on an international agreement and not the provisions of the EU secondary legislation, the Court has addressed the concept of an adequate level of protection.
[11] 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 ('DPD').
[12] Next to the transfers based on adequacy decisions, the GDPR foresees a possibility to transfer data subject to appropriate safeguards in various forms (Art. 46 GDPR). For more details on that see Section II below.
[13] *Schrems II,* at para. 96.
[14] *Schrems II,* at para. 92.
[15] In *Schrems I,* the Court limited itself to invalidating the Commission's adequacy decision based not on the alleged inadequacy of the U.S. data protection guarantees, but the simple fact that the Commission's decision did not even state that the U.S. offered an adequate level of protection. Therefore, both the question concerning the substantial requirements for the achievement of an essentially equivalent standard of protection as the one related to the level of protection required for transfers carried out on other legal bases than the adequacy decisions remained unanswered.

On the other hand, however, a closer analysis of the legal and jurisprudential evolution from the DPD to the GDPR and from *Schrems I* to *Schrems II* reveals that *Schrems II*'s clarity is only apparent. In reality, in equating the notions of essentially equivalent level of protection, adequate level of protection and appropriate safeguards, the Court has performed complicated legal gymnastics which has raised new questions and doubts. Notably, it calls into question one of the crucial interpretative directives of EU law, according to which the EU legislator is a reasonable actor who creates rules that are consistent and complete, in particular avoiding duplications.[16] This rule of interpretation requires, amongst others, to assume that (within one instrument) different terms do not have the same meaning and conversely that one term cannot have two different meanings.[17] Such interpretative premise ensures the respect of the principle of legal certainty and is one of the requirements in the systems based on the rule of law.[18] The *Schrems II* finding that a single standard of protection essentially equivalent to that which is guaranteed within the EU applies irrespective of the provision of Chapter V GDPR relied on is not only difficult to reconcile with this principle, but also – taken a great variety of requirements and elements to be taken into account present in Chapter V GDPR – makes it difficult to understand what the standard of protection required by it concretely entails.

[16] Koen Lenaerts and José A. Gutiérrez-Fons,'To say what the law of the EU is: methods of interpretation and the European Court of Justice' [2013] 9 *EUI Working Papers AEL*, 13. See also Michal Bobek, 'Reasonableness in Administrative Law: A comparative reflection on functional equivalence', in Giorgio Bongiovanni, Giovanni Sartor, Chiara Valentini (eds), *Reasonableness and Law* (Springer 2008) 312 and the references cited therein. According to Bobek, '[a] generally shared principle going well beyond the English rules of constructing statutes is the rule against absurdity, *i.e.*, the presumption of a reasonable legislator, who did not wish to achieve absurd results'.

[17] See *e.g.*, *Hässle,* Case C-127/00, [2003] EU:C:2003:661, at para. 57; *Parliament v Council,* Case C-414/04, [2006] EU:C:2006:742, at para. 32; *UGT-FSP,* Case C-151/09, [2010] EU:C:2010:452, at para. 36 ; *Unomedical*, Case C-152/10, [2011] EU:C:2011:402, at paras 29-34; *Delphi Deutschland,* Case C-423/10, [2011] EU:C:2011:315, at para. 26; *ADL,* Case C-546/13, [2014] EU:C:2014:2348, at para. 41; *Planta Tabak,* Case C-220/17, [2019] EU:C:2019:76*,* at para. 67; see also Lenaerts and Gutiérrez-Fons, *op.cit.,* 14; Giulio Itzcovich, 'The Interpretation of Community Law by the European Court of Justice' [2009] 10(5) German Law Journal 537, 552.

[18] See Armin von Bogdandy and Michael Ioannidis, 'Systemic deficiency in the rule of law: What it is, what has been done, what can be done' [2014] 51(1) CML Rev 59; Takis Tridimas, *The General Principles of EU Law* (2nd ed. OUP 2006) 4-7.

According to the established case law of the CJEU, 'rules of law [should] be clear and precise and predictable in their effect, so that interested parties can ascertain their position in situations and legal relationships governed by EU law'.[19] Admittedly, the principle of legal certainty does not demand an unattainable semantic precision.[20] It does, nevertheless, require legal provisions to be clear enough to be capable of guiding individual behaviour and this in particular in the case of rules liable to entail financial consequences,[21] as is the case of the GDPR. However, in the post-*Schrems II* reality, despite establishing a single standard of protection for all international transfers, it remains unclear what the substantial content of the standard actually is.

The collision between the rules governing international transfers of data and the principle of legal certainty could be explained by the position that the data protection holds in the EU legal system as a fundamental right. This line of argumentation recurs in *Schrems I, Opinion 1/15* and *Schrems II*, which all use the need to ensure the protection of the fundamental right to data protection as a justification for the interpretation favouring an extensive application of the EU rules, also in the international context. However, it is questionable whether it is truly necessary to safeguard the EU fundamental right to data protection by sacrificing the principle of legal certainty. The contrary can be claimed, as overlooking the need for the legal certainty can disserve the ultimate goal of achieving a high level of data protection worldwide.

[19] *GRDF,* Case C-236/18, [2019] EU:C:2019:1120, at para. 42 and the case law cited therein. See also Jérémie Van Meerbeeck, 'The Principle of Legal Certainty in the Case Law of the European Court of Justice: From Certainty to Trust', (2016) 41(2) EL Rev 275.

[20] Elina Paunio, *Legal Certainty in Multilingual EU Law: Discourse and Reasoning at the European Court of Justice* (Ashgate 2013) 5-50 cited in: Pablo Martin Rodríguez, 'The principle of legal certainty and the limits to the applicability of EU law' [2016] 52(1) Cahiers de Droit Européen 115, 117; Luis Miguel Poiares Pessoa Maduro, 'Interpreting European Law: Judicial Adjudication in a Context of Constitutional Pluralism' (2007) 1(2) European Journal of Legal Studies 1, 1-2 cited in: Rodríguez, *op.cit.*, 117.

[21] *Ireland* v *Commission*, Case 325/85, [1987] EU:C:1987:546, at para. 18; *Cabinet Medical Veterinar Dr. Tomoiagă Andre,* Case C-144/44, [2015] EU:C:2015:452, at para. 34.

This contribution will explore the standard of the 'essentially equivalent protection' required for international transfers of data. For this, it will first trace back the source of a single standard of protection through looking at the legislative and jurisprudential developments on the matter. In particular, it will pinpoint how the relation between different concepts changed with successive judgments of the CJEU, moving them closer and closer to one another and culminating in *Schrems II*'s conclusions. It will also argue that such a single standard could not be taken for granted on the basis of the GDPR but constitutes a choice motivated by the objective of guaranteeing the maximum respect of the European right to data protection in the international context. Section II will attempt to shed light on the content of the single standard of protection and it will pinpoint the reasons for which – despite extensive explanations of the Court on the matter – this standard is still far from being clear. This section will indicate in particular how the language used by the Court has created more confusion than certainty for the data exporters who seek to comply with EU law on personal data flux. The last section will discuss whether the Court's choice to prioritize a high level of protection of personal data at the cost of legal certainty was necessary to safeguard the fundamental right. It will be argued that, ultimately, the Court's approach might disserve the cause.

