EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 1/2016

Preliminary Opinion on the agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences

12 February 2016

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 41(2) of Regulation 45/2001 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies', and '…for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data'. He was appointed in December 2014 together with Assistant Supervisor with the specific remit of being constructive and proactive. The EDPS published in March 2015 a five-year strategy setting out how he intends to implement this remit, and to be accountable for doing so.

This Opinion builds on the general obligation that international agreements concluded by the EU must comply with the provisions of the Treaty of the Functioning of the European Union (TFEU) and the respect for fundamental rights that stands at the core of EU law. In particular, the assessment is made so as to analyse the compliance of the content of the Umbrella Agreement with Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union and Article 16 TFEU ensuring personal data protection.

EXECUTIVE SUMMARY

Investigating and prosecuting crime is a legitimate policy objective, and international cooperation including information exchange has become more important than ever. Until now, the EU has lacked a robust common framework in this area and so there are no consistent safeguards for individuals' fundamental rights and freedoms. As the EDPS has long argued, **the EU needs sustainable arrangements for sharing personal data with third countries for law enforcement purposes, fully compatible with the EU Treaties and the Charter of Fundamental Rights**.

Therefore, **we welcome and actively support the efforts of the European Commission to reach a first 'Umbrella Agreement'**, with the US. This international law enforcement agreement aims at establishing for the first time data protection as the basis for information sharing. While we recognise that it is not possible to replicate entirely the terminology and definitions of EU law in an agreement with a third country, the safeguards for individuals must be clear and effective in order to fully comply with EU primary law.

The European Court of Justice in recent years has affirmed data protection principles including fairness, accuracy and relevance of information, independent oversight and individual rights of individuals. **These principles are as relevant for public bodies as they are for private companies, regardless of any formal EU adequacy finding** with respect to third countries data protection safeguards; indeed they become all the more important considering the sensitivity of the data required for criminal investigation.

This Opinion aims to provide constructive and objective advice to the EU institutions as the Commission finalises this delicate task, with broad ramifications, not only for EU-US law enforcement cooperation but also for future international accords. The 'Umbrella Agreement' is separate from but has to be considered in conjunction with the recently announced EU-US 'Privacy Shield' on the transfer of personal information in the commercial environment. Further considerations may be necessary to analyse the interaction between these two instruments and the reform of the EU's data protection framework.

Before the Agreement is submitted for the consent of the Parliament, we encourage the Parties to consider carefully significant developments since last September, when they signalled their intention to conclude the Agreement once the Judicial Redress Act is passed. Many safeguards already envisaged are welcome, but they should be reinforced, also in the light of the *Schrems* judgment in October invalidating the Safe Harbor Decision and the EU political agreement on data protection reform in December, which covers transfers and judicial and police cooperation.

The EDPS has identified three essential improvements which he recommends for the text to ensure compliance with the Charter and Article 16 of the Treaty:

- clarification that all the safeguards apply to all individuals, not only to EU nationals;
- ensuring judicial redress provisions are effective within the meaning of the Charter;
- clarification that transfers of sensitive data in bulk are not authorised.

The Opinion offers additional recommendations for clarification of the envisaged safeguards by way of an accompanying explanatory document. We remain at the disposal of the institutions for further advice and dialogue on this issue.

TABLE OF CONTENTS

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty of the Functioning of the European Union, and in particular its Article 16,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Articles 7, 8 and 47,

Having regard to 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,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, and in particular Article 41(2) and 46(d) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

I. Context of the initialled Agreement

1. On 3 December 2010, the Council adopted a decision authorising the Commission to open negotiations on an Agreement between the European Union (EU) and the United States of America (US) on the protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters (hereinafter: the "Agreement")[1].

2. The negotiations between the Commission and the US began officially on 29 March 2011[2]. On 25 June 2014, the United States Attorney General announced that legislative action will be taken in order to provide for judicial redress concerning privacy rights in the US for citizens of the EU[3]. After several rounds of negotiations, which extended over 4 years, the Agreement was initialled on 8 September 2015. According to the Commission, the objective is to sign and formally conclude the Agreement only after the US Judicial Redress Act is adopted[4].

3. The European Parliament must consent to the initialled text of the Agreement, while the Council must sign it. As long as this has not taken place and the Agreement is not formally signed, we note that the negotiations can be reopened on specific points. It is in this context that the EDPS issues this Opinion, based on the text of the initialled Agreement published on the website of the Commission[5]. This is a preliminary Opinion based on a first analysis of a complex legal text and it is without prejudice to any additional recommendations to be made on the basis of further available information, including legislative developments in the US, such as the adoption of the Judicial Redress Act. The EDPS has identified three essential points which require improvement and also highlights other aspects where important clarifications are recommended. With these improvements, the Agreement can be considered compliant with EU primary law.

II. Standards of EU law regarding international data transfers and the respect of fundamental rights

4. Pursuant to Article 216(2) TFEU, international agreements to which EU is a party, such as the Agreement, "*are binding upon the institutions of the Union and on the Member States*". Moreover, according to the settled case law of the Court of Justice of the European Union (CJEU), international agreements become from their entry into force "*an integral part of [the European legal order]*"[6], and they can have primacy over acts of secondary Union legislation[7].

5. The CJEU found, with respect to international agreements concluded by the EU, that "the obligations imposed by an international agreement *cannot have the effect of prejudicing the constitutional principles of the EC Treaty, which include the principle that all Community acts must respect fundamental rights*, that respect constituting a condition of their lawfulness which it is for the Court to review in the framework of the complete system of legal remedies established by the Treaty"[8]. The subsequent analysis takes as starting point the requirement for international agreements to be compliant with the EU system for the protection of fundamental rights.

