Council of the European Union

Brussels, 9 November 2015
(OR. en)

13819/15

DATAPROTECT 189
USA 32
JAI 834
MI 701
DIGIT 86
FREMP 247
DAPIX 197

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	6 November 2015
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2015) 566 final
Subject:	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)

Delegations will find attached document COM(2015) 566 final.

Encl.: COM(2015) 566 final

EUROPEAN
COMMISSION

Brussels, 6.11.2015
COM(2015) 566 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)

1. INTRODUCTION: THE ANNULMENT OF THE SAFE HARBOUR DECISION

The Court of Justice of the European Union (hereafter: "the Court of Justice" or "the Court") ruling of 6 October 2015 in Case C-362/14 (Schrems)[1] reaffirms the importance of the fundamental right to protection of personal data, as enshrined in the Charter of Fundamental Rights of the EU, including when such data are transferred outside the EU.

Transfers of personal data are an essential element of the transatlantic relationship. The EU and the United States are each other's most important trading partners, and data transfers, increasingly, form an integral part of their commercial exchanges.

In order to facilitate these data flows, while ensuring a high level of protection of personal data, the Commission recognised the adequacy of the Safe Harbour framework through the adoption of Commission Decision 2000/520/EC of 20 July 2000 (hereafter: "the Safe Harbour Decision"). In this decision, based on Article 25(6) of Directive 95/46/EC[2], the Commission had recognised the Safe Harbour Privacy Principles and accompanying Frequently Asked Questions (FAQs) issued by the Department of Commerce of the United States as providing adequate protection for the purposes of personal data transfers from the EU[3]. As a result, personal data could be freely transferred from EU Member States to companies in the United States which signed up to the Principles, despite the absence of a general data protection law in the United States. The functioning of the Safe Harbour arrangement relied on commitments and self-certification of adhering companies. While signing up to Safe Harbour Privacy Principles and FAQs is voluntary, these rules are binding under U.S. law for those entities that have signed up to them and enforceable by the U.S. Federal Trade Commission[4].

In its judgment of 6 October 2015, the Court declared the Safe Harbour Decision invalid. It is against this background that the present Communication aims to provide an overview of the alternative tools for transatlantic data transfers under Directive 95/46/EC in the absence of an

---

1 Judgment of 6 October 2015 in Case C-362/14 Maximilian Schrems v Data Protection Commissioner, EU:C:2015:650 (hereafter also: "the judgment" or "the Schrems ruling").

2 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 L 281 of 23.11.95, p. 31 (hereafter: "Directive 95/46/EC" or "the Directive").

3 For the purposes of this Communication, the term "EU" shall also cover the EEA. Hence, references to "Member States" shall be understood to also cover EEA Member States.

4 For a more in-depth overview of the Safe Harbour arrangement, see Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM/2013/847 final.

adequacy decision. It also briefly describes consequences of the judgment for other Commission adequacy decisions. In the judgment, the Court clarified that an adequacy decision under Article 25(6) of Directive 95/46/EC is conditional on a finding by the Commission that in the third country concerned there is a level of protection of personal data which, while not necessarily identical, is "essentially equivalent" to that guaranteed within the EU by virtue of the Directive read in the light of the Charter of Fundamental Rights. Regarding specifically the Safe Harbour Decision the Court held that it did not contain sufficient findings by the Commission on the limitations as regards access by U.S. public authorities to data transferred under that decision and on the existence of effective legal protection against such interference. In particular, the Court clarified that legislation permitting public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life. Furthermore, the Court confirmed that even where there is an adequacy decision under Article 25(6) of Directive 95/46/EC, the Member States' Data Protection Authorities (DPAs) remain empowered and obliged to examine, with complete independence, whether data transfers to a third country comply with the requirements laid down by Directive 95/46/EC, read in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights. However, the Court also affirmed that only the Court of Justice can declare an EU act, such as a Commission adequacy decision, invalid.

The Court's judgment draws on the Commission's 2013 Communication on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU[5], in which the Commission identified a number of shortcomings and set out 13 recommendations. On the basis of these recommendations, the Commission has held talks with the U.S. authorities since January 2014 with the aim of putting in place a renewed and stronger arrangement for transatlantic data exchanges.

