MEMORANDUM

FROM: Prof. Lokke Moerel

DATE: February 1, 2016

RE: **An assessment of the impact of the Schrems judgement on the data transfer grounds available under EU data protection law for data transfers to the U.S.**

The purpose of this memorandum is to examine the export of personal data by data controllers established in the EU to countries outside of the EU,[1] in particular to the United States, in light of the judgment of the Court of Justice of the European Union (**CJEU**) in *Schrems v Data Protection Commissioner*[2] (**Schrems judgment**).

I. The EU data transfer regime

1. The general rule under EU Privacy Directive 95/46 (**Directive**) is that personal data can only be exported by a company established in the EU to third countries that provide an "adequate level of protection" for such data, unless certain conditions have been met (Article 25(1) of the Directive). Those conditions are split into two categories.

   (a) **Transfers based on an "adequacy decision" (issued under Article 25(6) of the Directive)**: Article 25(6) of the Directive allows the Commission to find – via an "adequacy decision" – that certain legal regimes are 'adequate' when assessed against the standard set by EU data protection law. Specific jurisdictional adequacy decisions include those permitting data export to Canada, New Zealand and Israel.[3] Only a very limited number of countries have obtained an adequacy decision, and these do not include main trading partners of the EU, such as China, Japan, Russia, India, and Brazil. The procedure for countries to obtain an adequacy finding can take years and requires a full assessment by the Commission of the rule of law, access to justice as well as international human rights norms and standards in such country, which assessment further has to be revised on a regular basis.[4]

   (b) **Specific data transfers grounds (regulated under Article 26 of the Directive)**: the general rule that personal data may only be exported from the EU to third countries that provide an "adequate level of protection" for such personal data is subject to a number of explicit "derogations". These derogations are set forth in Article 26 of the Directive, listing the circumstances in which a data exporter is permitted to transfer personal data from the

---

1 The countries of the European Free Trade Association (EFTA (Iceland, Liechtenstein and Norway) have ratified the Directive. References to the EU should be understood to include the EFTA countries, *i.e.*, they also concern the European Economic Area (EEA).

2 C-362/14 *Schrems* ECLI:EU:C:2015:650.

3 Currently, adequacy decisions have been adopted with regard to the following countries: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. See: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

4 Schrems, par. 76.

EU to a data importer in a jurisdiction that does not, or has not been recognised to, provide an 'adequate' level of protection as determined under EU data protection law.

II. The main finding of the Schrems judgment

2. In the Schrems judgment, the CJEU invalidated decision 2000/520 of the European Commission (**Commission**) which approved the Safe Harbour regime as providing for an adequate level of protection of personal data when assessed against the standard set by EU data protection law (**Safe Harbour Decision**).

3. The CJEU found that, in order for the Commission to adopt a decision pursuant to Article 25(6) of the Directive, it must find, duly stating reasons, that the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights that is essentially equivalent to that guaranteed in the EU legal order (known as an 'adequacy decision').

4. The CJEU held that the Commission's Safe Harbour Decision did not state that the United States in fact 'ensures' an adequate level of protection by reason of its domestic law or its international commitments, which was necessary for the Commission to have validly have concluded that Safe Harbour was adequate under Article 25(6) of the Directive (*Schrems* para 97).

5. The CJEU further held that Commission decisions, such as the Safe Harbour Decision, are binding upon the Member States, and can only be invalidated by the CJEU (*Schrems* para. 51-52). However, such a binding decision does not prevent the national DPAs, when hearing a claim lodged by a person concerning his or her data protection rights, to examine such claim with powers conferred upon the DPAs under Article 28 of the Directive, with complete independence, whether the relevant transfer of that data complies with the requirements laid down by the Directive (*Schrems* para. 57).

6. The CJEU held that the Safe Harbour Decision denied the national DPAs such powers under Article 28 of the Directive (*Schrems* para 102).

7. The CJEU then declared the Safe Harbour Decision invalid: "without there being any need to examine the content of the safe harbour principles" (*Schrems* para. 98).

8. **Conclusion.** The conclusion is that the CJEU did not independently assess the adequacy of U.S. law or the content and sufficiency of the Safe Harbour principles, but rather based its ruling on a conclusion of law regarding the sufficiency of the Commission's findings in the Safe Harbour Decision itself, also in light of the Commissions' own later findings in its Communication "Rebuilding Trust in EU-US Data Flows" (COM(2013) 846 final).