6. From a variety of legal instruments in different areas of application, we infer that the EU data protection law regime, which is now to be read in the light of Article 8 of the Charter and Article 16 TFEU, provides, in principle, that international data transfers can take place to a third country without additional requirements only when that country ensures an adequate level of protection[9]. When the third country has not been declared as adequate, exceptions apply for *specific* transfers, as long as appropriate safeguards are adduced.

7. The last round of negotiations on the Agreement was concluded before two important developments in the EU: the political agreement on the data protection reform package, including the General Data Protection Regulation[10] and the Data Protection Directive[11] in criminal matters, and the judgment of the Court of Justice in the *Schrems* case[12] invalidating the Safe Harbor Decision. Even though this judgment does not directly refer to international data transfers in the law enforcement area, we recommend to take it into account in assessing the role that the Agreement will have in the EU data protection legal regime. This is because the key findings[13] of the Court interpret or directly apply Articles 7, 8 and 47 of the Charter in relation to transfers[14], all of which also apply in the law enforcement area.

8. The EU legal framework for data protection in the law enforcement area is under modernisation. The current framework is composed of several different legal sources, such as:

a) Council Framework Decision 2008/977/JHA[15] (hereinafter, the Framework Decision), which applies to international data transfers in the area of law enforcement to the extent the data transferred were initially made available to the transferring Member State by the competent authorities of another Member State;
b) Regulation 45/2001[16], which applies to international data transfers to the extent data are transferred by an EU institution or body;
c) a series of EU secondary legislation - *lex specialis*, which applies to specific transfers of data in the law enforcement area, prohibiting transfers either completely[17] or with very strict exemptions[18], or requiring safeguards such as the existence of an adequate level of protection in the receiving third country[19];

d) specific international agreements concluded both at EU level and at Member State level that serve as legal bases for transfers[20];
e) national data protection laws of the Member States which govern other transfers in the area of law enforcement.

While this shows diversity in transfer instruments, consistency is ensured by the horizontal application of the Charter and the TFEU mentioned above. It should also be taken into account that all Member States are signatories of Convention 108 of the Council of Europe[21], which is applicable in the law enforcement area and is also under modernisation.

9. The following assessment of the proposed Agreement will take into account the current standards of EU law above mentioned with regard to international transfers of personal data as they are interpreted by the CJEU, and the perspective of their modernisation.

III. Purpose, scope and effect of the Agreement

1. High level of protection

10. According to Article 1(1) of the Agreement, the purpose of the Agreement is "*to ensure a high level of protection of personal information*" and to "*enhance cooperation between the United States and the European Union in relation to the prevention, investigation, detection or prosecution of criminal offenses, including terrorism*". The two contracting Parties acknowledge in the first paragraph of the Preamble that they are both "*committed to ensuring a high level of protection of personal information exchanged in the context of the prevention, investigation, detection and prosecution of criminal offences*". Therefore, the Agreement acknowledges the need for a high threshold for its future application. The EDPS welcomes this conclusion, which is in line with the general EU data protection legal framework[22] and the case law of CJEU in the interpretation and application of the right to the protection of personal data enshrined in Article 8 of the Charter[23]. However, the EDPS highlights that in order for the high level of protection to be effective and to comply with EU primary law, it needs to be fully reflected in the provisions of the Agreement and in their subsequent application.

2. Presumption of compliance and authorisations

11. With regard to the effect of the Agreement, Article 5(3) provides that, "*by giving effect to paragraph 2*" – referring to implementation in domestic laws, "***the processing of personal information*** *by the United States or the European Union and its Member States, with respect to matters falling within the scope of this agreement,* ***shall be deemed to comply with their respective data protection legislation*** *restricting or conditioning international transfers of personal information,* ***and no further authorization under such legislation shall be required***". Article 5(3) seems to establish that where the Parties have implemented in their national legal systems the provisions of the Agreement, every processing of personal data in the material scope of the Agreement is presumed to comply with the "domestic" data protection laws of the exporting countries governing international data transfers.

12. The wording used for this provision is similar to the one used in the EU-US PNR Agreement which establishes the adequacy of the US Department of Homeland Security's system for PNR data processing and use (Article 19, "Adequacy")[24]. However, the Agreement does not constitute an adequacy finding decision[25] and it does not appear as a self-standing legal instrument since it complements specific legal basis for transfers.

13. Nevertheless, the Agreement creates a general presumption of compliance. Subject to the existence of a specific legal basis, future transfers will not need any authorisation. Therefore it is crucial to ensure that this "presumption" is reinforced by all necessary safeguards within the text of the Agreement.

14. The "architecture" of Article 5 of the Agreement indicates that Article 5(3) will only take effect after Article 5(2) is fully complied with. Article 5(2) requires the Parties to take all necessary measures to implement the Agreement, and in particular the provisions regarding access, rectification, and administrative and judicial redress. In addition, it clearly states that "*the protections and remedies set forth in this Agreement shall benefit individuals and entities* ***in the manner implemented in the applicable domestic laws of each Party***", which means that the Agreement, in order to be effective ("to benefit individuals and entities"), needs to be implemented in the domestic legal systems of the Parties. Further analysis is needed to verify to which extent, also in the light of the *Medellin* jurisprudence[26], the Agreement can be considered as a self-executing agreement in the US legal order and which substantive provisions may be needed to be implemented by the US Congress in order to make it binding domestic law.

15. The Agreement refers to measures to be introduced in the applicable legal framework of the Parties. However, it does not appear to provide a specific mechanism for assessing the degree of its implementation in the domestic laws of the parties for the purpose of giving effect to Article 5(3). The periodical Joint Review mechanism provided for in Article 23 seems to have the general purpose of assessing the effectiveness of "the policies and procedures that implement this Agreement", with an obligation for the Parties to conduct the first joint review "no later than three years from the date of entry into force" of the Agreement. In this context, an essential question is "*when would the transfers of data with respect to matters falling within the scope of the Agreement* ***be deemed to comply*** *with the requirements of EU data protection law restricting or conditioning international transfers, without further needing any authorisation*"?