Following the judgment, the Commission remains committed to the goal of a renewed and sound framework for transatlantic transfers of personal data. In this respect, it has immediately resumed and stepped up its talks with the U.S. government in order to ensure that any new arrangement for transatlantic transfers of personal data fully complies with the standard set by the Court. Any such framework must therefore have sufficient limitations, safeguards and judicial control mechanisms in place to ensure the continued protection of the personal data of EU citizens including as regards possible access by public authorities for law enforcement and national security purposes. In the interim, concerns have been expressed by industry regarding the possibilities for continued data transfers[6]. There is thus a need to

---

5 Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847 final, 27.11.2013. See also Communication from the Commission to the European Parliament and the Council, "Restoring Trust in EU-US data flows", COM(2013) 846 final, 27.11.2013, and the related Memorandum "Restoring Trust in EU-US data flows – Frequently Asked Questions", MEMO/13/1059, 27.11.2013.

6 Representatives of industry associations voiced these concerns, inter alia, at a meeting organised shortly after the Schrems judgment by Vice President Ansip and Commissioners Jourová and Oettinger on 14 October. See Daily News of 14.10.2015 (MEX/15/5840). See also: "Open letter on the implementation of the CJEU Judgement on Case C-362/14 Maximillian Schrems v Data Protection Commissioner" dated 13 October 2015 addressed to Commission President Jean-Claude Juncker and signed by various EU and US

clarify under which conditions such transfers can continue. This has prompted the Article 29 Working Party – the independent advisory body that brings together representatives of all DPAs of the Member States as well as the European Data Protection Supervisor – to issue, on 16 October, a statement[7] regarding the first conclusions to be drawn from the judgment. Among other points, this statement contained the following guidance on data transfers:

- data transfers can no longer be based on the Commission's invalidated Safe Harbour Decision;

- Standard Contractual Clauses (hereafter also: "SCCs") and Binding Corporate Rules (hereafter also: "BCRs") can in the meantime be used as a basis for data transfers, although the Article 29 Working Party also stated that it will continue to analyse the impact of the judgment on these alternative tools.

The statement further called on Member States and EU Institutions to enter into discussions with the U.S. authorities with a view to find legal and technical solutions for data transfers; the negotiations for a new Safe Harbour could, in the view of the Article 29 Working Party, be part of this solution.

The Article 29 Working Party announced that if, by the end of January 2016, no appropriate solution is found with the U.S. authorities, and depending on the assessment of alternative tools for data transfers, the DPAs will take all necessary and appropriate action, including coordinated enforcement action.

Finally, the Article 29 Working Party stressed the shared responsibility of the DPAs, the EU Institutions, Member States and businesses to find sustainable solutions to implement the Court's judgment. In particular, the Working Party urged businesses to consider putting in place any legal and technical solutions to mitigate any possible risks they face when transferring data.

The present Communication is without prejudice to the powers and duty of the DPAs to examine the lawfulness of such transfers in full independence[8]. It does not lay down any binding rules and fully respects the powers of national courts to interpret the applicable law and, where necessary, to make a reference to the Court of Justice for a preliminary ruling. Nor can this Communication form the basis for any individual or collective legal entitlement or claim.

---

industry associations and companies: http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=1045&PortalId=0&TabId=353

7 Statement of the Article 29 Working Party, available on the internet at: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

8 See Article 8(3) of the Charter of Fundamental Rights and Article 16(2) TFEU. This independence has also been stressed by the Court in its Schrems ruling.

2. ALTERNATIVE BASES FOR TRANSFERS OF PERSONAL DATA TO THE U.S.

The rules on international data transfers laid down in Directive 95/46/EC are based on a clear distinction between, on the one hand, transfers to third countries ensuring an adequate level of protection (Article 25 of the Directive) and, on the other hand, transfers to third countries which have not been found to ensure an adequate level of protection (Article 26 of the Directive).

The Schrems ruling addresses the conditions under which, pursuant to Article 25(6) of Directive 95/46/EC, the Commission can determine that a third country affords an adequate level of protection.

Where the third country to which the personal data are to be exported from the EU has not been found to ensure this adequate level of protection, Article 26 of Directive 95/46/EC provides for a number of alternative grounds on which transfers may nevertheless take place. In particular transfers may be carried out where the entity responsible for determining the purposes and means of the processing of personal data (the "controller"):

– adduces appropriate safeguards, within the meaning of Article 26(2) of Directive 95/46/EC, regarding the protection of the privacy and fundamental rights and freedoms of individuals as well as with respect to the exercise of those rights. Such safeguards can notably be provided by means of contractual clauses binding the exporter and the importer of the data (see sections 2.1 and 2.2 below). These include SCCs issued by the Commission, and, with regard to transfers between the different entities of a multinational corporate group, BCRs authorised by DPAs; or

– relies on one of the derogations expressly listed in letters (a) to (f) of Article 26(1) of Directive 95/46/EC (see section 2.3 below).