I. Finding the source of a single standard of protection for international transfers of data

The *Schrems II* judgment introduced a single standard of protection essentially equivalent to the one guaranteed by the GDPR for all international transfers of data. Despite the fact that the CJEU presented this choice as clearly reflecting the objective of Chapter V GDPR 'to ensure the continuity of [the] high level of protection',[22] the path followed by the Court to reach this conclusion is far from obvious. In fact, the interpretative evolution of the notions used to

[22] *Schrems II*, at para. 93.

describe the standard of protection from the DPD's 'adequacy', through the *Schrems I'* 'essential equivalence' as a standard required for adequacy decisions, up to the *Schrems II'* extension of this standard to cover transfers subject to appropriate safeguards, shows the complexity of the Court's assessment. As will be shown in the present analysis, more often than not the Court has gone against the literal wording of the legal texts, instead favouring the objective of safeguarding the unique European fundamental right to data protection in the context of international data flows. However, as much as the protection of fundamental rights constitutes a general principle of EU law outranking secondary legislation, so does the principle of legal certainty which dictates that the law be predictable in its effects. It will be argued that in its case law on international transfers of data, the CJEU has not given as much attention to the latter principle as compared to the former, which resonates in the remaining uncertainty as to the content of the standard of protection required for international transfers.

a. *Schrems I*: the emergence of the concept of *essential equivalence*

Just like its successor, the DPD used a number of various terms to describe the standard(s) of protection of personal data required for international transfers, such as adequate level of protection, adequate safeguards and appropriate safeguards. Differently from the GDPR, however, in the DPD, the concept of equivalent protection was referred to only in the intra-EU context[23] and reflected the more general principle of mutual trust amongst Member States which allows to disregard – for the sake of the free movement of data – the differences

[23] See Recital 8, 9 and Art. 30(2) DPD.

remaining[24] despite the harmonization.[25] As far as the international transfers of data were concerned, the DPD established the principle according to which only transfers to third countries ensuring an adequate level of protection were allowed. To that effect, Article 25(2) DPD foresaw a number of 'circumstances surrounding a data transfer operation' to be taken into account while assessing the adequacy of a third country in question. However, no definition of the concept of adequacy was included in the DPD.

The CJEU has clarified the relationship between the equivalence and the adequacy standards in *Schrems I* where it interpreted the concept of adequacy as requiring the level of protection 'essentially equivalent to that guaranteed within the European Union'.[26] By putting an equals sign between the terms 'adequate' and 'essentially equivalent' and employing the vocabulary reserved under the DPD to the standard of protection ensured among Member States, the Court has somewhat raised the bar and moved the concept of adequacy closer to the one of equivalence.[27] However, because of the fact that the original notion of equivalence in the DPD was not a concrete substantive requirement but a principle, it has remained unclear when the standard of 'essential equivalence' is met. In particular, in *Schrems I,* the Court has not offered any insights on the matter except for the clarification that the level of protection does not need

[24] Indeed, despite the adoption of the DPD, Member States retained a margin of manoeuvre with regard to *e.g.* notification requirements, administrative burdens imposed on operators (see First report on the implementation of the Data Protection Directive (95/46/EC), COM(2003)265 fin, 11), approach to direct marketing (see Neil Robinson *et al.*, 'Review of the European Data Protection Directive' [RAND Europe 2009] 24, <https://danskprivacynet.files.wordpress.com/2009/05/review_of_eu_dp_directive.pdf> accessed 20 April 2021), treatment of sensitive data and data transfers to third countries (see Graham Pearce and Nicholas Platten, 'Achieving Personal Data Protection in the European Union', [1998] 36[4] Journal of Common Market Studies 529, 539).

[25] See in particular Recitals 9 and 10 DPD. See also Pearce and Platten, *op.cit.*, 532.

[26] *Schrems I*, at para. 73.

[27] See in the same sense Paul Roth, 'Adequate Level of Data Protection in Third Countries Post-Schrems and under the General Data Protection Regulation' (2017) 25(1) Journal of Law, Information and Science 49, 54. This approach has been criticized *e.g.*, by Determann according to whom 'it is worth noting that the EU Data Protection Directive 95/46/EC requires "equivalence" only with respect to data protection laws in the EEA Member States, see Art 31.2. With respect to third countries, the Directive requires "adequacy", see Arts 25 and 26, given that it would be unrealistic and counterproductive to demand total worldwide harmonization of data protection laws. The CJEU, however, ignores this prudent distinction in the Directive (…)'. See Lothar Determann, 'Adequacy of data protection in the USA: myths and facts' (2016) 6(3) International Data Privacy Law 244, 248.

to be identical to the one guaranteed in the EU[28] and that the means to which a third country has recourse can be different than the ones used in the EU.[29]

The *Schrems I'* finding concerned only adequacy decisions but, under the DPD, it is the adequacy decisions that constituted the primary basis for international transfers of data. The transfers subject to adequate safeguards, in their turn, constituted merely one of the derogations that could be used for international transfers of data where no adequacy decision was in place.[30] Since under EU law derogations from general rules are to be interpreted narrowly,[31] they could be relied on only exceptionally. The architecture of Chapter IV DPD on transfers of personal data to third countries reflected this dichotomous system by including only two provisions: Article 25 DPD relating to adequacy decisions entitled 'Principles' and Article 26 DPD dealing with derogations. The GDPR maintained the majority of the rules for international transfers of the DPD but reshuffled significantly the order in which those rules appear. Most importantly, the former Article 25 DPD has been divided into two provisions: Article 44 GDPR on the general principle for transfers and Article 45 GDPR which now deals specifically and exclusively with adequacy decisions. Such division is not surprising considering the fact that appropriate safeguards were not only developed by the new legislation, but also their status has changed – from derogations they have been promoted to a proper alternative to adequacy decision and a fully-fetched basis for international transfers of data.[32] As to the new key provision on the general principle governing all international transfers of personal – Article 44 GDPR – it stipulates that 'any transfer of personal data which are undergoing processing or are

[28] *Schrems I*, at para. 73.
[29] *Schrems I*, at para. 74.
[30] See Art. 26 DPD.
[31] See *e.g.*, *RFA International v Commission*, Case C-59/19 P [2021] EU:C:2021:102*,* at para. 54 and the case law cited therein.
[32] This is reflected by the architecture of Chapter V GDPR, which deals with the appropriate safeguards under Arts 46 and 47 GDPR, whereas derogations are treated by a separate provision – Article 49 GDPR. Moreover, the vocabulary has been adjusted, as the DPD talked about *adequate* safeguards, whereas the GDPR refers to *appropriate* safeguards.

intended for processing after transfer to a third country or to an international organisation shall take place only if (…) the conditions laid down in this Chapter are complied with by the controller and processor'. In addition, '[a]ll provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.'[33] Importantly, Article 44 GDPR does not mention any longer the concept of 'adequate level of protection' (nor does it introduce the one of 'essential equivalence'). Instead, in the GDPR, these terms continue to be used only with regard to the transfers based on the adequacy decisions adopted by the Commission.[34] The legislator seems, therefore, to make a clear distinction between, on the one hand, adequacy decisions (which, as indicated by Recital 104 GDPR reproducing *Schrems I*, need to meet the standard of essential equivalence), and on the other, the general principle governing all international transfers of data which, however, does not constitute a separate self-standing basis for transfers. Removing the concept of 'adequacy' from the provision on the general principle for transfers seems to remove altogether the question of the standard(s) of protection required for international transfers of data from the scope of this provision. Instead, the level(s) of protection can be deducted from the subsequent provisions of Chapter V GDPR dealing with specific legal bases for transfers, *i.e.*, adequacy decisions, appropriate safeguards and derogations, which seem to constitute a system in which the level of protection decreases accordingly.[35]