16. With regard to the fact that Article 5(3) of the Agreement eliminates the role of relevant authorities (data protection supervisory authorities or other institutions depending on the legal system of the EU Member State) from authorising the transfers, the EDPS would recall that the establishment in the EU Member States of independent national supervisory authorities is an essential component[27] of the protection of individuals with regard to the processing of their personal data[28]. National supervisory authorities are responsible for monitoring compliance with EU data protection law pursuant to Article 8(3) of the Charter and each authority is vested with the power to check whether a transfer of personal data from its own Member State to a third country complies with data protection law even when the legal system of a third country has been found adequate[29] or a presumption of compliance is introduced on a basis of an agreement. Therefore, the EDPS notes that the absence of any further authorisation for transfers pursuant to Article 5(3) of the Agreement is without prejudice to the competences and powers of independent supervisory authorities to monitor the legality of transfers and compliance with data protection law, also on the basis of Article 21 of the Agreement. Hence Article 5(3) must be interpreted as respecting this role of supervisory authorities so as to be compliant with Article 8(3) of the Charter. The EDPS recommends that for full clarity, this conclusion be inserted in an explanatory declaration to the Agreement.

3. Relation between the Agreement and specific legal bases for transfers

17. It is apparent from the second paragraph of the Preamble that the Agreement aims "*to facilitate the exchange of information*" in the areas relevant for criminal matters by establishing a *"framework for the protection of personal information when transferred*" between the Parties [Article 1(2)]. It is further clearly stated in Article 1(3) that the Agreement "*in and of itself shall not be the legal basis for any transfers of personal information*" and "*a legal basis for such transfers shall always be required*". The complete legal framework for the safeguards in relation to transfers covered by the Agreement is composed of the provisions of the Agreement, the manner that they are implemented in the domestic laws of the Parties together with the specific legal basis for transfers. The relationship between the Agreement and the subsequent legal bases for transfers between the Parties is very important. We read Article 5(1) in the sense that all specific instruments providing for the legal basis for transfers should comply with the requirements of the Agreement, which are to be considered as providing a minimum level of safeguards for transfers. For purposes of legal certainty, the EDPS recommends the Parties to consider confirming, at least within the explanatory declarations accompanying the Agreement, that the specific legal bases for transfers must fully comply with the safeguards provided in the Agreement and that, in the case of conflicting provisions between the specific legal basis and the Agreement, the latter will prevail.

4. Onward transfers to State authorities

18. Article 5(2) of the Agreement specifies that "*for the United States, its obligations shall apply in a manner consistent with its fundamental principles of federalism*". This provision may have an impact on onward transfers from federal competent authorities in the United States that are initial recipients of data, towards authorities at state level, which are not bound by the Agreement. In this sense, Article 2(5) defines the "competent authority" in the US as being a "*national law enforcement authority responsible for the prevention, investigation, detection or prosecution of criminal offenses, including terrorism*", excluding thus authorities at state level[30]. In contrast, all the authorities of the EU and its Member States that are competent in the same areas are bound by the Agreement, according to the definition in Article 2(5).

19. Some possible negative effects of the clause analysed under Article 5(2) may be counterbalanced by Article 14(2) of the Agreement, according to which the transfers of data from federal to State level can be discontinued if the federate States "*have not effectively protected personal information taking into account the purpose of this Agreement*". The EDPS welcomes this provision, but recommends clarifying, at least within the explanatory declarations of the Agreement, that in case of ineffective protection for data transferred to State level, the relevant measures under Article 14(2) will include, where necessary, measures concerning data already shared.

5. National security exemption

20. Article 3 establishes that the Agreement applies to "*personal information transferred*" between competent authorities of the Parties, or "*otherwise transferred in accordance with an agreement*" between the US and the EU or its Member States, "*for the prevention, detection, investigation and prosecution of criminal offences, including terrorism*". The EDPS welcomes that the bilateral agreements between the *Member States* and the US are also

brought in the scope of the Agreement. We also note that "transfers *or other forms of cooperation between the authorities of the Member States and of the United States other than those referred to in Article 2(5), responsible for safeguarding national security*" are not in the scope of the Agreement, pursuant to Article 3(2).

21. However, taking into account the broad definition of "*competent authority*" under Article 2(5), which, in respect of US authorities, refers to a "*national law enforcement authority responsible for the prevention, investigation, retention and prosecution of criminal offenses, including terrorism*", read together with the provisions of Article 6(2) which ensure that further processing of shared personal information "*by other national law enforcement, regulatory or administrative authorities shall respect the other provisions of this Agreement*", we understand that national authorities responsible for safeguarding national security will be subject to the provisions of the Agreement when processing data transferred for the purposes set forth in the Agreement. Where appropriate and for full clarity, this conclusion can be inserted within an explanatory declaration to the Agreement. Finally, the EDPS notes that the wide definition of "Competent Authority" also covers public prosecutors offices and judicial authorities, to the extent that they exercise the above mentioned tasks on criminal offences.

6. Transfers from private parties to competent authorities

22. The EDPS notes that while the Agreement mainly applies to data transferred between competent authorities of the parties, it can also apply to transfers organized between private parties and competent authorities, as long as an agreement is in place between the US and the EU or its Member States. In this respect, Article 3(1) specifies that the Agreement applies to personal data transferred between competent authorities "*or otherwise transferred in accordance with an agreement concluded between the [US] and the [EU] or its Member States"* in the law enforcement area. Therefore, we understand that the Agreement can also cover transfers of data from relevant private companies, such as air carriers (e.g. PNR transfers) or service providers which offer publicly available electronic communications services, to the competent authorities of the parties, but only when those transfers are based on an international agreement.