Compared to adequacy decisions which result from the overall assessment of a given third country's system and may in principle cover all transfers to that system, these alternative bases for transfers 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 Directive 95/46/EC. Moreover, when basing their transfers on such grounds, and as they cannot rely on a finding of adequacy of the third country contained in a Commission decision, data exporters and importers bear the responsibility of ensuring that the transfers comply with the requirements of the Directive.

2.1. Contractual solutions

As highlighted by the Article 29 Working Party, in order to offer sufficient safeguards for the purposes of Article 26(2) of Directive 95/46/EC, contractual clauses "must satisfactorily compensate for the absence of a general level of adequate protection, by including the

essential elements of protection which are missing in any given particular situation"[9]. With the aim of facilitating the use of such instruments in international transfers, the Commission has approved, in accordance with Article 26(4) of the Directive, four sets of SCCs considered as fulfilling the requirements of Article 26(2) of the Directive. Two sets of model clauses relate to transfers between controllers[10], while the other two sets of model clauses concern transfers between a controller and a processor acting under its instructions[11]. Each of these sets of model clauses lays down the respective obligations of data exporters and importers. These include obligations as regards, *inter alia,* security measures, information to the data subject in case of transfer of sensitive data, notification to the data exporter of access requests by the third countries' law enforcement authorities or of any accidental or unauthorised access, and the rights of data subjects to the access, rectification and erasure of their personal data, as well as rules on compensation for the data subject in case of damage arising from a breach by either party to the SCCs. The model clauses also require EU data subjects to have the possibility to invoke before a DPA and/or a court of the Member State in which the data exporter is established the rights they derive from the contractual clauses as a third party beneficiary[12]. These rights and obligations are necessary in contractual clauses because, in contrast to the situation where the Commission has made an adequacy finding, it cannot be presumed that the data importer in the third country is subject to an adequate system of oversight and enforcement of data protection rules.

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 the data to a third country on the sole basis that these SCCs do not offer sufficient safeguards. This is without prejudice to their power to examine these clauses in the light of the requirements set out by the Court in the Schrems ruling. In case of doubts, they should bring a case before a national court which in turn may make a request for a preliminary ruling to the Court of Justice. While there is no requirement for a prior national authorisation to proceed with the transfer in most Member States' legislation transposing Directive 95/45/EC, some Member States maintain a system of notification and/or pre-authorisation for the use of the SCCs. Where they do so, the national DPA has to compare the clauses actually contained in the contract at issue with the

---

9 See Article 29 Working Party, "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive" (WP 12), 24 July 1998, p. 16.

10 Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC, OJ L 181, 4.7.2001, p. 19, and Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, OJ L 385, 29.12.2004, p. 74.

11 Commission Decision 2002/16/EC of 27 December 2001 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 L 6, 10.1.2002, p. 52, and Commission Decision 2010/87/EU 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 L 39, 12.2.2010, p. 5. The former decision, which was repealed by the latter, applies only to contracts concluded before 15 May 2010.

12 See e.g. recital 6 of Commission Decision 2004/915/EC and Clause V of its Annex; Clause 7 of the Annex to Commission Decision 2010/87/EU.

SCCs and verify that no change has been made[13]. If the clauses have been used without amendment[14], the authorisation is in principle[15] automatically granted[16]. As further explained below (see section 2.4), this is without prejudice to additional measures the data exporter may have to take, in particular further to information received from the data importer on changes in the third country's legal system that may prevent the data importer from fulfilling its obligations under the contract. In the application of SCCs, both data exporters and, by subjecting themselves to the contract, data importers fall under the supervision of DPAs.

The adoption of SCCs does not prevent companies from relying on other instruments, such as *ad hoc* contractual arrangements, to demonstrate that their transfers take place with sufficient safeguards within the meaning of Article 26(2) of Directive 95/46/EC. Pursuant to Article 26(2) of the Directive, these need to be approved on a case-by-case basis by national authorities. Some DPAs have developed guidance in this field, including in the form of standardised contracts or detailed rules to be followed in drafting the data transfer clauses. Most contracts currently used by companies to carry out their international data transfers are, however, based on Commission-approved SCCs[17].