Indeed, the 'new' adequacy decisions differ from the DPD ones, also because Article 45 GDPR no longer links them to one concrete transfer or a set of transfers[36] but they are meant to assess

[33] Art. 44 GDPR.
[34] See Art. 45, Recitals 103, 104, 107, 114 GDPR. On top of that, it should be noted that the GDPR refers to the equivalence only when describing the level of protection ensured between Member States.
[35] See Daniele Nardi, '« Courtoisie internationale » et portée extraterritoriale du droit européen à la protection des données à l'épreuve de la Cour' (2018) 54(2) Cahiers de Droit Européen 327, 340 ; Christopher Kuner, 'Commentary to Article 45 GDPR' in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR). A Commentary* (Oxford University Press 2020), 774.
[36] Differently from Art. 25(2) DPD, according to which '[t]he adequacy decisions of the level of protection afforded by a third country shall be assessed in light of all the circumstances surrounding a data transfer operation or set of data transfer operations'.

the situation in a given third country (a territory or one or more specified sectors within that third country) more generally, in order to 'clear' all type of future transfers to that country. As stems from the wording of Article 46 GDPR, transfers on the basis of this provision may take place there, where no adequacy decision has been adopted. In such cases, it is for the controllers and processors to provide appropriate safeguards. While adequacy decisions are to assess the totality of factors characterizing the legal system of a third country, appropriate safeguards, by contrast, are tailored to particular transfers or types of transfers.[37] Finally, when no adequacy decision nor appropriate safeguards are in place, the remaining 'fall back option' for international transfers is the recourse to Article 49 GDPR which foresees a number of derogations for specific situations. Data transfers that rely on one of them benefit from no extra protection. This 'three-tiered structure' of Chapter V GDPR suggests a hierarchical system that gives preference to the transfers based on adequacy decisions, followed by appropriate measures and leaving derogations as an extraordinary basis for transfers in line with the decreasing level of protection offered in each case. [38] In its case law, however, the Court rejected this interpretative logic establishing instead a single standard of protection for all transfers.

b. *Opinion 1/15 and Schrems II*: *essential equivalence* as a self-standing standard for all international transfers

First, in *Opinion 1/15,* the CJEU has used *Schrems I* logic to indicate that the essential equivalence should be considered as a stand-alone standard for all transfers of personal data to third countries.[39] Some doubts, however, remained as to the exact scope of the statement, since

[37] Kuner, 'Commentary to Article 46 GDPR' in Kuner, Bygrave, Docksey (eds), *op.cit.*, 802. See also Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017), 119. Voigt and von dem Bussche considered that '[w]here contractual parties use [standard contractual clauses], an adequate level of data protection is only guaranteed by the data importer that is party to the contract and located in a third country'.
[38] See in the same sense Kuner, 'Commentary to Article 45 GDPR', *op.cit.*, 774, Nardi, *op.cit*., 340.
[39] *Opinion 1/15,* at para. 134.

the envisaged EU-Canada Passenger Name Record Agreement ('PNR Agreement'), which was the subject of *Opinion 1/15,* was substantially similar to the adequacy decision that was at stake in *Schrems I.* Indeed, the PNR Agreement recognized a Canadian authority as offering an *adequate* level of protection,[40] thereby borrowing the language of the GDPR's provisions on adequacy decisions. The extent of the *Opinion 1/15* finding was, however, made quite clear in the subsequent judgment.

In *Schrems II*, the Court referred to the last phrase of Article 44 GDPR[41] as requiring that the same level of protection must be guaranteed 'irrespective of the provision of that chapter on the basis of which a transfer of personal data to a third country is carried out'.[42] This level is understood by the Court as 'a level of protection of fundamental rights and freedoms (…) essentially equivalent to that guaranteed within the European Union by virtue of the [GDPR], read in light of the Charter'.[43] Through connecting 'equivalence' to Article 44 GDPR, the Court detached this condition from its original source – *i.e.* the requirement of an adequate level of protection of adequacy decisions – and expanded the 'essential equivalence' prescription to all international transfers of data, regardless of the specific basis relied on.[44] As to the last phrase of Article 44 GDPR, the latter does state that '[a]ll provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined' but admittedly, this phrase meant to indicate that 'flows of personal data outside the EU should not be allowed to circumvent the protections contained in EU data

[40] Art. 5 of the envisaged EU-Canada Passenger Name Record Agreement, Council of the European Union, Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record 12657/5/13 REV 5, 2014.
[41] According to this provision, '[a]ll provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined'.
[42] *Schrems II*, at para. 92.
[43] *Schrems II,* at para. 96.
[44] *Schrems II,* at para. 94-96 (here with regard to the transfers subject to appropriate safeguards).

protection regulation, in particular the GDPR'.[45] In any case, it seems difficult to deduct from this provision what level of protection is required for *all* international transfers.

The significance given to this provision by the Court is also not supported by the analysis of *travaux préparatoires.* It is true that the last phrase of Article 44 GDPR was indeed added to the GDPR draft as a direct consequence of the *Schrems I* judgment on the explicit request by the European Parliament ('EP') who wished to include in this provision a general clause 'about the need to ensure a high level of protection when data are transferred to a third country'.[46] Even though from the beginning of the interinstitutional negotiations the Council was requesting the deletion of Article 44 GDPR altogether,[47] since according to many Member States this provision was superfluous,[48] eventually it agreed to keep it in the shape requested by the EP. However, despite its roots in *Schrems I*, this inclusion does not seem to indicate the co-legislators' will to establish a single level of protection essentially equivalent to the one guaranteed by the GDPR for all international transfers. Indeed, from the Council's side, the insertion of the additional phrase in Article 44 GDPR was considered a 'minor modification'.[49] As to the EP, this change did intend to establish that a high level of protection is required for international transfers, still, at no time did the EP insist on the essential equivalence wording.

The finding of a single standard of protection is, furthermore, difficult to reconcile with the differentiated terms used in Article 45 GDPR on transfers based on adequacy decisions ('adequate level of protection'), Article 46 GDPR on transfers subject to appropriate safeguards ('appropriate level of protection')[50] and Article 49 GDPR on derogations (which refers to 'suitable safeguards').[51] The literal reading of these provisions in light of the requirement that

[45] Kuner, 'Commentary to Article 44 GDPR' in Kuner, Bygrave, Docksey (eds), *op.cit.,* 757.
[46] Council of the European Union, Doc. No. 14071/15, 13 Nov. 2015, 2.
[47] Council of the European Union, Doc. No. 10349/14, 28 May 2014, 19.
[48] In particular Czech Republic, Greece, France, Sweden, Netherlands, the UK – see Council of the European Union, Doc. No. 6723/4/13 REV 4, 25 March 2013, 16, 51 71, 84, 123, 130.
[49] Council of the European Union, Doc. No. 14901/15, 4 Dec. 2015, 4.
[50] See Recital 102 GDPR.
[51] For more details on the concept of suitable safeguards see the Sub-section IIb below.

different terms should not have the same meaning,[52] would suggest that each of the specific bases for international transfers is supposed to guarantee a different standard of protection. Also, the structure of Chapter V GDPR (described in the previous sub-section) supports such reading.

It is therefore clear, that in reaching its conclusion on the single standard of protection essentially equivalent to the one guaranteed by the GDPR for all international transfers of data, the Court has relied primarily on the purposive reading of Article 44 GDPR. Whereas it is true that the discrepancies between the various language versions of the GDPR do call for the referral to other methods of interpretation, and the purposive method of interpretation is usually preferred by the Court, the finding seems seriously detached from the content of other provisions of Chapter V GDPR creating a situation of a legal uncertainty as to what the required standard of protection really entails.