7. Application of the safeguards to individuals

23. Article 3 ("Scope") does not contain any specific reference to the *rationae personae* scope of the Agreement. It establishes a wide *rationae materiae* scope, by stating that the Agreement applies to (any) "*personal information transferred*" between the Parties in the law enforcement area. This general reference to personal information seems to imply that the personal information of any individual equally enjoys the safeguards enshrined in the Agreement. This interpretation is encouraged by specific references to a wide personal scope of Articles 16 "Access", 17 "Rectification" and 18 "Administrative redress" (since they refer to "any individual"). However, it may be contradicted by the general "Non-discrimination" provision in Article 4. According to this Article, each Party must comply with the obligations of the Agreement to protect "*personal information of its own nationals and the other Party's nationals"* without arbitrary discrimination. In addition, Article 19 "Judicial redress" only applies to "citizens" of the Parties.

24. Where implemented by excluding anyone other than EU nationals from the personal scope of the Agreement, the Agreement would not be compliant with the protection afforded by Articles 7, 8 and 47 of the Charter, according to which the fundamental rights to privacy, personal data protection and an effective remedy apply to "everyone" in the EU, irrespective

of nationality or status. Therefore, the EDPS recommends an important clarification, at least within explanatory declarations to the Agreement, to confirm that the personal scope of the Agreement is in compliance with the Charter.

IV. Analysis of substantive provisions of the Agreement

1. Definitions

25. The EU data protection legal regime provides for well-established definitions of concepts such as “personal data” and “processing [of personal data]”. Even though the terminology chosen for the text of the Agreement partly differs from the relevant legal regime in the EU – as the Agreement refers to "personal information", and not to "personal data", the EDPS welcomes the wide definition in Article 2(1) of "personal information", which follows the corresponding definition of "personal data" as enshrined in Directive 95/46/EC and Regulation 45/2001. However, the definition in Article 2(1) of the Agreement does not refer to "any information”, but to "information". Therefore, for instance, doubts may arise whether metadata referring to an identified or identifiable individual will be considered as personal information in the framework of the Agreement.

26. With regard to the definition of "processing of personal information" in Article 2(2) of the Agreement, some substantive differences are noted compared to the definition of "processing of personal data" as enshrined in the Framework Decision, Directive 95/46/EC and Regulation 45/2001. As defined in the Agreement, "processing of personal information" means "*any operation or set of operations involving collection, maintenance, use, alteration, organization or structuring, disclosure or dissemination, or disposition*". Contrary to the relevant EU instruments, this definition excludes from the scope of the Agreement operations involving "*recording, storage, retrieval, consultation, alignment or combination, blocking, erasure or destruction*". On the other hand, Article 2(1) of the Agreement, unlike the definition in the EU legal regime, refers to "*maintenance*" and "*disposition*". These two notions do not seem to cover the meaning of the operations enumerated in EU law.

27. A clarification is recommended to guarantee the application of the safeguards provided for in the Agreement in key operations, for instance where a competent authority records data or when the authority merely stores information it receives, without making other use of the information. It should be made clear that "consultation", which is also absent from the definition, is covered by the term "use", as misuse often originates in practice in illegitimate consultation of personal data.

28. The EDPS therefore recommends a definition of processing operations in compliance with the basic requirements of EU law, to include the key operations mentioned above such as the recording and storage of information. In the event that the Parties do not fully align the definitions of “personal information” and “processing operation” with the ones provided for in EU law, the EDPS recommends clarifying in the explanatory documents accompanying the Agreement that the application of the two notions will not differ on substance from their understanding in EU law.

2. Purpose limitation and onward transfers

29. The EDPS welcomes the recognition of the principles of proportionality and necessity set out in the last paragraph of the Preamble. In light of this, Article 6(1) of the Agreement limits the transfer of personal information to "*specific purposes authorized by the legal basis for the transfer (...)*" and Article 6(5) adds that it must be processed "*in a manner that is directly relevant to and not excessive or overbroad in relation to the purposes of such processing*". In addition, Article 6(2) prohibits further processing which is incompatible with the purposes for which it was transferred.

30. With regard to onward transfers to a State not party to the Agreement, Articles 7(1) and 7(2) require consent from the competent authority which initially transferred the personal data and, for this purpose, due account must be taken of "*all relevant factors*" detailed in the provision. This level of protection is further reinforced by the possibility to discontinue the transfer of personal information to authorities of constituent territorial entities of the Parties pursuant to Article 14(2) of the Agreement, where the provisions on purpose limitation and onward transfers are not complied with. The EDPS welcomes these provisions.

31. Article 7(3) further stipulates that where the Parties conclude an agreement on transfers other than in relation to specific cases, they must follow "specific conditions" included in the agreement authorising the transfers. We note that such transfers can also imply, in practice, bulk transfers of data. The conditions are not defined in Article 7(3). Processing of bulk data constitutes a serious interference with the rights to privacy and protection of personal data because of the number of people and the amount of personal data involved[31]. An indicative list of the above mentioned “specific conditions” would we welcome where included in the explanatory declaration.

3. Information security

32. The EDPS welcomes the provisions of Article 9 on information security. However, with regard to the notification of information security incidents, Article 10(2)(b) allows for the omission of the notification of a data breach where the notification "*may endanger national security*", with an unclear effect on the ground of a possible consequence ("*may*") on national security is unclear. The EDPS also questions the necessity of omitting the notification altogether, and not merely delaying it or restricting for security reasons the quality of recipients entitled to receive the information. Moreover, specific conditions for delaying notifications to the transferring Competent Authority are not referred to in the text. The EDPS would recommend highlighting in an explanatory declaration the intention of the Parties to apply these provisions with a view to limit as much as possible omission of the notifications, on one hand, and to avoid excessive delays of notifications, which would lead to a long time period for a competent authority not being aware of data breaches concerning data they transferred, on another hand.