2.2. Intra-group transfers

To transfer personal data from the EU to affiliates located outside the EU in compliance with the requirements set out in Article 26(2) of Directive 95/46/EC, a multinational company can adopt BCRs. This type of code of practice provides a basis only for transfers made within the corporate group.

The use of BCRs thus allows personal data to move freely among the various entities of a corporate group worldwide – dispensing with the need to have contractual arrangements between each and every corporate entity – while ensuring that the same high level of

---

13 It should be noted that the proposal for the General Data Protection Regulation (COM(2012) 11 final) foresees that transfers based on SCCs or BCRs, to the extent that these have been adopted by the Commission or in accordance with the envisaged consistency mechanism, shall not require any further authorisation.

14 The use of SCCs does not, however, prevent the parties from agreeing to add other clauses, as long as they do not directly or indirectly contradict the clauses approved by the Commission or prejudice fundamental rights or freedoms of the data subjects. See European Commission, "Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries" (FAQ B.1.9), p. 28 (available on the internet at: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf).

15 If a DPA has doubts about the compatibility of SCCs with the requirements of the Directive, it should refer the question to a national court which can then make a reference for a preliminary ruling to the Court of Justice (cf. § 51, 52, 64 and 65 of the Schrems ruling).

16 The Article 29 Working Party has established a specific cooperation procedure between DPAs for the approval of contractual clauses that a company is seeking to use in different Member States. See Article 29 Working Party, "Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on 'Contractual clauses' Considered as compliant with the EC Model Clause" (WP 226), 26 November 2014. See also Clause VII of the Annex to Commission Decision 2004/915/EC, and Clause 10 of the Annex to Commission Decision 2010/87/EU.

17 See Article 29 Working Party, "Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on 'Contractual clauses' Considered as compliant with the EC Model Clause" (WP 226), 26 November 2014, p. 2.

protection of personal data is complied with throughout the group by means of a single set of binding and enforceable rules. Having a single set of rules creates a simpler and more effective system, which is easier for staff to implement and for data subjects to understand. With a view to helping companies in the drafting of BCRs, the Article 29 Working Party has spelled out the substantive (e.g. purpose limitation, security of processing, transparent information to data subjects, restrictions on onward transfers outside the group, individual rights of access, rectification and opposition) and procedural (e.g. audits, monitoring of compliance, complaints' handling, cooperation with DPAs, liability and jurisdiction) requirements for BCRs based on EU data protection standards[18]. These rules are not only binding on the members of the corporate group but, similarly to the SCCs, they are also enforceable in the EU: individuals whose data are being processed by an entity of the group shall be entitled as third-party beneficiaries to enforce compliance with BCRs by lodging a complaint before a DPA and bringing an action before a Member State court. Furthermore, the BCRs must designate an entity within the EU which accepts liability for breaches of the rules by any member of the group outside of the EU which is bound by these rules.

Under most Member States' laws transposing the Directive, data transfers on the basis of BCRs have to be authorised by the DPA in each Member State from which the multinational company intends to transfer data. To facilitate and speed up the process, as well as lessen the burdens on applicants, the Article 29 Working Party has established a standardised application form[19] and a specific co-operation procedure between concerned DPAs[20] which includes the designation of one "lead authority" responsible for handling the approval procedure.

2.3. Derogations

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:[21]

– the data subject has unambiguously given his/her consent to the proposed transfer;

---

18 See Article 29 Working Party, "Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules" (WP 153), 24 June 2008; "Working Document setting up a framework for the structure of Binding Corporate Rules" (WP 154), 24 June 2008; and "Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules" (WP 155), 24 June 2008.

19 Article 29 Working Party, "Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data" (WP 133), 10 January 2007.

20 Article 29 Working Party, "Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From 'Binding Corporate Rules'" (WP 107), 14 April 2005.

21 As the Article 29 Working Party has stressed, to the extent that other provisions of Directive 95/46/EC contain additional requirements relevant for the use of these derogations (for example the limitations of Article 8 for the processing of sensitive data), these need to be respected. See Article 29 Working Party, "Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995" (WP 114), 25 November 2005, p. 8. See also European Commission, "Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries" (FAQ D.2), p. 50.

– the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request;

– the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party;

– the transfer is necessary or legally required on important public interest grounds[22], or for the establishment, exercise or defence of legal claims;

– the transfer is necessary in order to protect the vital interests of the data subject;

– the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

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 protection, and he will usually not need to obtain prior authorisation for the transfer from the relevant national authorities. Nevertheless, due to their exceptional character, the Article 29 Working Party considers that these derogations have to be strictly interpreted[23].