9. The CJEU reached this conclusion primarily based on the following considerations:

   (a) The fact that the Safe Harbour Decision (see fourth paragraph of Annex I), explicitly "lays down that 'national security, public interest, or law enforcement requirements' have primacy over the safe harbour principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard the safe harbour principles without limitation where they conflict with those requirements and therefore prove incompatible with them." (*Schrems* para. 82).

(b) The fact that the Safe Harbour Decision "does not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States nor does refer to the existence of effective legal protection against interference of that kind" (*Schrems* para. 88).

(c) The CJEU further explicitly stated that its analysis of the Safe Harbour Decision is "borne out by the Commission's own assessment of the situation resulting from the implementation of the Safe Harbour Decision entitled 'Rebuilding Trust in EU-US Data Flows' (COM(2013) 846 final) (**Commission Decision Rebuilding Trust**), "where the Commission found that the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security. Also, the Commission noted that the data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased" (*Schrems* para. 90).

Note: The Commission Decision Rebuilding Trust dates from 2013 and, since then, more in-depth research has been undertaken into the adequacy of U.S. law, U.S. government access powers to data of European citizens and the safeguards provided to EU citizens in respect thereof as well as into government access powers in the EU and safeguards provided to EU individuals in respect thereof, in order to establish equivalence.[5] In particular, I refer to the opinion of Geoffrey Robertson QC, of December 4, 2015[6], evaluating European standards of privacy protection compared to the U.S. It should further be pointed out that, since 2013, the U.S. has undertaken substantive reforms of its legal regime because of, and consequent upon, the Snowden revelations. Based on this research and legal developments, the conclusions of the Commission Decision Rebuilding Trust are no longer current and merit (a more in-depth) re-assessment. Further, the conclusions relating to the Safe Harbour Decision date from 2000 and therefore have no relevance for the new Safe Harbour agreement under negotiation and which is expected to be announced in the next few days. This

[5] See *e.g.* the Sidley Austin report, "Essentially Equivalent, A comparison of the legal orders for privacy and data protection in the European Union and the United States, January 2016, to be found at http://www.sidley.com/~/media/publications/essentially-equivalent---final.pdf. This rapport was commissioned by the U.S. Chamber of Commerce, The Software Alliance, the Computer and Communications Industry Association, and the Information Technology Industry Council and provides a comprehensive comparison of US and EU legal frameworks, particularly with respect to government access to data for law-enforcement and intelligence purposes. The report compares the EU and US legal orders on government surveillance, which were central to the allegations influencing Mr. Schrems' complaint in Ireland. To assess the EU legal order, the report focuses on the laws in eight EU Member States (Belgium, France, Germany, Ireland, Italy, the Netherlands, Poland, and the UK). See further: Privacy and Civil Liberties Oversight Board: Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, July 2, 2014, see also the President's Review Group on Intelligence and Communications Technologies, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies (12 Dec 2013) available at: https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf; and Professor Peter Swire: US Surveillance Law, Safe Harbor, and Reforms, December 17, 2015.

[6] Opinion of Geoffrey Robertson QC, December 4, 2015, to be found at http://www.bcl.com/downloads/RobertsonSafeHarbour.pdf.

memorandum does not take into account, and therefore does not contain, any views on the adequacy of this new Safe Harbour agreement.

10. **Status of the Schrems case**. The CJEU referred the case back to the Irish High Court which, in its turn, referred the case back to the Irish DPA to investigate whether, in the absence of Safe Harbour Decisions, Facebook has valid grounds for data transfers to the U.S.

III. Impact of the Schrems judgement on EU data transfer grounds

Re (a) 'adequacy decisions' (Article 25 of the Directive)

11. The Safe Harbour Decision concerns an 'adequacy decision' under Article 25 of the Directive. The Schrems judgement focused only on the Safe Harbour Decision and whether it was an appropriate adequacy decision under Article 25. The Schrems judgement will likely impact other adequacy decisions under Article 25(6) because these also deny the national DPAs the powers which they derive from Article 28 of the Directive. Confirming this view, the Commission stated that Article 25(6) decisions may need to be amended following the Schrems judgment.[7]

Re (b) Specific data transfers grounds (Article 26 of the Directive)

12. In contrast, the derogations in Article 26 of the Directive are intended to allow transfers to jurisdictions that do not provide for adequate protection. The CJEU in the Schrems decision did not opine on the appropriateness of the derogations in Article 26. Following the Schrems decision, the Commission stated that the derogations in Article 26 remain valid.[8] Moreover, the derogations listed in Article 26 have all been maintained in the latest agreed text of the General Data Protection Regulation (**GDPR**),[9] demonstrating their continued relevance and validity. Far from reducing reliance on the derogations, the GDPR substantially extends the derogations in Article 26, recognising that the current transfer rules constitute substantial impediments to trade[10] and the limited value of the 'adequacy system' in practice for companies.[11]