4. Data retention

33. Article 12(1) mandates the Parties "*to ensure that personal information is not retained for longer than is necessary and appropriate*". In the light of the purpose limitation principle invoked by the Parties in the Agreement, the following specification should be added: *"for the specific purposes for which they were transferred"*.

34. In addition, Article 12(2), referring to data retention rules in the situation of bulk transfers, should also make reference to the criteria to be taken into account to determine the length of the retention period as set out in Article 12(1), taking into account the principles of proportionality and necessity.

5. Bulk transfers of sensitive data

35. In light of the fact that the notion of sensitive data differs amongst the Parties[32], the special categories of data listed in Article 13(1) are to be welcomed because the text clarifies the meaning of sensitive data for the purpose of the Agreement and aligns it with the EU definition[33].

36. Nevertheless, the EDPS is concerned that Article 13(2) opens the possibility of having bulk transfers of sensitive data, as it allows an agreement concluded between the US and the EU or a Member State to provide for the possibility of a "*transfer of personal information other than in relation to specific cases, investigations or prosecutions*". Although Article 13(2) requires taking into account the nature of the information, it leaves to each specific agreement the determination of categories of data to be exchanged. In this context, the EDPS would recall his previous Opinions on the use of Passenger Name Records (PNR), in which he advocated the complete exclusion of sensitive data in the context of bulk transfers[34]. For instance, the EDPS had specifically questioned the processing of sensitive data by the Department of Homeland Security, recommending that the agreement at issue specify that air carriers should not transfer sensitive data to the Department[35].

37. Therefore, the EDPS recommends that bulk transfers of sensitive data be excluded from the scope of the Agreement.

6. Rights of the data subject

38. The EDPS welcomes that the Agreement provides for several rights of the data subject: the right to be informed (Article 20), the right of access (Article 16), the right to rectification - which also refers to erasure and blocking (Article 17), the rights to administrative and judicial redress (Articles 18 and 19) and the right not to be subject to automated decisions (Article 15). The EDPS would recall that the rights of the data subject, and in particular the rights to access and rectification, are enshrined as essential elements of the right to personal data protection in Article 8(2) of the Charter.

39. The exemptions foreseen in the Agreement for the exercise of the rights of access and information are considerable. With regard to the right of access, Article 16(2) provides for restriction of access following additional criteria such as avoidance to obstruct "*official or legal inquiries, investigations and proceedings*", protection of "*law enforcement sensitive information*", avoidance to prejudice the "*prevention, detection, investigation or prosecution of criminal offenses or the execution of criminal penalties*", in addition to both "*public and national security*". Another exemption states that restrictions to access may be imposed to "*protect interests provided for in legislation regarding freedom of information and public access to documents*"[36]. It is difficult to conceive of a situation in which personal data transferred for the purposes of this Agreement will not be considered "law enforcement sensitive information" by the competent authority, in the absence of specific criteria to determine[37] what "law enforcement sensitive information" means.

40. The EDPS recommends reconsidering the list of exemptions in order to make sure that, *de facto*, the possibility for the person to have access to their own data would still exist, even if limited or performed by a trusted third party in situations where access is denied to protect sensitive law enforcement information. In that sense, Article 16(4) is welcomed as it provides for an indirect form of access, but its application is limited only to cases 'permitted under applicable domestic law'.

41. In addition, Article 16(1) allows access to data "*in accordance with the applicable legal framework of the State in which relief is sought*". If the current regime of access available in the US would apply for data transferred in the scope of the Agreement, it does not seem, *prima facie*, that the conditions of Article 8(2) of the Charter would be fulfilled. Although the US Privacy Act of 1974 grants individuals a right to access to their personal data[38], this right is significantly curtailed by several exceptions[39]. Firstly, a special exemption stipulates that this right does not apply to any information *"compiled in a reasonable anticipation of a civil action or proceeding*"[40]. Secondly, general exemptions remove the obligation to grant access where an agency whose principal activity pertains to criminal law enforcement requests the exemption by promulgating a rule to that effect[41]. Thirdly, specific exemptions provide, amongst others, that an agency may publish a rule exempting it from the obligation to grant a right to access to a system of record containing classified information that is "national defence or foreign policy material or investigatory material compiled for law enforcement purposes."[42] These exceptions significantly limit the exercise of the right of access, if indeed it were to be exercised in accordance with the current applicable law in the US.

42. An effective right to be informed is important. In this regard, the CJEU established that "*the requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by data subjects of their right of access to, and right to rectify the data being processed*"[43]. The provision regarding "Transparency" (Article 20) has a very limited effect, due to the fact that the information notices are to be published *"in a form and at a time provided for by the law applicable to the authority providing the notices"*, which could mean, in practice, that even general information notices could be published long after a certain transfer or a certain processing operation has taken place. In addition, all limitations applicable to the right of access apply equally to the transparency obligations.

43. As a result of this preliminary analysis, the EDPS considers that the Parties to the Agreement should increase their efforts to ensure that restrictions to the exercise of the right of access are selectively limited to what is indispensable to preserve the public interests enumerated and to strengthen the obligation for transparency.

44. The EDPS welcomes that automated decisions "*may not be based solely on the automated processing of personal information without human involvement*", pursuant to Article 15. This is especially important in the area of law enforcement, where the consequences of profiling on individuals are potentially more severe. However, the threshold to be met before triggering the applicability of Article 15 is quite high, because it requires the decisions to produce "*significant adverse actions*" in order not to be solely based on automatic processing, while EU law usually prohibits such decisions that produce "*adverse legal effects or significantly affect*" the individual[44].