II. Understanding the standard of essential equivalence of personal data protection

The finding of a single standard of protection of personal data for all international transfers is not a straight-forward conclusion that can be supported by most interpretative techniques typically used to interpret EU law. As much as such approach is not a new one for the CJEU, the exclusive reliance on the teleological interpretation of Article 44 GDPR to establish a single standard of protection essentially equivalent to the one guaranteed by the GDPR results in even more of an interpretative discomfort when one attempts to unveil the substance of the required level of protection. As will be shown in the present section, in *Schrems II,* to support its finding of a single standard, the Court had to *de facto* equalize the content of the provisions on adequate decisions and appropriate safeguards, devoting as little as three paragraphs to this important

[52] See *e.g.*, *Hässle,* Case C-127/00, *op.cit.*, at para. 57; *Parliament v Council,* Case C-414/04, *op.cit.*, at para. 32; *UGT-FSP*, Case C-151/09, *op.cit.*, at para. 36; *Unomedical*, *op.cit.*, Case C-152/10, at paras 29-34; *Delphi Deutschland*, Case C-423/10, *op.cit.*, at para. 26; *ADL*, Case C-546/13, *op.cit.*, at para. 41; *Planta Tabak,* Case C-220/17, *op.cit.,* at para. 67; see also Lenaerts and Gutiérrez-Fons, *op.cit.,* 14; Itzcovich, *op.cit.*, 552.

finding[53] and leaving little explanation as to the substantial understanding of the essentially equivalent level of protection.[54] In reality, it seems that this standard is much higher than the Court would like to admit, making the distinction between equivalent and essentially equivalent very theoretical.

a. Legal gymnastic of the CJEU: establishing *factors to be taken into consideration* in all international transfers of data

Looking at the provisions on the various conditions and/or circumstances to be taken into account in the case of data transfers based on each of the available legal bases, it seems impossible to argue that the legislator intended for these four notions to have the same meaning. In the case of adequacy decisions, Article 45(2) GDPR gives an extensive – though non-exhaustive – list of elements to be taken into account in the assessment of the adequacy of the level of protection provided by a third country under consideration. These elements can be divided into 3 groups. First, the provision focuses on the characteristics of the scrutinized system from the perspective of democracy and fundamental freedoms, listing general factors such as the rule of law, respect for human rights and fundamental freedoms, access to justice as well as specific factors such as the existence of general and sectoral legislation and the existence of effective and enforceable data subject rights. The second element of importance is connected to the oversight of data protection practices, in particular the existence of judicial and administrative redress and the existence of an independent data protection authority. Finally, the international commitments the third country in question has entered into are to be considered. As apparent from the wording of Article 45(2) GDPR, these are *elements* (criteria) to be taken into account. Only some of them, in particular the existence of effective and

[53] *Schrems II,* at paras 102-104.

[54] See in the same sense: Theodore Christakis, 'After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe' (*European Law Blog,* 21 July 2020) <https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/> accessed 20 April 2021.

enforceable rights and effective administrative and judicial redress, could be considered as *requirements*, based on the interpretative guidelines of Recital 104.[55]

As far as appropriate safeguards are concerned, according to Article 46 GDPR,

> a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

Article 46 GDPR, therefore, mentions two requirements for transfers.[56] One of these requirements – namely the existence of enforceable data subject rights and effective legal remedies for data subjects – is identical to the one requested under Article 45(2) GDPR.[57] This is where the similarities between the two provisions end. Indeed, the second requirement to provide appropriate safeguards is not only a *requirement* (as opposed to an *element to be taken into account)*, but it also does not mention any of the substantial criteria listed in Article 45(2) GDPR, nor does it refer to this provision.

Yet, in *Schrems II* the Court decided that 'the factors to be taken into consideration in the context of Article 46 [GDPR] correspond to those set out, in a non-exhaustive manner, in Article 45(2) [GDPR]'.[58] Even though, this interpretation is a necessary consequence of the Court's choice to link equivalence to Article 44 GDPR (and by extension to adequacy and appropriate safeguards), connecting the content of these provisions to one another required an impressive legal gymnastic from the Court. As already mentioned, the requirement of the

[55] In line with Recital 104 GDPR, '(…) [t]he 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'.
[56] The CJEU itself refers to the '*requirements* of Art. 46 GDPR' see *Schrems II,* at paras 92 and 140.
[57] In fact, as stems from Recital 114 GDPR, the existence of enforceable data subject rights and effective legal remedies for data subjects is required for any transfer conducted on the basis of Chapter V GDPR.
[58] *Schrems II,* at para. 104.

existence of enforceable data subject rights and effective legal remedies for data subjects is explicitly included in both provisions. Considering that – according to the Court – the content of the two provisions is the same, that would mean that all the other criteria included in Article 45(2) GDPR fit in the concept of appropriate safeguards that are required under Article 46 GDPR. However, there are at least three reasons for which this 'equation' is questionable.

First, the *elements* that need to be taken into account in the assessment of adequacy simply do not belong to the same semantic category as *requirements* referred to in Article 46(1) GDPR. In other words, something cannot be an element (factor) to be taken into account and a requirement (condition) at the same time. The most telling example of this contradiction is Article 45(2)(c) GDPR, which – in the assessment of the adequacy of the level of protection offered by a third country – requires to look at the international commitments the third country has entered into. Indeed, as underlined by Recital 105 GDPR, participation in multilateral or regional systems, in particular in relation to the protection of personal data, constitutes an indication of the commitment to the protection of personal data. This, however, is neither required nor sufficient for the adoption of an adequacy decision by the Commission. It is simply an *element* to consider.

Second, since Article 45(2) GDPR enumerates *criteria,* it is not surprising that the list is non-exhaustive. The same cannot be said, when these criteria become *requirements,* in particular, in the context when non-compliance with the GDPR can generate serious financial repercussions for data controllers and processors.[59] Admitting that the list of *requirements* to comply with in the case of international transfers of data based on Article 46 GDPR is non-exhaustive introduces legal chaos and the risk of a retroactive effect of this provision. Moreover, Article 46 GDPR explicitly states that the appropriate safeguards require no prior

[59] On the legal certainty requirements in the context of of rules liable to entail financial consequences see *Cabinet Medical Veterinar Dr. Tomoiagă Andrei*, Case C-144/44, *op.cit.,* at para. 34; *Ireland* v *Commission*, Case 325/85, *op.cit.,* at para. 18.

authorization from supervisory authorities. Confronted with a non-exhaustive list of factors that need to be considered and compensated by the adequate safeguards proposed by the data exporter, little legal security can be offered to the latter. Data exporters may therefore want to seek an authorization for international transfers subject to appropriate safeguards to bar themselves from liability. This, however, would go against the purpose of the provision.[60]

Finally, the Court takes no notice of the provisions on adequate safeguards that are present in other chapters of the GDPR that are not related to international transfers.[61] One of such provisions is Article 89 GDPR, according to which '[p]rocessing for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards'.[62] The provision specifies that those safeguards shall warrant, in particular, the principle of data minimization and can be ensured through means such as pseudonymization (or – as mentioned in Article 6(4)(e) GDPR – encryption). The appropriate safeguards are thereby defined as technical and organisational measures[63] designed to minimize the risks that are incumbent upon data subjects in these specific processing activities[64] and ensure a high level of security of the processing. In the context of the presumption of the legislator as a reasonable actor who does not designate with the same name two different concepts, it is fair to assume that the appropriate safeguards under Article 46 GDPR should be

[60] Indeed, para. 134 of *Schrems II* states that 'the contractual mechanisms provided for in Article 46(2) of the GDPR is based on the responsibility of the controller (…) and, in the alternative, of the competent supervisory authority. It is therefore, above all, for that controller (…) to verify, on a case-by-case basis (…) whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses'.