The Article 29 Working Party has issued several non-binding guidance documents on the application of Article 26(1) of Directive 95/46/EC[24]. These include a number of "best practice" rules that are devised to orientate the enforcement action of the DPAs[25]. In particular, the Working Party recommends that transfers of personal data which might be qualified as repeated, mass or structural should be carried out with sufficient safeguards and, where possible, within a specific legal framework such as SCCs or BCRs[26].

---

22 This may include, for example, data transfers between tax or customs authorities, or between services competent for social security matters (see recital 58 of Directive 95/46/EC). Transfers between supervisory bodies in the financial services sector may also benefit from the derogation. See Article 29 Working Party, "Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive" (WP 12), 24 July 1998, p. 25.

23 Article 29 Working Party, "Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995" (WP 114), 25 November 2005, p. 7, 17.

24 Article 29 Working Party, "Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive" (WP 12), 24 July 1998; "Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995" (WP 114), 25 November 2005. See also European Commission, "Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries" (FAQ D.1 to D.9), p. 48-54.

25 Article 29 Working Party, "Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995" (WP 114), 25 November 2005, p. 8-10.

26 Article 29 Working Party, "Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995" (WP 114), 25 November 2005, p. 9. According to the Working Party, mass

In the present Communication, the Commission will only address those derogations which appear particularly relevant to transfers in the commercial context following the finding that the Safe Harbour Decision is invalid.

2.3.1. Transfers necessary for the performance of a contract or the implementation of pre-contractual measures taken in response to the data subject's request (Article 26(1)(b))

This derogation might be applicable, for example, in the context of a hotel reservation, or when payment information is transferred to a third country in order to effect a bank transfer. However, in each of these cases the Article 29 Working Party considers that there has to be a "close and substantial connection", a "direct and objective link" between the data subject and the purposes of the contract or the pre-contractual measure (necessity test)[27]. Also, the derogation cannot be applied to transfers of additional information not necessary for the purpose of the transfer, or transfers for a purpose other than the performance of the contract (for example, follow-up marketing)[28]. As regards pre-contractual measures, the Article 29 Working Party took the view that only contacts initiated by the data subject (for example, a request for information about a particular service) would be covered but not those resulting from marketing approaches made by the data controller[29].

2.3.2. Transfers necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller or a third party (Article 26(1)(c))

This derogation might be applicable, for example, when the data subject is the beneficiary of an international bank transfer, or when a travel agent forwards the details of a flight booking to an airline. Again, the necessity test applies and in this case requires a close and substantial link between the data subject's interest and the purpose pursued with the contract.

2.3.3. Transfers necessary or legally required for the establishment, exercise or defence of legal claims (Article 26(1)(d))

This derogation might be applicable, for example, where a company needs to transfer data to defend itself against a legal claim, or to make such a claim in court or before a public

---

or repeated transfers may only be carried out on the basis of a derogation where recourse to SCCs or BCRs is impossible in practice and where the risks to data subjects are small (e.g. international money transfers). See also European Commission, "Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries" (FAQ D.1), p. 49.

27 Article 29 Working Party, "Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995" (WP 114), 25 November 2005, p. 13. See also "Opinion 6/2002 on transmission of passenger manifest information and other data from airlines to the United States" (WP 66), 24 October 2002.

28 Article 29 Working Party, "Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive" (WP 12), 24 July 1998, p. 24; "Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995" (WP 114), 25 November 2005, p. 13.

29 Article 29 Working Party, "Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive" (WP 12), 24 July 1998, p. 24.

authority. As for the two previous derogations, this is subject to the necessity test:[30] there should be a close connection with litigation or legal (including administrative) proceedings.

According to the Article 29 Working Party, the derogation can only be applied if any international rules on cooperation in criminal or civil proceedings governing the type of transfer have been complied with, notably as they derive from the provisions of the Hague Convention of 18 March 1970 ("Taking of Evidence" Convention)[31].