7. Judicial redress and administrative remedies

45. In the different context of an adequacy finding decision (the Safe Harbor), the CJEU has found[45] that the lack of effective judicial redress when personal data are transferred to a third country goes to the essence of Article 47 of the Charter, which provides for the right to effective judicial protection. In that context, the CJEU found that "*legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter*" and that "*the first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to* ***an effective remedy*** *before a tribunal in compliance with the conditions laid down in that article*"[46].

46. Article 19 (1) and (2) of the Agreement requires the Parties to provide in their applicable legal framework the possibility for their *citizens* to seek judicial review regarding denial of access or of amendment of records or intentional unlawful disclosure of information. While Article 19 (1) and (2) provides for a possibility for citizens of the EU to seek legal remedies in relation to some of the substantive provisions of the Agreement, *individuals other than EU citizens* who are otherwise protected by the Charter (e.g. asylum seekers, EU residents) do not have on a basis of these two paragraphs a possibility to pursue legal remedies to have access to personal data relating to them or to obtain the rectification. In addition, neither citizens, nor individuals that are not citizens have any possibility to pursue legal remedies to obtain *erasure* of data. Article 19 (3) establishes that these limitations "*are without prejudice to any other judicial review available with respect to the processing on an individual´s personal information under the law of the State in which relief is requested*". The EDPS is not in the position to fully assess in this preliminary Opinion the effectiveness of alternative legal remedies that can be provided for in sectorial legislation particularly in the US and at State level, and to which extent they could offer an organic and comprehensive remedy to all relevant individuals. Therefore, he has serious concerns about compliance of Article 19 with the Charter. As for the **effective nature** of the legal remedies, which is also a requirement of Article 47 of the Charter, it must be assessed after the provisions in the Agreement are implemented in the domestic law of the US[47].

47. With regard to administrative redress, the EDPS observes that Article 18 refers to administrative redress provided by the competent authority, as defined in Article 2 of the Agreement, and not by an oversight authority. Article 18(1) establishes that this kind of administrative redress will be available for alleged breaches of the rights to access, rectification and erasure. The CJEU has stressed that it is essential for individuals to be able to file complaints with independent supervisory authorities[48] and seek, therefore, administrative redress. The EDPS reads the provision referring to effective oversight (Article 21) and the provision regarding administrative redress (Article 18) as not restricting the possibility of an individual to file a complaint with the oversight authority pursuant to breaches of Articles 16 and 17 of the Agreement (rights to access, rectification and erasure).

8. Effective oversight

48. The EDPS welcomes the provisions on accountability in Article 14, as mentioned in paragraph 19 of this Opinion. However, these provisions should be complemented by independent external supervision.

49. In this respect, the EDPS recalls that Article 8(3) of the Charter provides that respect for the rules on data protection has to be supervised by an independent authority[49], which means, according to the CJEU, an authority able to make decisions independently from any direct or indirect external influence. Such a supervisory authority must not only be independent from the parties it supervises, but must also not be part of the government, since the government itself may be an interested party.[50]

50. The EDPS welcomes the requirement under Article 21(1)(a) that oversight authorities must *"exercise independent oversight functions and powers"*. However, also in the light of the current debate regarding the effective powers to **enforce** data protection and privacy law of some of the US oversight authorities[51] enumerated in Article 21(3), we consider as essential that a bilateral explanatory declaration to the Agreement is signed by the parties to specifically list:

- the supervisory authorities that have competence in this matter and the mechanism for the Parties to inform each other about future changes;
- the effective powers they may exercise;
- the identity and coordinates of the contact point which will assist with the identification of the competent oversight body (see Article 22(2)). [52]

9. Joint review and suspension

51. The EDPS welcomes Article 23 on the joint review of the Agreement. Article 23(3) prevents the "duplication" of joint reviews, which may have an impact on joint reviews already foreseen in existing agreements: however, he recommends the EU Commission to clarify how this may have an impact on the implementation of specific Agreements such as those relating to the exchange of Passenger Name Records[53] or financial records[54].

52. The EDPS also welcomes the fact that Article 26 allows for the suspension of the Agreement in the event of a material breach of its provisions. To this effect, the EDPS stresses the paramount role of independent supervision of the application of the Agreement in order for breaches to be identified.

V. Conclusions

53. The EDPS welcomes the intention to provide for a legally binding instrument that aims to ensure a high level of data protection for the personal data transferred between the EU and the US for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism.

54. Most of the substantive provisions of the Agreement aim to fully or partially correspond with the essential guarantees of the right to personal data protection in the EU (such as the rights of the data subject, independent oversight and the right to judicial review).

55. Although the Agreement does not technically constitute an adequacy finding decision, it creates a general presumption of compliance for transfers grounded on a specific legal basis, in the framework of the Agreement. Therefore, it is crucial to ensure that this "presumption"

is reinforced by all necessary safeguards within the text of the Agreement, to avoid any breach of the Charter, in particular of Articles 7, 8 and 47.

56. There are three essential improvements the EDPS recommends for the text to ensure compliance with the Charter and Article 16 TFEU:

1) clarification that all the safeguards apply to all individuals, not only to EU nationals;

2) ensuring judicial redress provisions are effective within the meaning of the Charter;

3) clarification that transfers of sensitive data in bulk are not authorised.