---

7 "The scope of the judgment is limited to the Commission's Safe Harbor Decision. However, each of the other adequacy decisions contains a limitation on the powers of the DPAs that is identical to Article 3 of the Safe Harbor Decision and which the Court of Justice considered invalid. The Commission will now draw the necessary consequences from the judgment by shortly preparing a decision, to be adopted pursuant to the applicable comitology procedure, replacing that provision in all existing adequacy decisions." Communication on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgement of the Court of Justice in Case C-362/14 (Schrems) COM (2015) 566 Final, 6 November 2015 (the "**Commission Communication**"), pages 14 and 15.

8 Commission Communication, p. 15.

9 See Chapter V of the Regulation (EU) No XXX/2016 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - the text as agreed by the trilogue and adopted by the LIBE committee is available at: http://www.emeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE(2015)1217_1/sitt-1739884

10 See Chapter 2 of the Explanatory Memorandum of the Commission to the Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM/2012/011 final - 2012/0011 (COD), to be found at: http://eur-europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012PC0011&from=EN.

11 See WP169 'The Future of Privacy', Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, 1 December 2009, p. 2 and 11.

13. The legislative intent to permit transfers to countries that are not adequate is also set forth in the text of Article 26 of the Directive itself. Article 26(1) expressly provides that its operation is "by way of derogation from Article 25" and that EU Member States' data protection law "shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2) may take place on condition that …" (*emphasis added*).

14. The specific derogations provided by Article 26 of the Directive can (in their turn) be split into two categories:

(a) **Specific legal basis provided by Article 26(1) of the Directive**: such as (a) where the individual has given consent for the transfer; when the transfer is (b) necessary in relation to a contract ('contractual necessity') or (c) a legal claim; (d) necessary or legally required on important public interest grounds; or (e) necessary in order to protect the vital interests of the data subject. These derogations are also included in the GDPR. In addition, the GDPR provides that a data transfer may, under limited circumstances, be justified on a legitimate interest of the controller or processor.[12]

Note. As to the legal basis of consent, it should be noted that EU data protection law expressly recognises that consent is a core part of the right to data protection. The consent-derogation is based on the essential premise that a data subject is aware of the risks that he or she is assuming by permitting the export of their personal data outside of the EEA to the specified data importer, but chooses to act regardless, having been informed of the transfer.[13] This is in line with Article 8 of the Charter of Fundamental Rights, which expressly recognises that consent is a core part of the right to data protection.[14] Consent is an important safeguard which respects data subjects' autonomy, allowing individuals to control the access to and collection of their information.[15]

Also the "contractual necessity"-basis is based on the premise that a data subject is aware of the risks that he or she is assuming by entering into a transaction where it is necessary for their personal data to be exported outside of Europe.[16] In other words, data subjects are free to determine whether or not they enter into contracts that would inherently require the transfer of their data outside the EU.

(b) **The controller "adduces adequate safeguards" pursuant to Article 26(2) of the Directive:** the Directive explicitly envisages that the data exporter and data importer may also agree to safeguards specifically for their transfer arrangement, in particular in the form

---

12 Article 44(1)(h) GDPR.

13 This is expressly stated as the intention behind Article 26(1) in the travaux préparatoires – see COM(92) 422 final - SYN 287 at page 35.

14 Article 8(2) of the Charter explicitly recognises that the ability of data subjects to consent (or not) to how their data is used is a primary aspect of the right to the protection of personal data: "data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law" (emphasis added).

15 By analogy, it has been held that there was no interference with Article 10 of the European Convention of Human Rights where the individual had agreed or contracted to limit his freedom of expression – see *Vereniging Rechtswinkels Utrecht v Netherlands 46 DR 1986, EcomHR.* See also, by analogy, the case of *Stedman v UK (1997) 23 EHRR CD168* where the applicant complained that a requirement to work Sundays was an interference with her religious freedoms. The European Court of Human Rights held that the applicant had a free choice in employment, could have taken another job and thus the right was not engaged.