2.3.4. Unambiguous prior consent by the data subject to the proposed transfer (Article 26(1)(a))

While consent can be used as the basis for data transfers, a number of considerations should be taken into account. Since consent must be given to the "proposed" transfer, this requires prior consent for the particular transfer (or a particular category of transfers). Where it is requested online, the Article 29 Working Party has recommended the use of boxes to be ticked (rather than pre-ticked boxes)[32]. Because the consent must be unambiguous, any doubt about whether it actually has been given would render the derogation inapplicable. This will likely mean that many situations where consent is at best implied (for example, because an individual has been made aware of a transfer and has not objected) would not qualify. Conversely, the derogation could be used in cases where the transferring entity has direct contact with the data subject, the necessary information can easily be provided and unambiguous consent obtained[33].

Moreover, according to Article 2 (h) of Directive 95/46/EC, consent must be freely given, specific and informed. According to the Article 29 Working Party, the first requirement means that any "pressure" may invalidate the consent. This is particularly relevant in the employment context, where the relationship of subordination and inherent dependency of employees will normally call into question reliance on consent[34]. More generally, consent

---

30 Article 29 Working Party, "Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995" (WP 114), 25 November 2005, p. 15. For example, in an employment context the derogation cannot be used to transfer all employee files to the group's parent company established in a third country on the grounds of possible future legal proceedings.

31 Hague Convention on the Taking of Evidence Abroad in Civil and Commercial Matters, *opened for signature* 18 March 1970, 23 U.S.T. 2555, 847 U.N.T.S. 241. This Convention covers, for example, pre-trial discovery or requests by the judicial authority of one state to the competent authority of another state to obtain evidence intended for use in judicial proceedings in the requesting state.

32 Article 29 Working Party, "Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995" (WP 114), 25 November 2005, p. 10, with reference to "Opinion 5/2004 on unsolicited direct marketing communications under Article 13 of Directive 2002/58/EC" (WP 90), 27 February 2004, point 3.2.

33 Article 29 Working Party, "Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive" (WP 12), 24 July 1998, p. 24.

34 Article 29 Working Party, "Opinion 8/2001 on the processing of personal data in the employment context" (WP 48), 13 September 2001, p. 3, 23 and 26. According to the Working Party, reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment. See also Article 29 Working Party, "Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995" (WP 114), 25 November 2005, p. 11.

given by a data subject who has not had the opportunity to make a genuine choice or has been presented with a *fait accompli* cannot be considered valid[35].

Of significant importance is that the data subjects are properly informed in advance that the data may be transferred outside the EU, to which third country and under which conditions (its purpose, the identity and details of the recipient(s), etc.). This information should address the specific risk that their data will be transferred to a third country lacking adequate protection[36]. Furthermore, as pointed out by the Article 29 Working Party, withdrawal of a data subject's consent, while not retroactive, should, as a principle, prevent any further processing of personal data[37]. In light of these limitations, the Article 29 Working Party takes the view that consent is unlikely to provide an adequate long-term framework for data controllers in cases of structural transfers[38].

2.4. Summary on alternative bases for transfers of personal data

It follows from the above that companies can use a number of different alternative tools for carrying out their international data transfers to third countries that are not deemed to grant an adequate level of protection within the meaning of Article 25(2) of Directive 95/46/EC. Following the Schrems ruling, the Article 29 Working Party has notably clarified that SCCs and BCRs can be used to transfer data to the U.S. while it continues its assessment and without prejudice to the powers of DPAs to investigate particular cases[39]. For its part, industry has reacted in different ways to the judgement including basing their data transfers on these alternative tools[40].

However, two important conditions need to be pointed out. First, it should be recalled that, irrespective of the specific legal basis relied on, transfers to a third country can be lawfully made only if the data have originally been collected and further processed by the data controller established in the EU in accordance with the applicable national laws transposing Directive 95/46/EC. The Directive expressly specifies that processing activity taking place prior to the transfer, as the transfer itself, must fully respect the rules adopted by Member States pursuant to the other provisions of the Directive[41]. Secondly, in the absence of a

---

35 Article 29 Working Party, "Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995" (WP 114), 25 November 2005, p. 11. See also "Opinion 6/2002 on transmission of passenger manifest information and other data from airlines to the United States" (WP 66), 24 October 2002.

36 Article 29 Working Party, "Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive" (WP 12), 24 July 1998, p. 24.

37 Article 29 Working Party, "Opinion 15/2011 on the definition of consent" (WP 187), 13 July 2011, p. 9.

38 Article 29 Working Party, "Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995" (WP 114), 25 November 2005, p. 11.