57. Moreover, for the purpose of legal certainty, the EDPS recommends that the following improvements or clarifications be introduced in the text of the Agreement or within explanatory declarations to be attached to the Agreement, or in the implementing phase of the Agreement, as detailed within this Opinion:

1) that Article 5(3) must be interpreted as respecting the role of supervisory authorities so as to be compliant with Article 8(3) of the Charter;
2) that the specific legal bases for transfers (Article 5 (1)) must fully comply with the safeguards provided in the Agreement and that, in the case of conflicting provisions between a specific legal basis and the Agreement, the latter will prevail;
3) that in case of ineffective protection for data transferred to authorities at State level, the relevant measures under Article 14(2) will include, where necessary, measures concerning data already shared;
4) that the definitions of processing operations and personal information (Article 2) are aligned to be in compliance with their well-established understanding under EU law; in case the Parties will not fully align these definitions, a clarification should be done in the explanatory documents accompanying the Agreement that the application of the two notions will not differ on substance from their understanding in EU law;
5) that an indicative list of the "specific conditions" where data are transferred in bulk (Article 7 (3)) could be included in the explanatory declaration;
6) that the Parties intend to apply the provisions regarding information breach notifications (Article 10) with a view to limit as much as possible omission of the notifications, on one hand, and to avoid excessive delays of notifications;
7) that the data retention provision in Article 12(1) is complemented by the specification *"for the specific purposes for which they were transferred"*, in the light of the purpose limitation principle invoked by the Parties in the Agreement;
8) that the Parties of the Agreement consider increasing their efforts to ensure that restrictions to the exercise of the right of access are limited to what is indispensable to preserve the public interests enumerated and to strengthen the obligation for transparency;
9) that a detailed explanatory declaration to the Agreement specifically list (Article 21):
    - the supervisory authorities that have competence in this matter and the mechanism for the Parties to inform each other about future changes;
    - the effective powers they may exercise;
    - the identity and coordinates of the contact point which will assist with the identification of the competent oversight body (see Article 22(2)).

58. Finally, the EDPS would recall the need that any interpretation, application and implementing measure of the Agreement should be done, in the case of lack of clarity and

apparent conflict of provisions, in a way compatible with the EU constitutional principles in particular with regard to Article 16 TFEU and Articles 7 and 8 of the Charter, regardless of the welcome improvements to be adduced following the recommendations in this Opinion.

Done in Brussels, 12 February 2016

(**signed**)

Giovanni BUTTARELLI

European Data Protection Supervisor

Notes

[1] See MEMO 10/1661 of the European Commission, published on 3 December 2010, available here: http://europa.eu/rapid/press-release_IP-10-1661_en.htm.
[2] See MEMO 11/203 of the European Commission, published on 29 March 2011, available here: http://europa.eu/rapid/press-release_MEMO-11-203_en.htm.
[3] See Press release 14-668 of the Office of the Attorney General, published on 25 June 2014, available here: http://www.justice.gov/opa/pr/attorney-general-holder-pledges-support-legislation-provide-eu-citizens-judicial-redress.
[4] See MEMO 15/5612 of the European Commission, published on 8 September 2015, available here: http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm.
[5] Text available here: http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf.
[6] See Case-181/73, *R. & V. Haegeman v. Belgian State*, ECLI:EU:C:1974:41, at 5 (in the "Grounds" section).
[7] Case C-308/06, *Intertanko and Others*, ECLI:EU:C:2008:312, at 42.
[8] Joined cases C-402/05 P and C-415/05 P, *Kadi v. Council*, ECLI:EU:C:2008:461, at 285.
[9] To this effect, see the relevant provisions:
- for the area of the common single market: Articles 25 and 26 of Directive 95/46/EC;
- for the law enforcement area, regarding only data processed as a result of a cross-border transfer: Article 13 of the Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters OJ L 350/60;
- for transfers of data from Europol to third countries: Article 23(6)(b) of the Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office, OJ L 121/37;
- for transfers of data by EU institutions and bodies: Article 9 of Regulation 45/2001.
There is no available overview of national data protection laws in the area of law enforcement. In addition, see the Study for the LIBE Committee, "*A Comparison between US and EU Data Protection Legislation for Law Enforcement*" (Author: F. Boehm), PE 536.459, published in September 2015 (hereinafter "Boehm study"), p. 30 to 35.
[10] 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)11 [first reading] (hereinafter "proposed GDPR").
[11] The Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data COM(2012)10 [first reading] (hereinafter "proposed Data Protection Directive in criminal matters").
[12] Case C-362/14, *Schrems*, ECLI:EU:C:2015:650 (hereinafter "*Schrems*").
[13] See *Schrems* at 38, 40, 47, 53, 54, 58, 64, 66, 72, 91, 94, 95.
[14] More precisely, the Court of Justice recently affirmed that the requirements for ensuring lawful international transfers of personal data enshrined in secondary EU legislation, in particular the possibility of the Commission to adopt adequacy decisions for the purpose to "*protect the private lives and basic freedoms of individuals*" [Article 25(6) of Directive 95/46], stem from Article 8(1) of the Charter of Fundamental Rights of the EU (the Charter) and the obligation expressly enshrined therein "to protect personal data". In this regard see *Schrems* at 72: "*Thus, Article 25(6) of Directive 95/46* (n. – conditions for the European Commission to find that a third country has an adequate level of protection) *implements the express obligation laid down in Article 8(1) of the Charter to protect personal data and, as the Advocate General has observed in point 139 of his Opinion, is intended to ensure that the high level of that protection continues where personal data is transferred to a third country*". In addition, the Court requires that ensuring an "adequate level of protection" must be understood as "*requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter"* [*Schrems,* at 73].The condition of the existence of an essentially equivalent level of protection is foreseen both in the forthcoming General Data Protection Regulation [Recital 81 of the Preamble] and the Data Protection Directive in criminal matters [Recital 47 of the Preamble].
[15] Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters OJ L 350/60.