16 This is expressly stated as the intention behind Article 26(1) in the *travaux préparatoires* – see footnote 11.

> of contractual clauses. Article 26(2) allows Member States to authorise transfers "to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights" whereby "such safeguards may in particular result from appropriate contractual clauses". These contractual solutions include the use of Standard Contractual Clauses issued by the Commission under Article 26(4) of the Directive (see Sections 20 - 27), and, with regard to transfers between the different entities of a multinational corporate group, Binding Corporate Rules authorised by national DPAs (see Sections 28 - 31). To provide more flexibility for companies, the GDPR adds, as new components, that appropriate safeguards may also be provided for by approved codes of conduct and certification mechanisms, as well as standard data protection clauses adopted by a DPA and declared generally valid by the Commission.[17]

15. Compared to 'adequacy decisions' which result from the overall assessment of a given third country's system and which in principle may cover all transfers to that system, the alternative bases for transfers under Article 26 have both a more limited scope (as they apply only to specific data flows) and a broader coverage (as they are not necessarily confined to a specific country). They apply to data flows carried out by particular entities which have decided to make use of one of the possibilities offered by Article 26 of the Directive.[18]

Re (a) specific legal bases Article 26(1) of the Directive

16. The Schrems judgment has no relevance for an analysis of the derogations provided for by Article 26(1) of the Directive. Article 26(1) is designed to set up a framework to allow the transfer of personal data in specific cases where the EU regulators determined that certain transfers should be permitted regardless of the lack of adequacy in the regime of the data importer (for example, where the data subject him/herself has exercised choice (consenting to the transfer), where there are circumstances necessitating the transfer (performance of a contract), or in circumstances of important public interest or the vital interest of the individual). Those determinations are entirely separate from the analysis of adequacy. By definition, the failure of the Commission to properly assess adequacy in the Safe Harbour context should therefore have no bearing on whether the derogations under Article 26 are appropriate. Following the Schrems judgement, the Commission therefore stated that the derogations in Article 26(1) remain valid:

> "In the absence of an adequacy decision under Article 25(6) of Directive 95/46/EC and irrespective of the use of SCCs and/or BCRs, personal data may still be transferred to entities established in a third country to the extent that one of the alternative derogations set out in Article 26(1) of Directive 95/46/EC applies;" [19]
>
> and
>
> "These grounds provide a derogation from the general prohibition of transferring personal data to entities established in a third country without an adequate level of protection. In fact, the data exporter does not have to ensure that the data importer will provide adequate

[17] Article 42(2) GDPR.

[18] See in these words in Commission Communication, p. 5.

[19] Commission Communication, para. 2.3.

protection, and he will usually not need to obtain prior authorisation for the transfer from the relevant national authorities."[20]

17. Moreover, we note that the DPAs of the Member States do not have the authority to declare one of the specific derogations of Article 26(2) of the Directive invalid. This is the prerogative of the CJEU only.

18. However, as held by the CJEU (*Schrems para.* 57), the national DPAs remain authorised, when hearing a claim lodged by a person concerning his or her data protection rights, to examine, whether the relevant transfer of that data complies with the requirements laid down by the Directive. Such investigation will, however, be restricted to examining whether the requirements for the relevant legal basis are met, *e.g.*, whether consent in the specific case is freely given or whether contractual necessity exists. In these evaluations, the 'adequacy' of the regime of the data importer is not relevant.

Re (b) controller "adduces adequate safeguards" pursuant to Article 26(2) of the Directive

19. Controllers can 'adduce adequate safeguards' pursuant to Article 26(2) by entering into Standard Contractual Clauses for the transfer of data to processors and controllers in third countries (**SCCs**) or by adopting Binding Corporate Rules (**BCR**).

Re SCCs

20. Since 2001 the Commission adopted a number of decisions under Article 26(4) approving standard contractual clauses for the transfer of data to processors and controllers in third countries (the "**SCC Decisions**").[21]

21. The SCCs derive from decisions of the Commission.[22] Such decisions are EU legal measures which are binding upon all Member States[23] (including national institutions such as DPAs). Commission decisions, such as the SCC Decisions, must also be presumed to be lawful, in accordance with well-established principles of EU law.[24] This presumption of legality was expressly reiterated by the CJEU in the Schrems judgment.[25]

---

20 Commission Communication, p. 9.

21 There are three relevant European Commission Decisions upon which the SCCs are founded: Commission Decision 2001/497/EC, Commission Decision 2004/915/EC and Commission Decision 2010/87/EU. This paper refers in particular to European Commission Decision 2010/87/EU (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) (in this note, referred to as the "**SCC Decision**") upon which EEA established data controllers may rely upon in respect of transfers of personal data to non-EEA data processors.

22 See footnote above.

23 Article 288 of the TFEU provides that "*A decision shall be binding in its entirety. A decision which specifies those to whom it is addressed shall be binding only on them.*" The SCC Decision is addressed to all Member States.

24 See Case C-475/01 *Commission v Greece* paragraph 18; Case C-137/92 P *Commission* v *BASF and Others* paragraph 48; and Case C-245/92 P *Chemie Linz* v *Commission* paragraph 93.