[61] See Arts 6(4)(e), 9(2)(d), 10, 58(4), 87, 89 GDPR.

[62] Art. 89 GDPR.

[63] See Art. 89 GDPR, Recital 156 GDPR.

[64] See by analogy concerning the compatible further processing regulated by Art. 6(4) GDPR: Waltraut Kotschy, 'Commentary to Article 6 GDPR' in Kuner, Bygrave, Docksey (eds), *op.cit.*, 342. According to Kotschy, '[r]isks created by the "compatible further processing" may be mitigated by special safeguards. Data minimisation might be advantageous. Encryption (of the whole data set) is mentioned in Article 6(4)(e) as one example, pseudonymisation as another. Regarding the special purposes explicitly declared as compatible by Article 5(1)(b), risk containment has to be achieved according to Article 89(1) GDPR. The latter provision requires adequate technical and organisational measures for ensuring appropriate safeguards, pseudonymisation or even anonymisation being a mandatory measure as far as the "purpose of further processing can be fulfilled in that manner"' (footnote omitted).

understood in the same way, *i.e.*, as technical and organizational measures. The goal of appropriate safeguards in this context would be to minimize the risk and to 'ensure compliance with data protection requirements and the rights of the data subjects *appropriate* to processing within the Union'.[65] Importantly, however, the risk is not eliminated by such appropriate safeguards. It is apparent that technical or organisational measures such as pseudonymization or encryption cannot fully compensate for all inadequacies that may appear in a foreign system.[66] This is why, instead of relying on the explanation and examples of adequate safeguards provided by the GDPR itself, the Court chose to define them differently, in line with the reasoning that, if Article 44 GDPR is the source of the standard of essential equivalence, the elements that are taken into account for all the transfers need to be the same.[67]

b. The question of derogations

When no adequacy decision nor appropriate safeguards are in place, the remaining 'fall back option' for international transfers is the recourse to Article 49 GDPR which foresees a number of derogations for specific situations. In the context of the Court's rejection of the hierarchical structure of legal bases for international transfers of data, the question that arises is what effects

---

[65] Recital 108 GDPR, emphasis added. A possibility to rely on the risk-based approach in the context of determining appropriate safeguards for a specific data transfer (*i.e.* on the basis of a data transfer risk assessment instead of on the presumption that all international transfers constitute under the GDPR a high risk processing *per se*) has been advocated, *e.g.*, in the Centre's for Information Policy Leadership White Paper 'A Path Forward for International Data Transfers under the GDPR after the CJEU Schrems II Decision', (Information Policy Centre 2020)
<https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_gdpr_transfers_post_schrems_ii__24_september_2020__2_.pdf> accessed 20 April 2020.

[66] Indeed, differently from anonymisation, these measures do not depersonalise data, thus rendering the GDPR inapplicable, but only increase their security. In the assessment of the Canadian Passenger Name Record, despite the existence of encryption measures, the Court did not consider this to be on its own sufficient to ensure compliance with Arts 7 and 8 of the Charter. The Advocate General referred to the measures as being accessory in establishing that the essence of the right to protection of personal data is satisfied. See *EU-Canada PNR Agreement*, Opinion of Advocate General Mengozzi, [2016] EU:C:2016:656, at paras 265-267.

[67] Ignoring the possibility to deploy the risk-based approach in the context of transfers based on adequate safeguards (contrary to other provisions of the GDPR referring to the concept of 'adequate safeguards') is also apparent in the European Data Protection Board's 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' published in the aftermath of *Schrems II* which currently undergo public consultations – see Theodore Christakis, '"Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 2)' (*European Law Blog,* 16 November 2020) <https://europeanlawblog.eu/2020/11/16/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-2/#_ftnref1> accessed 20 April 2021.

the recognition of a sole standard of protection has on the interpretation of Article 49 GDPR. A strict application of the *Schrems II* finding that the same level of protection applies 'irrespective of the provision of [Chapter V GDPR] on the basis of which a transfer of personal data to a third country is carried out',[68] would dictate to assume that this standard is also required for transfers based on derogations. However, it seems that such an interpretation would lead to a *reductio ad absurdum* of Article 49 GDPR as it would deprive the provision of its entire purpose of being an extraordinary basis for transfers. In the absence of an adequacy decision or appropriate safeguards, it would also effectively prevent all transfers of personal data for *e.g.*, humanitarian reasons, legal claims purposes or transactions, even when a data subject's consent is given.

Yet, even if one accepts that data transfers that rely on one of the derogations benefit from no extra protection,[69] not all derogations in Article 49 GDPR should be seen as equal. The second subparagraph of Article 49(1) GDPR creates a so-called 'last resort derogation'[70] applicable when none of the other 'normal derogations' can be used. This special provision can be described as a 'soft derogation', as its use is conditional upon a number of prerequisites.[71] The most important one, distinguishing it from "normal derogations", is the fact that the data exporter must provide *suitable safeguards* with regard to the protection of personal data. This requirement places it somewhere between a traditional derogation and a normal (though restrictive) legal basis for international transfers. Chapter V GDPR does not specify what level of protection should be guaranteed by suitable safeguards.[72] Only Recital 113 GDPR indicates vaguely that they should 'protect fundamental rights and freedoms of natural persons with

[68] *Schrems II*, at para. 92.
[69] Kuner, 'Commentary to Article 49 GDPR' in Kuner, Bygrave, Docksey (eds), *op.cit.*, 846.
[70] European Data Protection Board ('EDPB'), 'Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679', 2018, 14. See also Council of the European Union, 'Statement of the Council's reasons', 5419/1/16 REV 1 ADD 1, 27, where the derogation in question is labelled as an '*ultimum remedium'.*
[71] For more on these conditions see Kuner, Commentary to Article 49 GDPR, *op.cit.,* 853.
[72] In its guidelines, the EDPB refers to pseudonymization and encryption as possible suitable safeguards (see EDPB, *op.cit.*, 16).

regard to the processing of their personal data'. Even though in *Schrems II,* the Court pronounced itself with regard to the transfers based on adequacy decisions and appropriate safeguards,[73] if one follows the purposive approach of the Court, also transfers subject to suitable safeguards could be covered by the essentially equivalent level of protection requirement. In addition, some language versions of Article 49 GDPR and Recital 113 GDPR use the same term to describe the safeguards required by Article 46 GDPR (in the English version – 'appropriate safeguards') and those referred to by Article 49 GDPR (in the English version – 'suitable safeguards').[74] Drawing a definite conclusion on the nature of safeguards referred to in Article 49 GDPR is, however, far from being straightforward, as some other language versions of Chapter V GDPR follow the English distinction,[75] and still others use not two but three different notions in Recital 113, Article 46 and Article 49 GDPR.[76] Therefore, even if through *reduction ad absurdum* the application of the essentially equivalent standard of protection to 'normal derogations' should be rejected, due to the language discrepancies of the GDPR and in the context of *Schrems II,* its applicability to the 'special derogation' of the second sub-paragraph of Article 49(1) GDPR remains unclear.

c. Differentiating between the essential equivalence of protection of personal data and the equivalence *tout court*

The inconsistencies and contradictions in Chapter V GDPR and the relevant case law make it very difficult to know what the standard of essential equivalence, so desired by the Court, concretely means and what the substantial (minimum) requirements in this regard are.

