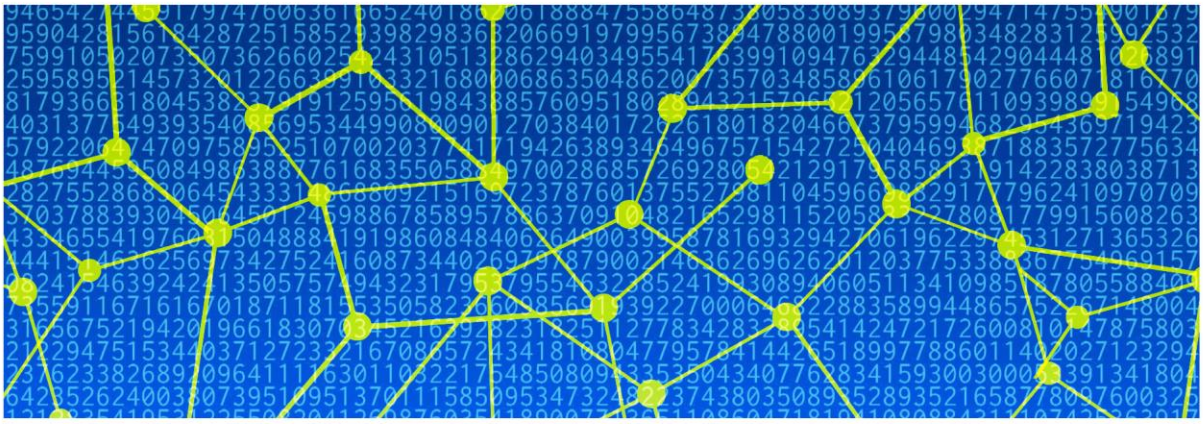

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 4/2016

Opinion on the EU-U.S. Privacy Shield draft adequacy decision

EDPS

30 May 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'. Under Article 28(2) of Regulation 45/2001, the Commission is required, 'when adopting a legislative Proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data...', to consult the EDPS.

He was appointed in December 2014 together with the 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 relates to the EDPS' mission to advise the EU institutions on the data protection implications of their policies and foster accountable policymaking - in line with Action 9 of the EDPS Strategy: 'Facilitating responsible and informed policymaking'.

Executive Summary

Data flows are global. The EU is bound by the Treaties and the Charter of Fundamental Rights of the European Union which protect all individuals in the EU. The EU is obliged to take all necessary steps to ensure the rights to privacy and to the protection of personal data are respected throughout all processing operations, including transfers.

Since the revelations in 2013 of surveillance activities, the EU and its strategic partner the United States have been seeking to define a new set of standards, based on a system of self-certification, for the transfer for commercial purposes to the U.S. of personal data sent from the EU. Like national data protection authorities in the EU, the EDPS recognises the value, in an era of global, instantaneous and unpredictable data flows, of a sustainable legal framework for commercial transfers of data between the EU and the U.S., which represent the biggest trading partnership in the world. However, this framework needs to fully reflect the shared democratic and individual rights-based values, which are expressed on the EU side in the Lisbon Treaty and the Charter of Fundamental Rights and on the U.S. side by the U.S. Constitution.

The draft Privacy Shield may be a step in the right direction but as currently formulated it does not adequately include, in our view, all appropriate safeguards to protect the EU rights of the individual to privacy and data protection also with regard to judicial redress. Significant improvements are needed should the European Commission wish to adopt an adequacy decision. In particular, the EU should get additional reassurances in terms of necessity and proportionality, instead of legitimising routine access to transferred data by U.S. authorities on the basis of criteria having a legal basis in the recipient country, but not as such in the EU, as affirmed by the Treaties, EU rulings and constitutional traditions common to the Member States.

Moreover, in an era of high hyperconnectivity and distributed networks, self-regulation by private organisations, as well as representation and commitments by public officials, may play a role in the short term whilst in the longer term they would not be sufficient to safeguard the rights and interests of individuals and fully satisfy the needs of a globalised digital world where many countries are now equipped with data protection rules.

Therefore, a longer term solution would be welcome in the transatlantic dialogue, to also enact in binding federal law at least the main principles of the rights to be clearly and concisely identified, as is the case with other non EU countries which have been ‘strictly assessed’ as ensuring an adequate level of protection; what the CJEU in its Schrems judgment expressed as meaning ‘essentially equivalent’ to the standards applicable under EU law, and which according to the Article 29 Working Party, means containing 'the substance of the fundamental principles' of data protection.

We take positive note of the increased transparency demonstrated by the U.S. authorities as to the use of the exception to the Privacy Shield principles for the purposes of law enforcement, national security and public interest.

However, whereas the 2000 Safe Harbour Decision formally treated access for national security as an exception, the attention devoted in the Privacy Shield draft decision to access, filtering and analysis by law enforcement and intelligence of personal data transferred for commercial purposes indicates that the exception may have become the rule. In particular, the EDPS notes from the draft decision and its annexes that, notwithstanding recent trends to move from indiscriminate surveillance on a general basis to more targeted and selected

approaches, the scale of signals intelligence and the volume of data transferred from the EU, subject to potential collection and use once transferred and notably when in transit, may still be high and thus open to question.

Although these practices may also relate to intelligence in other countries, and while we welcome the transparency of the U.S. authorities on this new reality, the current draft decision may legitimise this routine. We therefore encourage the European Commission to give a stronger signal: given the obligations incumbent on the EU under the Lisbon Treaty, access and use by public authorities of data transferred for commercial purposes, including when in transit, should only take place in exceptional circumstances and where indispensable for specified public interest purposes.