25 *Schrems* paragraph 51: "*Measures of the EU institutions are in principle presumed to be lawful and accordingly produce legal effects until such time as they are withdrawn, annulled… or declared invalid*".

22. As noted above, the Schrems judgment confirmed that only the CJEU – not national regulators or courts – can strike down a SCC Decision.[26] Until such a time (if any) as this occurs, the SCC Decisions are binding on national courts and DPAs.

23. On 6 November 2015, the European Commission reiterated this position:

> "Since Commission decisions are binding in their entirety in the Member States, incorporating the SCCs in a contract means that national authorities are in principle under the obligation to accept those clauses. Consequently, they may not refuse the transfer of data to a third country on the sole basis that these SCCs do not offer sufficient safeguards".[27] (*emphasis added*)

24. However, as held by the CJEU (*Schrems, para.*57), it remains the case that national DPAs are authorised, when hearing a claim, to examine whether a specific data transfer under SCCs complies with the requirements laid down by the Directive. This competence of the DPAs is duly reflected in the SCCs themselves, where Article 4 of the SCCs provides that the DPAs may exercise their powers to suspend or prohibit data flows in cases where "the law to which the data importer or a sub-processor is subject imposes upon him requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society […], where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses" (*emphasis added*).[28]

25. The test to be applied here by the individual DPAs under Article 4 of the SCCs is very different from the assessment to be made by the Commission to decide on an adequacy decision (and as evaluated in the Schrems judgement):

- First of all, the Commission has already made an assessment in respect of the SCCs that these do adduce adequate contractual safeguards under Article 26(4) of the Directive. Note that also the function of the SCC Decisions by the Commission under Article 26(4) of the Directive is already very different from an 'adequacy decision'. In the latter case the Commission evaluates whether the laws of a country provide for adequate safeguards so transfers can take place without any additional mitigating (including contractual) measures. Under the SCC Decisions, the Commission evaluates whether a certain set of contractual clauses will offer sufficient safeguards[29] so transfers can take place to a country that does not provide for adequate protection. These two assessments: (1) whether the law is adequate or (2) whether contractual measures can provide sufficient safeguards if the law is not

---

26 *Schrems*, paragraph 61.

27 Commission Communication, p. 6.

28 See the full text of Clause 4(1)(a) SCCs under Decision 2010/87/EU:
"Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to Chapters II, III, V and VI of Directive 95/46/EC, the competent authorities in the Member States may exercise their existing powers to prohibit or suspend data flows to third countries in order to protect individuals with regard to the processing of their personal data in cases where:
(a) it is established that the law to which the data importer or a sub-processor is subject imposes upon him requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive 95/46/EC where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses."

29 Whether or not ultimately an adequate level of protection is in place "*should be assessed in the light of all the circumstances surrounding the data transfer operation*". Recital 3 of the SCC Decision.

adequate, are entirely different assessments based on different criteria (for which the Schrems judgement has no relevance).

- Commissions' decisions are binding upon the Member States and the DPAs and the SCCs Decisions are assumed to be valid, which in this case means that the DPAs will have to take as a given that the SCCs **in principle** provide for adequate contractual safeguards.

- For a national DPA to subsequently prohibit or suspend a transfer on the basis of Article 4(1)(a) of the SCC Decision, such DPA will need to conduct an investigation in order to establish whether, in the relevant specific circumstances of the case, the law of the importing country goes beyond "what is necessary in a democratic society" to such extent that despite the adequate contractual measures in the SCCs this is "likely to have a substantial adverse effect" on the individuals whose data are transferred.

26. It is clear, therefore, that this is a much more stringent test than the test to assess whether the laws of a country are adequate. This test requires a case-by case assessment by the DPA upon hearing a claim in respect of a specific transfer, as to whether in the specific circumstances of the case, such substantial adverse effect on the individuals concerned is likely. Relevant factors in this assessment will include the nature of the data transferred (would the data concerned be of interest to U.S. governmental agencies to start with?), the purpose of the processing, number and type of subpoena's received by the data importer in the past (are these excessive in number or limited, do these concern specific investigations into e.g. fraud or are these of a generic nature, e.g. bulk tapping?), specific additional mitigating measures implemented by the data exporter and importer (e.g. encryption). Such factors will have to be assessed in light of the contractual safeguards adduced by the SCCs (see **examples below**). The DPA will further have to conduct its own assessment into the current state of the relevant law and practice in the destination country. As indicated in Section 9, the conclusions of the Commission Decision Rebuilding Trust (on which the CJEU based the Schrems judgement) are no longer current in light of recent more in depth research into U.S. law and practices (compared to EU law) and further recent changes in U.S. law, and therefore merit in-depth re-assessment.