[73] *Schrems II*, at para. 96.
[74] This is the case of *e.g.*, French, German, Dutch, Italian and Polish versions which in both Articles 46 and 49 GDPR use the same term – respectively: 'garanties appropriées', 'geeignete Garantieren', 'passende waarborgen', 'garanzie adeguate', 'odpowiednie zabezpieczenia'.
[75] *E.g.*, Spanish version, which distinguishes between 'garantías apropiadas' and 'garantías adecuadas'.
[76] *E.g.*, Slovak version, which refers to 'náležité záruky', 'primerané záruky' and 'vhodné záruky' respectively.

In *Schrems II*, the Court unsurprisingly refrained from providing a comprehensive list of conditions that are to be required for a sufficient standard of protection for international transfers of data. In its ruling, however, the Court attempted to outline certain general framework for data exporters. First, as mentioned previously, the CJEU declared that the appropriate standard to consider in assessing the essential equivalence of protection are the rules established by the GDPR itself read in light of the Charter.[77] Thereby, the Court rejected the Advocate General's proposition to differentiate the standard of protection and – in the cases where the Charter does not apply, in particular in the instances where national security is involved – refer instead directly to the ECHR and the relevant case law of the European Court of Human Rights.[78] The essentially equivalent level of protection needs to be therefore assessed solely in light of EU law.

Second, by invalidating the Commission's adequacy decision and the Privacy Shield principles,[79] the Court pronounced itself as to what does *not* meet the required standard of protection. In its assessment, the CJEU focused on the limitations to the protection of privacy and personal data brought by the interferences authorized by the US law. The Court assessed these limitations in light of the conditions of Article 52(1) of the Charter. The fact that the relevant national legislation did not indicate any limitations on the power it confers to implement surveillance programme rendered it non-compliant with the proportionality condition.[80] Moreover, the Court considered that the requirements of Article 57 of the Charter are not met either, as data subjects were not granted actionable rights against the US authorities

[77] *Schrems II*, at para. 101.
[78] This would be the case when the issues of national security are at stake and the measures of surveillance are executed directly by the State authorities without the involvement of private actors. Conversely, according to the proposition of Advocate General, the Charter standard would be relevant for the cases of access by public authorities to data collected by private parties, in particular telecom companies. See *Schrems II,* Opinion of Advocate General Saugmandsgaard Øe, [2019] EU:C:2019:1145 ('Opinion in *Schrems II'*), at para. 207 *et seq*.
[79] 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.
[80] *Schrems II,* at para. 180.

before the courts.[81] This assessment aligns with the Court's stand on the similar national measures adopted by Member States.[82]

Third, the Court upheld the Commission's decision on standard contractual clauses ('SCC Decision'),[83] thereby confirming that the latter *does* meet the required standard of essentially equivalent level of protection. As pointed out by the CJEU, the SCC Decision requires to ensure that the processing of the transferred data will be carried out in accordance with 'the applicable data protection law', of which the GDPR read in light of the Charter forms part.[84] In other words, the Standard Contractual Clauses ('SCC') extend contractually the application of the GDPR to non-EU data recipients. At the same time, they require from data exporters and recipients to ensure that no conflicting national legislation bars them from fulfilling the obligations undertaken through such a contract.[85] The only recognized limitation constitute 'mandatory requirements of that legislation which do not go beyond what is necessary in a democratic society to safeguard, inter alia, national security, defence and public security',[86] which are the same objectives as the ones that can be relied on by the EU Member States to limit the right to privacy and the right to protection of personal data in their domestic legislations.[87]

By saying what *does* (Standard Contractual Clauses) and what does *not* meet the standard of the equivalent level of protection (the guarantees of the Privacy Shield), the Court seems to

[81] *Schrems II,* at paras 181-182, 187.
[82] See *Tele2 Sverige*, Case C-203/15, [2016] EU:C:2016:970, at para. 121 *et seq*., *La Quadrature du Net*, Joined Cases C-511/18, C-512/18, C-520/18, [2020] EU:C:2020:791*,* at para*.* 190 *et seq*.
[83] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ 2010 L 39/5 as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 amending Decisions 2001/497/EC and 2010/87/EU on standard contractual clauses for the transfer of personal data to third countries and to processors established in such countries, under Directive 95/46/EC of the European Parliament and of the Council, OJ 2016 L 344/100 ('SCC Decision').
[84] *Schrems II,* at para. 138.
[85] *Schrems II,* at paras 139-140.
[86] *Schrems II*, at para. 141.
[87] See *La Quadrature du Net*, Joined Cases C-511/18, C-512/18, C-520/18*, op.cit.,* at paras 136, 146 and the case law cited therein; *Privacy International,* Case C-623/17, [2020] EU:C:2020:790, at para. 75.

narrow down the zone within which data exporters should search for a formula that will ensure the legality of their transfers. However, a closer look at the positive and negative examples given by the Court reveals that the margin of manoeuvre for data exporters is potentially very small. Even though, presumably, a foreign system does not need to be identical to the EU one,[88] in assessing the Privacy Shield scheme, the Court compared the US legislation with each of the very concrete requirements of EU law one by one.[89] At the same time, in assessing the SCC Decision, the Court approved of the protection that essentially amounts to the indirect application of the EU rules (through a contract). In this context, the assertion that a third country does not need to ensure a level of protection identical to that guaranteed in the EU legal order seems to be theoretical and makes wonder whether the differentiation between an 'essentially equivalent level of protection' (as required from third States) and 'equivalent level of protection' (as required from Member States) is not a factitious one.

d. In search of 'conflicting obligations'

In the light of the establishment of such a high standard of protection for international data flows, it is interesting to turn to the concept of 'conflicting national legislation' resulting from Clause 5(b) of the SCC that can bar data controllers from relying on the SCC (when no adequacy decision is in place) to export data outside the EU.[90] This clause has been considered by the Court as crucial for confirming the validity of the SCC developed by the Commission.[91] Even though in the context of the Privacy Shield and the level of protection offered by the US, the discussion on such conflicting national legislation has been focused on the US national

[88] *Schrems II,* at para. 94; *Schrems I,* at para. 73.
[89] The Court has used the same methodology in *Opinion 1/15.*
[90] According to Clause 5(b) of SCC Decision (*op.cit.*), the recipient certifies that 'it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract'. The new Draft Implementing Decision on SCC maintains this rule – see Recital 19, Ares(2020)6654686.
[91] *Schrems II, op.cit.,* at para. 139 *et seq.*

security measures, arguably also other legislation could stand in the way of complying with the standard of protection essentially equivalent to the one guaranteed by the GDPR. In lack of an adequacy decision, the assessment of such laws will be incumbent upon data controllers.