39 See Statement of the Article 29 Working Party of 16 October 2015 (above footnote 8).

40 A number of multinational companies have declared that they base their data transfers to the U.S. on alternative tools. See e.g. the statements by Microsoft (http://blogs.microsoft.com/on-the-issues/2015/10/06/a-message-to-our-customers-about-eu-us-safe-harbor/) or Salesforce (http://www.salesforce.com/company/privacy/data-processing-addendum-faq.jsp). Other U.S. companies such as Oracle have said that they offer cloud customers the ability to store their data in Europe so that it is not sent for storage elsewhere: http://www.irishtimes.com/business/technology/oracle-keeps-european-data-within-its-eu-based-data-centres-1.2408505?mode=print&ot=example.AjaxPageLayout.ot

41 See recital 60 and Article 25(1) of Directive 95/46/EC.

Commission finding of adequacy, the responsibility is on controllers to ensure that their data transfers take place with sufficient safeguards in accordance with Article 26(2) of the Directive. This assessment needs to be carried out in the light of all the circumstances surrounding the transfer at issue. In particular, both the SCCs and BCRs provide that if the data importer has reasons to believe that the legislation applicable in the recipient country may prevent it from fulfilling its obligations, it shall promptly inform the data exporter in the EU. In such a situation, it is up to the exporter to consider taking the appropriate measures necessary to ensure the protection of personal data[42]. These may range from technical, organisational, business-model related or legal or measures[43] to the possibility to suspend the data transfer or to terminate the contract. Taking into account all the circumstances of the transfer, data exporters may thus have to put in place additional safeguards to complement those afforded under the applicable legal basis for transfer to meet the requirements of Article 26(2) of the Directive.

Compliance with such requirements is ultimately to be assessed by DPAs on a case-by-case basis as part of the exercise of their supervision and enforcement functions, including in the context of the approval of contractual arrangements and BCRs or on the basis of individual complaints. While certain DPAs have expressed doubts about the possibility to use transfer instruments such as SCCs and BCRs for transatlantic data flows[44], in the statement it issued further to the Schrems ruling, the Article 29 Working Party announced that it will continue its analysis of the impact of the judgment on other transfer tools[45]. This is without prejudice to the powers of DPAs to investigate particular cases and to exercise their powers in order to protect individuals.

3. THE CONSEQUENCES OF THE SCHREMS RULING ON ADEQUACY DECISIONS

In its judgment, the Court of Justice does not call into question the powers of the Commission pursuant to Article 25(6) of Directive 95/46/EC to find that a third country ensures an adequate level of protection, as long as the requirements set out by the Court are respected. In

[42] See e.g. Clause 5 of the Annex to Commission Decision 2010/87/EU, and Article 29 Working Party, "Working Document setting up a framework for the structure of Binding Corporate Rules" (WP 154), 24 June 2008, p. 8.

[43] See e.g. guidance issued by the European Network and Information Security Agency (ENISA): https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf.

[44] See e.g. the position paper issued by the Data Protection Conference of the German Data Protection Authorities at Federal and State Level on 26.10.2015:https://www.datenschutz.hessen.de/ft-europa.htm#entry4521. Stressing that the Schrems ruling contains "strict substantive requirements" that both the Commission and the DPAs have to respect, the position paper indicates that the German DPAs will assess the lawfulness of data transfers based on alternative tools (SCCs, BCRs) and will no longer grant new authorisations for the use of these tools. In parallel, individual German DPAs have issued clear warnings that the alternative transfer tools are under legal scrutiny. See e.g. the position papers issued by the DPAs of Schleswig-Holstein:https://www.datenschutzzentrum.de/artikel/981-ULD-Position-Paper-on-the-Judgment-of-the-Court-of-Justice-of-the-European-Union-of-6-October-2015,-C-36214.html and of Rheinland-Pfalz: https://www.datenschutz.rlp.de/de/aktuell/2015/images/20151026_Folgerungen_des_LfDI_RLP_zum_EuGH-Urteil_Safe_Harbor.pdf.

[45] See Statement of the Article 29 Working Party of 16 October 2015 (above footnote 8).

line with these requirements, the 2012 proposal for a General Data Protection Regulation[46] to replace Directive 95/46/EC further clarifies and details the conditions under which adequacy decisions can be adopted. In the Schrems ruling, the Court also clarified that where the Commission adopts an adequacy decision, it is binding on all the Member States and their organs, including the DPAs until such time as it is withdrawn, annulled or declared invalid by the Court of Justice, which alone has jurisdiction in this regard. The DPAs remain competent to examine claims within the meaning of Article 28(4) of Directive 95/46/EC that the data transfer complies with the requirements laid down by the Directive (as interpreted by the Court of Justice), but cannot make a definitive finding. Rather, the Member States have to provide for the possibility to bring the case before a national court, which in turn can trigger the jurisdiction of the Court of Justice by way of a request for a preliminary ruling pursuant to Article 267 of the Treaty on the Functioning of the European Union (TFEU).