[16] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.
[17] Article 54 of the Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System II, OJ L 205/63.
[18] Article 31 of Regulation 767/2008/EC of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas, OJ L 218/60.
[19] Article 23(6)(b) of the Council Decision 2009/371/JHA.
[20] See, for instance, the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ L 215/5; Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America, OJ L 291/40; see also different Mutual Legal Assistance Treaties between Member States and third countries.
[21] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, ETS 108.
[22] Recital 10 of Directive 95/46/EC and Recital 10 of the Council Framework Decision 2008/977/JHA expressly foresee that, in general, the legal regime for data protection created under each of the two legal acts "*must (...) seek to ensure a high level of protection*".
[23] See, for instance, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland* (C-293/12) and *Seitlinger* (C-594/12), ECLI:EU:C:2014:238 (hereinafter "*DRI*"), at 67 and *Schrems*, at 39 and 72.
[24] "*In consideration of this Agreement and its implementation, DHS shall be deemed to provide, within the meaning of relevant EU data protection law, an adequate level of protection for PNR processing and use. In this respect, carriers which have provided PNR to DHS in compliance with this Agreement shall be deemed to have complied with applicable legal requirements in the EU related to the transfer of such data from the EU to the United States*.".
[25] The EDPS recalls that the Court of Justice of the EU underlined in its case-law applying Article 8(1) of the Charter that the term "adequate level of protection" "*must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union"* (*Schrems* at 73). The Court further established that "*when examining the level of protection afforded by a third country"*, the assessment must refer to *"the content of the applicable rules in that country resulting from its domestic law or international commitments and the practice designed to ensure compliance with those rules*" (*Schrems* at 75) and also that it must "*take account of all circumstances surrounding a transfer of personal data to a third country*" (*Schrems* at 75). Moreover, one of the main reasons of the CJEU to invalidate the 2000 Safe Harbor decision was that it did not in fact contain any reasoned finding that the legal system in question "ensures" an adequate level of protection (*Schrems* at 96 to 98).
[26] See the judgment of the US Supreme Court in *Medellin v Texas* 552 US (2008) at 505 and 505 n.2: "*What we mean by self-executing is that the treaty has automatic domestic effect as federal law upon ratification*"; "*In sum, **while treaties may comprise international commitments... they are not domestic law unless Congress has either enacted implementing statutes or the treaty itself conveys an intention that it be self-executing and is ratified on these terms***". See "International Law and Agreements: Their Effect upon U.S. law", issued by the Congressional Research Service, February 18, 2015, available on www.crs.gov.
[27] *DRI*, at 68.
[28] Recital 33 of the Framework Decision reiterates that it "*is an essential component of the protection of personal data processed within the framework of police and judicial cooperation between the Member States*". See also Case C-518/07, *Commission v Germany*, EU:C:2010:125, at 25; Case C-288/12, *Commission v Hungary*, EU:C:2014:237, at 48 and *Schrems*, at 41.
[29] *Schrems*, at 47, which specifically refers to Article 8(3) of the Charter when establishing the power of supervisory authorities to check whether transfers are lawful.
[30] For a possible indication on the impact of such transfers, see the Study for the LIBE Committee, "*The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens*" (Author: F. Bignami), PE 519.215, published in May 2015 (hereinafter "Bignami study"), p. 6 and 7.
[31] *Schrems* at 93 and 94; See also the Bignami study, p.6.
[32] To this effect, see Bignami study, p.12.
[33] Article 8(1) of the Directive 95/46/EC lists "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life as special categories of personal data*".

[34] See, for instance, Opinion of the EDPS on the EU-Canada PNR Agreement, 30.09.2013, at 47; EDPS Opinion on the Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries, 19.10.2010, at 26; EDPS Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, 25.03.2011, at 6; EDPS Opinion on the EU-Australia PNR Agreement, 15.07.2011, at 26; See also the Opinion 4/2003 of the Article 29 Data Protection Working Party on the Level of Protection ensured in the United States for the Transfer of Passengers' Data, adopted on 23 June 2003, p.7.
[35] EDPS Opinion on the Proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, 9.12.2011, at 15 and 16.
[36] For comparison, Article 9 of Council of Europe's Convention 108 allows exceptions to the right to access, including in the law enforcement area, when they are provided for by law and are necessary in a democratic society in the interests of "*(a) protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences; and (b) protecting the data subject or the rights and freedoms of others*".
[37] As required, by analogy, in *DRI*, at 60 to 62.
[38] 5 U.S.C. §552a(d)(1).
[39] See Bignami study in general and Boehm study, p. 53 and 54.
[40] 5 U.S.C. §552a(d)(5); see also Bignami study, p. 12.
[41] 5 U.S.C. §552a(j).
[42] 5 U.S.C. §552a(k).
[43] Case C-201/14 *Bara v CNAS*, ECLI:EU:C:2015:638, at 33.
[44] Article 7 of the Council Decision 2008/977/JHA and Article 19 of the proposed Data Protection Directive in criminal matters.
[45] *Schrems*, at 95.
[46] *Schrems*, at 95.
[47] The bill was passed by the Congress on 10 February 2016, but further procedures are needed before it will be considered adopted. The draft bill has been met with criticism by US observers, who consider that it provides insufficient legal protection to citizens of the EU and in any case significantly less protection than the one afforded to US persons under the Privacy Act 1974. See, in this regard, the Bignami study, p. 13 and the letter sent by EPIC to US House of Representatives Committee on the Judiciary, 16 September 2015, available here https://epic.org/foia/umbrellaagreement/EPIC-Statement-to-HJC-on-HR1428.pdf.
[48] *Schrems*, at 56 to 58.
[49] Case C-614/10, *Commission v Austria*, ECLI:EU:C:2012:631, at 36; Case C-288/12, *Commission v Hungary*, at 47; *Schrems*, at 40.
[50] Case C-518/07, *Commission v Germany*, at 18-19, 25 and 30.
[51] See Bignami study, p. 34 and Boehm study, p. 54 and 72.
[52] *Commission v Austria*, at 36; *Commission v Hungary*; *Commission v Germany* and *Schrems.*
[53] Council Decision 2012/472/EU of 26 April 2012 on the conclusion of an Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security, OJ L 215.
[54] Council Decision 2010/412/EU of 13 July 2010 on the conclusion of an Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ L 195.