One such possible conflict has been recently highlighted by the U.S. *hiQ v. LinkedIn*[92] case which concerned the practice of scraping of personal data from *LinkedIn* pages by the start-up *hiQ.* Even though the case dealt with what from the EU law perspective is considered to constitute personal data, in the US context, the main legal questions were raised with regard to the problem of blocking access to the publicly available information (which therefore escapes privacy protection). As the result, the US court required *LinkedIn* to get rid of the technical safeguards hindering *hiQ* from scraping *LinkedIn* profiles.[93] Considering that *LinkedIn*'s data centres which store *LinkedIn* members' information are located in the US, transfers of data from the EU to the US are necessary.[94] In the aftermath of the *Schrems II* judgment and the invalidation of the *Privacy Shield, LinkedIn* continues to transfer data to the US on the basis of SCC. In light of the *hiQ v LinkedIn* judgment, it is, however, questionable whether the obligation requiring *LinkedIn* to remove technical safeguards protecting personal data of *LinkedIn* members from scraping is not in conflict with the GDPR's principle of privacy by design.[95] In addition, in a factually similar EU case, a Polish data controller has been fined nearly €220,000 (943,470 PLN) for scraping personal data from publicly available Internet pages without informing data subjects about this subsequent processing and thereby violating data subjects' right to information.[96]

---

[92] *hiQ Labs, Inc v LinkedIn Corp* 273 F. Supp. 3d 1099 (N.D. Cal. 2017), confirmed on appeal by *hiQ Labs, Inc v LinkedIn Corp* No.17-16783 (US 9th Circuit Court of Appeals (9th Cir.), 9 September 2019 and currently pending before the US Supreme Court.

[93] For a detailed analysis of the case, see Zuzanna Gulczyńska 'Scraping personal data from internet pages – a comparative analysis of the Polish Bisnode decision and the US hiQ Labs v LinkedIn Corp judgment' (2020) 45(6) EL Rev 857.

[94] *LinkedIn*, 'EU, EEA, and Swiss Data Transfers', <https://www.linkedin.com/help/linkedin/answer/62533/eu-eea-and-swiss-data-transfers?lang=en> accessed 20 April 2021.

[95] Art. 25 GDPR.

[96] For a detailed analysis of the case, see Gulczyńska, *op.cit.*

In line with the *Schrems II* judgment,

> where the Commission has not adopted a decision on the adequacy of the level of data protection in a third country, the controller or, where relevant, the processor 'should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject'.[97]

It is, therefore, the responsibility of data controllers to verify what conflicting obligations they might be subject to in the transfer's destination country. In the context of the US *hiQ v LinkedIn* judgment, they will have to assess, amongst others, whether the obligation to refrain from hindering data scraping practices complies with the SCC (in particular the requirement to ensure appropriate technical measures to protect personal data against unauthorised access and the data subjects' right to information), or – to the contrary – infringes the terms of SCC, and therefore fails to provide the required essentially equivalent level of protection.

This task is by far not an easy one. Following the example used hereabove, the right to information about the ongoing processing of personal data is considered as one of the crucial prerequisites for the enjoyment of other rights.[98] At the same time, in many jurisdictions, including the US, the right to privacy can protect personal data only to the extent there is an expectation of privacy, which excludes information disclosed on the Internet by data subjects themselves, let alone providing any information about the processing to the person concerned. Deciding whether such conceptual differences of the right to data protection can be justified by the fact that the foreign systems arguably do not have to be identical to the EU one or instead

[97] *Schrems II,* at para. 131.
[98] See Recitals 39 and 60 GDPR.

meet the threshold of a 'conflicting obligation' is the risk that will have to be taken by data controllers.[99]

III. Essential equivalence requirement in the context of the promotion of a high standard of data protection globally

The underlaying objective of the Court's interpretative choices in *Schrems I, Schrems II* and *Opinion 1/15* was undoubtedly to ensure a high level of protection of personal data. However, one could question whether the methods deployed by the Court and the lack of flexibility truly ensure the achievement of this goal, which after all is enshrined also in the GDPR itself,[100] and should therefore guide the CJEU.

In this regard, it is worth pointing to the arguments put forward by some Member States in the context of the PNR Agreement that gave rise to *Opinion 1/15*. These arguments come down to the acknowledgment that even though the envisaged agreement might not be ideal, in its absence 'measures taken in relation to passengers arriving from the European Union would be at risk of being less targeted and more intrusive'.[101] Indeed, as pointed out by the French Government, the obligation placed on air carriers to transfer data is provided by the Canadian legislation,[102] and will most likely remain whether the EU concludes an agreement with Canada or not. Even though the Court does not pick up this line of argumentation (instead underlying throughout the judgment the imperative objective of safeguarding the level of protection of personal data guaranteed within the EU),[103] the *Schrems* case law shows that the standard

[99] For more on the increased role and responsibilities of data controllers in the context of international transfers of data, see Róisín Áine Costello, 'Schrems II: Everything Is Illuminated?', [2020] 5(2) European Papers 1045 <https://www.europeanpapers.eu/en/europeanforum/schrems-II-everything-is-illuminated> accessed 20 April 2021.

[100] Art. 50 GDPR, see also Arts 3(5) and 21 Consolidated Version of the Treaty on European Union, OJ 2016 C 208/16.

[101] *EU-Canada PNR Agreement*, Opinion of Advocate General Mengozzi, *op.cit.,* at para. 153

[102] *Ibid.,* at para. 148.

[103] For the same reason, the Advocate General also proposes to conduct a strict review, despite the international character of the instruments relating to international transfers of data which form part of the context of international relations – see *EU-Canada PNR Agreement*, Opinion of Advocate General Mengozzi, *op.cit.*, at paras 200-204. This approach has been followed by the Court in *Opinion 1/15*.

required is so high that it might be very difficult to achieve by outsiders.[104] As pointed out, this standard is not automatically ensured even by the countries that may be following the standards established by the ECHR.

Conversely, when the less strict standards of the ECHR are not followed by Member States, the consequences for the intra-EU data exchanges are far less serious than for the flows of data to third countries.[105] Indeed, as pointed out by Christakis, the European Court of Human Rights ('ECtHR') has found the surveillance measures deployed by several Member States, most recently Hungary[106] and the UK (while it still was an EU Member State)[107] as violating the ECHR. Similarly, the CJEU considered that the laws of France, Belgium and the UK[108] do not meet the EU standards either.[109] Yet, due to the principle of equivalent protection, intra-EU transfers cannot be restricted.[110] The level of protection of personal data required from third countries is therefore – at least in some instances – higher than the one followed by Member States. This paradox is not only an inconvenience for the EU's relations with third countries undermining its leverage to improve the protection of personal data globally, but in the context of Convention 108,[111] it may amount to a violation of legal obligations incumbent upon Member States.

---

[104] See in the same sense Roth, *op.cit.,* 63.

[105] This is why, in the cases where the Charter does not apply, in particular in the instances where national security is involved Advocate General Saugmandsgaard Øe proposed to use the standard of protection as defined by the ECHR, as 'it would be wholly unjustified, having regard to that objective, if a third country were expected to comply with requirements that did not correspond to obligations borne by the Member States', see Opinion in *Schrems II,* at para. 204.

[106] *Szabó and Vissy v. Hungary*, App. no 37138/14, (ECtHR, 12 January 2016).

[107] *Big Brother Watch,* App nos 58170/13, 62322/14 and 24960/15 (ECtHR, 13 September 2018). The violation has been confirmed recently by the Grand Chamber (ECtHR, 25 May 2021).

[108] *La Quadrature du Net*, Joined Cases C-511/18, C-512/18, C-520/18, *op.cit.; Privacy International,* Case C-623/17, *op.cit*.

[109] Theodore Christakis, '"Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 1)' (*European Law Blog,* 13 November 2020) <https://europeanlawblog.eu/2020/11/13/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-1/> accessed 20 April 2021.

[110] Art. 1(3) GDPR. For more details on the principle of equivalence in the GDPR see Section II above.

[111] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS 108 ('Convention 108').