Moreover, the Court of Justice expressly confirmed that recourse by a third country to a system of self-certification (as with the Safe Harbour Privacy Principles) does not exclude an adequacy finding pursuant to Article 25(6) of Directive 95/46/EC as long as there are effective detection and supervision mechanisms that make it possible in practice to identify and sanction any infringements of the data protection rules.

Given that the Safe Harbour Decision did not contain sufficient findings in this regard, the Court of Justice declared the decision invalid. It is thus clear that data transfers between the EU and the United States can no longer be carried out on that basis, i.e. solely by invoking adherence to the Safe Harbour Privacy Principles. As data transfers to a third country which do not ensure an adequate level of protection (or at least where this has not been established in a Commission decision pursuant to Article 25(6) of Directive 95/46/EC) are in principle prohibited[47], they will only be lawful if the data exporter can rely on one of the alternative tools described above in Section 2. In the absence of an adequacy decision, it is the responsibility of the data exporter – under the control of the DPAs – to ensure that the conditions for relying on (one of) these tools are fulfilled with regard to the respective data transfer.

The scope of the judgement is limited to the Commission's Safe Harbour Decision. However, each of the other adequacy decisions[48] contains a limitation on the powers of the DPAs that is identical to Article 3 of the Safe Harbour Decision and which the Court of Justice considered

---

46 European Commission, 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). See also European Parliament, Legislative Resolution of 12 March 2014 on 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)0011 – C7-0025/2012 – 2012/0011(COD); Council, 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), Preparation of a General Approach, 9565/15. The proposal is currently in the final stage of the legislative process.

47 See recital 57 of Directive 95/46/EC.

48 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.

invalid[49]. 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. Also, the Commission will engage in a regular assessment of existing and future adequacy decisions, including through the periodic joint review of their functioning together with the competent authorities of the third country in question.

4. CONCLUSION

As confirmed by the Article 29 Working Party, alternative tools authorising data flows can still be used by companies for lawful data transfers to third countries like the United States. However, the Commission considers that a renewed and sound framework for transfers of personal data to the United States remains a key priority. Such a framework is the most comprehensive solution for ensuring effective continuity of the protection of personal data of European citizens when they are transferred to the United States. It also provides the best solution for transatlantic trade as it offers a simpler, less burdensome and therefore less costly transfer mechanism, in particular for SMEs.

Already in 2013, the Commission started negotiations with the U.S. government on a new arrangement for transatlantic data transfers based on its 13 recommendations[50]. There has been considerable progress in bringing the views of both sides together, for example on stronger monitoring and enforcement of the Safe Harbour Privacy Principles by, respectively, the U.S. Department of Commerce and the U.S. Federal Trade Commission, more transparency for consumers as to their data protection rights, easier and cheaper redress possibilities in case of complaints, and clearer rules on onward transfers from Safe Harbour companies to non-Safe Harbour companies (e.g., for processing or sub-processing purposes). Now that the Safe Harbour Decision has been declared invalid, the Commission has intensified the talks with the U.S. government to ensure that the legal requirements formulated by the Court are complied with. The objective of the Commission is to conclude these discussions and achieve this objective in three months.

Until such time as the renewed transatlantic framework is in place, companies need to rely on the alternative transfer tools available. However, this option entails responsibilities for data exporters, under the supervision of the DPAs.

In contrast to a situation where the Commission has found that a third country ensures an adequate level of data protection, on which data exporters can rely for the purposes of data transfers from the EU, the latter remain responsible for verifying that the personal data are effectively protected when using alternative tools. This may include having to take appropriate measures where necessary.

[49] See paragraphs 99-104 of the Schrems ruling.
[50] See above footnote 4.

In this regard, the DPAs have a central role to play. As the main enforcers of the fundamental rights of data subjects, the DPAs are both responsible for and empowered to supervise data transfers from the EU to third countries, in full independence. The Commission invites data controllers to cooperate with the DPAs, thereby helping them to effectively carry out their supervisory role. The Commission will continue to work closely with the Article 29 Working Party to ensure a uniform application of EU data protection law.