27. DPAs which are requested to assess specific data transfers under SCCs can therefore not prohibit or suspend transfers on the sole consideration that the system of a country is not considered adequate due to too extensive government access and lack of redress for individuals (as the CJEU did in the Schrems judgement). It is therefore possible that the laws of a country will not be considered adequate due to too extensive government access powers and lack of redress for individuals, while specific transfers under the SCCs are allowed to such country. As noted previously, the SCCs are intended to facilitate transfers to countries whose systems are not considered adequate. Any other interpretation would lead to the current systems of derogations for data transfers to non-adequate countries under the Directive having no function. Transfers would then only be possible to countries providing an adequate protection, which is contrary to the legislative history of the Directive which recognises that data transfers to third countries are an intrinsic part of trade and that data exporters and data importers should be able to adduce adequate safeguards despite the fact that these third countries are not considered adequate.

Examples where SCCs provide for additional protections that address the shortcomings of the Safe Harbour system as identified by the CJEU, and for which such additional protections should be taken into account by national DPAs assessing specific transfers under Article 4 of the SCCs:

- **U.S. government access.** SCCs do not provide for any specific exceptions for sharing with governments or law enforcement agencies outside of the EU (as the Safe Harbour

Decision did, see Schrems, para. 82, as cited in Section 9). Rather SCCs require the data importer to promptly notify the data exporter of any legally binding request for disclosure by a law enforcement authority (unless otherwise prohibited), which enables and entitles the data exporter to suspend the transfer of data and/or terminate the contract. The data importer is further required to deal promptly and properly with all inquiries from the data exporter and to abide by the advice of the supervisory authority with regard to the relevant processing.[30]

- **Oversight, compliance monitoring and jurisdiction.** The CJEU held that the Safe Harbour Decision does not "refer to the existence of effective legal protection against interference" by U.S. government and further that "procedures before the Federal Trade Commission (…) are limited to commercial disputes (…) and the private dispute resolution mechanisms concern compliance by the United States undertakings with the safe harbour principles and cannot be applied in disputes relating to the legality of interference with fundamental rights that results from measures originating from the State." (*Schrems*, para. 88 and 89).

  In contrast, compliance with **SCCs** is entrusted to the DPAs themselves, and such compliance is reviewed under EU law.[31] Furthermore, in some EU member states SCCs are subject to prior approval by the national DPA, which means that national DPAs have the opportunity to conduct an *ex ante* review of transfers based on SCCs whereas no such approval was required for transfers based on Safe Harbour.[32]

- **Insufficient Judicial Redress**. The CJEU relied on Commission Communications (COM (2013) 846 final and COM (2013) 847 final) according to which individuals have "no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased" (*Schrems* para. 90, cited in Section 9).

  In contrast, **SCCs** provide for a right of action for individuals before EEA courts and/or DPAs.[33] Whereas Safe Harbour does not explicitly guarantee third party rights for individuals, SCCs give individuals the right to also obtain compensation for any damages they have suffered.[34]

Re BCR

28. Controllers and processors can also "adduce appropriate safeguards" under Article 26(2) for their intra-group transfers by adopting 'binding corporate rules'. As BCR are not codified in the Directive, BCR are subject to national authorisation by the national DPAs. Since 2003, the Working Party 29 (WP29) has adopted a series of Working Documents, setting out the criteria that the WP29 recommends being incorporated in BCR and considered by the national DPAs in their

30 Clause 5(d) and (e) of SCCs under Decision 2010/87/EU.

31 See, inter alia, Clauses 8 and 9 of SCCs under Decision 2010/87/EU, Section IV of Decision 2004/915/EC.

32 There are requirements for prior DPA approval of SCCs in Austria, Belgium, Croatia, Cyprus, Estonia, France, Hungary, Latvia, Lithuania, Luxembourg, Malta, Portugal (for transfers of non-sensitive data only), Romania, Slovenia, and Spain.