The EU's devotion to the protection of personal data is reflected not only by means of its internal legislation but also by its involvement in the only legally binding international multilateral agreement in the field of personal data protection – the Council of Europe Convention 108. All Member States are party to the said convention. They are also almost all signatories to the amending Protocol (with the exception of Denmark),[112] which, after its entrance into force, will allow the EU itself to adhere to the modernized version of the convention. The significance of Convention 108 is recognized by the GDPR in the context of adopting adequacy decisions, for which 'the third country's accession to the [Convention 108] and its Additional Protocol[[113]] should be taken into account'.[114]

Even though Convention 108 and the GDPR share many similarities, their substantial rules are not identical. Some particular requirements, such as the existence of national data protection authorities, are missing from the convention. Also, its more modest size makes it in general significantly less detailed in comparison with the GDPR. This is why, similarly to the case of the ECHR,[115] it can be presumed that the essentially equivalent standard of protection of personal data will not be automatically ensured even by the countries that may be following the standards established by Convention 108. The exclusion of any 'automatic equivalence' was, after all, the original purpose of Article 44 GDPR – which was designed to make sure that international transfers can take place 'only if (…) the conditions laid down in [Chapter V] are complied with', *i.e.*, in particular that every transfer is executed on one of the three bases available therein.

[112] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 2018, ETS No.223.
[113] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows 2001, ETS No.181.
[114] Recital 105 GDPR.
[115] See the preceding Sub-section II(c).

Differently than in the case of the ECHR, however, Convention 108 clearly states that '[a] Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorization transborder flows of personal data going to the territory of another Party'.[116] It is true that in the modernized version of Convention 108 ('Convention 108+'), this provision is amended and foresees an exception allowing for such a limitation 'if [a Party is] bound by harmonised rules of protection shared by States belonging to a regional international organisation'.[117] However, the applicability of Convention 108+ is distant in time, as currently over 40 ratifications necessary for its entry into force are still missing.[118] Meanwhile, in its current shape, such derogation is not possible. The Court's findings in *Schrems II,* which establish a single standard of essential equivalence for all international transfers of data, in particular including also transfers subject to appropriate safeguards, in combination with the very high content of that standard, is therefore in direct contradiction with the internationally contracted obligation of Member States stemming from Convention 108. It also undermines the seriousness of EU's efforts undertook within the Council of Europe to advance a unified global approach to the protection of personal data and questions the EU's commitment to participate in this joint effort.

The Court's lack of flexibility might be linked to the fact that the prohibition of international transfers of data when no essentially equivalent level of protection can be achieved, applies only to the EU-based processors and controllers as a requirement of legitimacy of processing. At the same time, in the instances of what would be a direct imposition of those standards externally (*i.e.*, when the GDPR applies extraterritorially), the Court took a completely

[116] Art. 12(2), Convention 108.
[117] Art. 14(1), Convention 108+, consolidated text of Convention 108+, <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf> accessed 20 April 2021.
[118] See Council of Europe, Chart of signatures and ratifications of Treaty 223 Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures> accessed 20 April 2021.

different stand. In the *Google* case,[119] it distanced itself from 'judging' the solutions adopted in other parts of the world, that may be different than the EU approach[120] and refused to extend the territorial scope of the GDPR right to dereferencing globally.[121] Still, even though the Court closed the door of the direct imposition of EU data protection standards extraterritorially, it clearly left open the one allowing for an indirect imposition of such standards, *i.e.* through the provisions on international transfers of data. The result is that the conflicting national rules of third countries, which may be justified in the specific national context (*e.g.*, history of terrorist attacks), will anyway result in it being impossible to export personal data. In addition, numerous companies based outside the EU[122] apply the GDPR by virtue of Article 3(2) GDPR when they offer services to the individuals located in the EU (even when some conflicting obligations exist in the legal system of a given third State). At the same time, this activity can be accompanied by international transfers of data, which, however, based on *Schrems II* findings, might be forbidden because of the same conflicting obligations. The legal situation for these companies is highly unclear and, so far, despite *Schrems II* findings of an inadequate level of protection in the US which is unlikely to be compensated by private law measures, they continue to transfer data to US.[123]

Conclusions: less legal certainty and less protection of personal data globally?

Despite the apparent gradation of the levels of protection for international transfers of data that could be deducted from the GDPR, through its judgments in *Schrems I* and *Schrems II*, the CJEU has opted for a unique standard. However, as has been shown, the Court has built its interpretation on a number of presumptions that are far from being straight-forward.

[119] *Google (Territorial scope of dereferencing),* Case C-507/17, [2019] EU:C:2019:772.
[120] *Ibid.,* at para. 59.
[121] *Ibid.,* at para. 64.
[122] Airbnb, Netflix, Facebook to name just a few.
[123] See Noyb, 'Opening Pandora's Box: How companies addressed our questions about their international data transfers after the CJEU's ruling in C-311/18 - Schrems II' <https://noyb.eu/files/web/Replies_from_controllers_on_EU-US_transfers.pdf> accessed 20 April 2021.

Accordingly, it first developed the concept of 'essentially equivalent level of protection to the one guaranteed by the GDPR' and linked it to the one of adequacy in *Schrems I*. Subsequently, it stretched this link not only to the adequacy but to the general principles governing international transfers in *Schrems II*, thereby establishing a single standard of protection. The transfers based on adequacy decisions, subject to appropriate safeguards (perhaps even suitable safeguards) are therefore all supposed to meet the same standard. The objective of the Court in doing so is 'to ensure the continuity of [the] high level of protection where personal data is transferred to a third country.'[124] However, by focusing solely on this objective, the Court disregarded other goals and principles of EU law, in particular the principle of legal certainty.

The Court has not only introduced one standard of 'essential equivalence', but on top of that, it placed an equals sign between the elements to be taken into account for the assessment made by the Commission for adequacy decisions and requirements necessary for an international transfer subject to appropriate safeguards. Interpreting what these factors or requirements are, is far from being straight-forward. An additional element of confusion is added by the fact that in *Schrems II,* the Court has clearly made an assessment that compares a foreign system on a one-to-one basis with the EU one. This makes it particularly diffiult for data controllers to decide what third country's legislation might constitute an obligation conflicting with the principles established by the SCC. This not only undermines legal certainty, but also questions the very objective of ensuring a high level of protection of personal data.

Indeed, taking into account that the EU is the global leader in the field of data protection with a sophisticated system designed to offer the highest level of protection in the world,[125] complying with it constitutes a challenge for foreign actors. The Court's reading of the EU

[124] *Schrems II,* at para. 92.
[125] For more on the supremacy of the EU data protection regime by design see Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015) 41 *et seq.* On the impact of the GDPR globally, see *e.g.* He Li, Lu Yu & Wu He, 'The Impact of GDPR on Global Technology Development' (2019) 22:1 Journal of Global Information Technology Management 1.

obligation to promote high standards of data protection internationally (which are *de facto* identical to the EU rules) as simply *requesting* such level is short-sided, as a mere prohibition to transfer data to third countries (even subject to appropriate safeguards) is unlikely to stop such processing,[126] and can have the effect of the overall decrease in the level of protection. Such approach is also in clear contradiction with the terms agreed under Convention 108.

To conclude, the system created by the CJEU is not only complex and questionable from the perspective of the principle of legal certainty. The Court's lack of flexibility and disregard for other national and international instruments may also act to the detriment of the GDPR's objective of promoting a high standard of the fundamental right to data protection globally.

[126] See Noyb, *op.cit.*