33 See Clause 7 of SCCs under Commission Decision 2010/87/EU and Section III of SCCs under Decision 2004/915/EC.

34 Article 6 of SCCs under Commission Decision 2010/87/EU and Section III of SCCs under Decision 2004/915/EC.

assessment of adequacy.[35] To stream-line the national approval procedures, the DPAs of 21 Member States joined the "Mutual Recognition Procedure" (MRP), which entails that a "lead" DPA (together with 2 co-leads) will evaluate and authorise BCR, and the other DPAs will mutually recognise such approval.[36]

29. The GDPR now explicitly includes BCR as a data transfer tool and codifies the criteria set out by the WP29.[37]

30. The authorisation of BCR by the lead DPA as to whether BCR meet the requirement of "adducing adequate safeguards" under Article 26(2) of the Directive is similar to the Commission assessing whether SCCs can be considered to adduce adequate contractual safeguards. The authorisation by the lead DPA is based on the criteria for approval for BCR set by the WP29 in its series of BCR Working Documents, which will now be codified in the GDPR, confirming that EU legislators also consider BCR to provide for appropriate safeguards for data transfers (in this case between group companies of a multinational corporation).

31. In Section 15, it was previously noted that BCR are both broader and more limited in scope than adequacy decisions; broader as they may cover transfers to all countries, and more limited as BCR cover transfers by a specific company only (rather than covering all transfers to a country). Thus, the assessment by the lead DPA as to whether BCR can be authorised under Article 26(2) of the Directive as adducing adequate safeguards should not be based on specific assessments of transfers to specific countries, but should be a **general assessment** of whether BCR meet the criteria set by the WP29 (and by the EU regulators in the GDPR) in respect of BCR. This general assessment must be distinguished from the assessment by DPAs, upon hearing a claim, as to whether specific transfers under specific BCR should be prohibited or suspended based on the powers conferred upon the DPAs under Article 28 of the Directive. In other words, it is possible that BCR receive an EU authorisation under Article 26(2) of the Directive as adducing adequate safeguards **in general** (as they indeed do, see **examples below**), while specific transfers under BCR are suspended by a DPA based on a case-by-case assessment (similar to the one under Article 4 of the SCCs).

32. It is further possible (as with SCCs), that the laws of a country are not considered adequate for reasons of too extensive government access powers and lack of redress for individuals, while DPAs, upon hearing a claim, come to the conclusion that the specific transfers to such country under BCR are allowed because, in the specific case, there is no substantial adverse impact on individuals. Such specific assessment, however, should not be part of the assessment to be made by a national DPA in the general authorisation procedure of BCRs under Article 26(2) of the Directive. Recent statements by certain national DPAs that they will no longer authorise BCR under Article 26(2) of the Directive are therefore unfounded.[38]

---

35 See WP 74 Transfer of personal data to third countries: applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on June 3, 2003 and subsequent Article Working Party documents WP 107, 108, 133, 153, 154, 155, 195, and 204.

36 See for a first press release Working Party 29 on 2 October 2008. See on the Mutual Recognition Procedure and for the member states that have joined the Mutual Recognition Procedure: http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/mutual_recognition/index_en.htm.

37 Article 42((2)(a) and 43 GDPR.

38 Such as the German DPAs of Rhineland-Palatinate, Schleswig-Holstein, and the German Conference of Data Protection Commissioners (Konferenz der Datenschutzbeafutragen des Bundes und der Länder), see

Examples where BCR provide for additional protections that address the shortcomings of the Safe Harbour system as identified by the CJEU, and which additional protections should be taken into account by national DPAs making their assessment in respect of specific transfers under BCR (similar to an assessment under Article 4 of the SCCs):

- **U.S. government access.** BCRs for Controllers **(BCR-C)** do not provide for any specific exception for sharing with governments or law enforcement agencies outside of the EU (as the Safe Harbour Decision did, see Schrems, para. 82, as cited in Section 9). Rather BCR-C require that where a member of the group has reasons to believe that the legislation applicable to it prevents the company from fulfilling its obligations under the BCR-C and has substantial effect on the guarantees provided by the rules, such member will promptly inform the EU headquarters (except where prohibited by law). In addition, the BCR-C require that where there is conflict between national law and the commitments in the BCR-C, the EU headquarters, will take a responsible decision on what action to take and will consult with the competent DPA in case of doubt.[39]

  BCRs for Processors (**BCR-P**) require that where a member of the processor's group has reasons to believe that legislation applicable to it may prevent it from fulfilling the instructions received from the controller, or its obligations under the BCR or the service agreement, it will promptly notify this to both the controller and the DPA competent for the controller.[40] BCR-P further require that a specific procedure be implemented for dealing with requests for disclosure of personal data by a law enforcement authority or state security body, which requires the processor to (i) assess each access request on a case-by-case basis as to whether it is valid and binding, (ii) to inform the controller and the lead DPA for the BCR-P of any legally binding Disclosure Requests, unless otherwise prohibited; (iii) to commit to putting the request on hold for a reasonable delay in order to notify the DPA competent for the controller and the lead DPA for the BCR-P prior to the disclosure to the requesting body; (iv) to use its best efforts to obtain the right to waive a prohibition to disclose; and (v) in any event provide to the competent DPA general information on the requests it received to the competent DPAs (*e.g.*, number of applications for disclosure, type of data requested, requester if possible, etc.).[41]

- **Oversight, compliance monitoring and jurisdiction.** As with SCCs, compliance with BCR is entrusted to the DPAs themselves, and such compliance is reviewed under EU law. Furthermore, BCR are subject to prior approval by the lead DPA, which means that such lead DPAs and the relevant co-leads, have the opportunity to conduct an *ex ante* review of transfers based on BCR, whereas no such approval was required for transfers based on Safe Harbour.[42]

- **Insufficient Judicial Redress**. BCR-C require an internal complaints handling process, which enables individuals to file a complaint against the group company in their own

---

for the position of the latter: http://www.bfdi.bund.de/SharedDocs/Publikationen/EU/Art29Gruppe/Safe-Harbor_Positionspapier-DSK_Engl.pdf?__blob=publicationFile&v=1.

39 See WP 74, section 3.3.3.

40 See WP 204, section 2.3.4.

41 See WP 204 section 2.3.4

42 See n. 36

country. BCR-C and BCR-P further provide for the possibility for individuals to lodge a complaint before the competent DPAs and before the EU courts.[43]

IV. Conclusions

33. In conclusion, the *Schrems* judgment confirmed that only the CJEU – not national regulators or courts – can strike down a derogation under Article 26.[44]

34. The derogations in Article 26 of the Directive are of a different nature to the adequacy decisions and the considerations of the Commission in the Safe Harbour Decision. The CJEU observations in the Schrems judgement concerning the 'adequacy' of U.S. law are therefore inapplicable to the Article 26 derogations.

35. The derogations of Article 26 of the Directive remain valid, including the SCCs. Recent blanket statements by certain national DPAs that they will no longer authorise transfers under SCCs are therefore legally unfounded.

36. Any authorisation of BCR by a lead DPA under the Mutual Recognition Procedure under Article 26(2) of the Directive should not be based on specific assessments of transfers to specific countries, but should be a **general assessment** of whether the BCRs meet the criteria set by the WP29 (and by the EU regulators in the GDPR) in respect of BCRs. This general assessment must be distinguished from the assessment by DPAs, upon a claim, whether specific transfers under specific BCRs should be prohibited or suspended based on the powers conferred upon the DPAs under Article 28 of the Directive. Recent statements by certain national DPAs that they will no longer authorise BCR under Article 26(2) of the Directive are therefore unfounded.

37. National DPAs remain at all times authorised, when hearing a claim, to examine such claim with the powers conferred upon the DPAs under Article 28 of the Directive, whether the relevant specific data transfer complies with the requirements laid down by the Directive.

- **Specific legal bases Article 26(1) of the Directive**: if the relevant transfer is based on a specific legal basis of Article 26(1), the investigation by the national DPAs should be restricted to evaluating whether the requirements for the relevant legal basis are met, e.g. whether consent is freely given or whether contractual necessity exist. In these evaluations the 'adequacy' of the laws of the country of destiny is not of relevance and should not be taken into account.

- **Controller adduces adequate safeguards under Article 26(2) of the Directive**: when DPAs receive a claim that specific transfers under SCCs or BCR are in violation of the Directive, the relevant DPA has to conduct an investigation in order to establish whether in the relevant specific circumstances of the case, the law of the importing country goes beyond "what is necessary in a democratic society" to such extent that despite the adequate contractual measures in the SCCs or BCRs it is " likely to have a substantial adverse effect" on the individuals whose data are transferred under the relevant mechanism. This requires a case-by-case assessment considering all relevant circumstances including the state of the relevant law and practice in the destination country, the nature of the data transferred, the number and type of subpoena's the data importer normally receives as well as any mitigating measures taken by the data exporter and the data importer. The 'adequacy' of the

[43] See WP 74, Section 5.6 and WP 204, Section 4.3and 4.7.

[44] *Schrems*, paragraph 61.

laws of the country of destiny is one factor only and can in itself not be the basis for deciding that the transfers under SCCs or BCR should be prohibited or suspended.

38. DPAs when making this assessment will have to take new developments into account, such as recent research into the adequacy of U.S. law, government access powers to data of European citizens and the safeguards provided to them in respect thereof, as well as into government access powers in the EU and safeguards provided to EU individuals thereunder (in order to establish equivalence as to what "goes beyond what is necessary in a democratic society"). In any event, based on this research, the conclusions of the Commission Decision Rebuilding Trust seem no longer current and merit (a more in depth) re-assessment.

***