On the provisions for transfers for commercial purposes, controllers should not be expected constantly to change compliance models. And yet the draft decision has been predicated on the existing EU legal framework, which will be superseded by Regulation (EU) 2016/679 (General Data Protection Regulation) in May 2018, less than one year after the full implementation by controllers of the Privacy Shield. The GDPR creates and reinforces obligations on controllers which extend beyond the nine principles developed in the Privacy Shield. Regardless of any final changes to the draft, we recommend the European Commission to comprehensively assess the future perspectives since its first report, to timely identify relevant steps for longer term solutions to replace the Privacy Shield, if any, with more robust and stable legal frameworks to boost transatlantic relations.

The EDPS therefore issues specific recommendations on the Privacy Shield.

TABLE OF CONTENTS

I. INTRODUCTION 5

II. MAIN RECOMMENDATIONS 7

1. INTEGRATING ALL MAIN DATA PROTECTION PRINCIPLES 7
2. LIMITING DEROGATIONS 7
3. IMPROVING REDRESS AND OVERSIGHT MECHANISMS 8

III. ADDITIONAL RECOMMENDATIONS 9

1. PROVISIONS ON TRANSFERS FOR COMMERCIAL PURPOSES 9

Fully integrating the data minimisation and data retention principles 9
Adding safeguards as regards automated processing 9
Clarifying the purpose limitation principle 10
Limiting exceptions 10
Improving redress and oversight 10

2. RECOMMENDATIONS REGARDING ACCESS BY U.S. AUTHORITIES 11
3. ASSESSING THE IMPACT OF OTHER RELEVANT STATUTES AND RULES 11
4. A MEANINGFUL REVIEW 12
5. INTERACTION WITH THE GDPR 12

IV. CONCLUSION 12

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 Articles 7 and 8 thereof,

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 (hereafter: the Directive),

Having regard to Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters,

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 Articles 28(2), 41(2) and 46(d) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

On 6 October 2015, the Court of Justice of the European Union (hereafter: CJEU) invalidated[1] the Decision on the adequacy of the Safe Harbour[2]. The European Commission reached a political agreement with the U.S. on 2 February 2016 on a new framework for transfers of personal data called "the EU-U.S. Privacy Shield" (hereafter: the Privacy Shield). On 29 February, the European Commission made public a draft decision on the adequacy of this new framework (hereafter: the draft decision)[3] and its seven annexes, including the Privacy Shield principles and written representations and commitments by U.S. officials and authorities. The EDPS received the draft decision for consultation on 18 March this year.

The EDPS has expressed his position on transfers of personal data between the EU and the U.S. on a number of occasions[4] and has contributed to the Article 29 Working Party (hereafter: WP29) Opinion on the draft decision as a member of this group[5]. The WP29 has raised serious concerns and asked the European Commission to identify solutions to address them. The members of the WP29 expect that all the clarifications required in the Opinion will be provided[6]. On March 16, 27 non-profit organisations addressed their criticisms to the draft Decision in a letter addressed to EU and U.S. authorities[7]. On 26 May, the European Parliament adopted a resolution on transatlantic data flows[8], which calls on the Commission to negotiate further improvements to the Privacy Shield arrangement with the U.S. Administration in the light of its current deficiencies[9].

As the independent advisor to the EU legislators under Regulation (EC) No. 45/2001, the EDPS is now issuing recommendations to the parties involved in the process, in particular the Commission. This advice is intended to be both principled and pragmatic, in view of

proactively helping the EU to achieve its objectives with adequate measures. It complements and underlines some, but not all, of the recommendations in the WP29 Opinion.

The draft decision shows a number of improvements compared to the Safe Harbour Decision, in particular with respect to the principles for processing of data for commercial purposes. As regards access by public authorities to the data transferred under the Privacy Shield, we also welcome the involvement for the first time of the Department of Justice, the Department of State and the Office of the Director of National Intelligence in the negotiations. However, progress compared to the earlier Safe Harbour Decision is not in itself sufficient. The correct benchmark is not a previously invalidated decision, since the adequacy decision is to be based on the current EU legal framework (in particular, the Directive itself, Article 16 of the Treaty on the Functioning of the European Union as well as Articles 7 and 8 of the EU Charter of Fundamental Rights of the European Union, as interpreted by the CJEU). Article 45 of the EU General Data Protection Regulation (hereafter: the GDPR)[10] will provide new requirements for transfers of data based on an adequacy decision.

Last year, the CJEU affirmed that the threshold for the adequacy assessment is "essential equivalence" and demanded a strict assessment against this high standard[11]. Adequacy does not require adopting a framework which is identical to the one existing in the EU, but, taken as whole, the Privacy Shield and the U.S. legal order should cover all the key elements of the EU data protection framework. This requires both an overall assessment of the legal order and the examination of the most important elements of the EU data protection framework[12]. We assume that the assessment should be performed in global terms though respecting the essence of these elements. Moreover, because of the Treaty and the Charter, specific elements such as independent oversight and redress will need to be considered.

In this regard, the EDPS is aware that many organisations on both sides of the Atlantic are waiting for the outcome on this adequacy decision. However, the consequences of a new invalidation by the CJEU in terms of legal uncertainty for data subjects and the burden, in particular for SMEs, may be high. Furthermore, if the draft decision is adopted and subsequently invalidated by the CJEU, any new adequacy arrangement would have to be negotiated under the GDPR. We therefore recommend a future-oriented approach, in view of the imminent date of full application of the GDPR two years from now.

The draft decision is key for EU-U.S. relations, in a moment where they are also subject to trade and investment negotiations. Furthermore, many of the elements considered in our Opinion are indirectly relevant for both the Privacy Shield and other transfer tools, such as the Binding Corporate Rules (hereafter: BCRs) and Standard Contractual Clauses (hereafter: SCCs). It also has a global relevance, as many third countries will be closely following it against the background of the adoption of the new EU data protection framework.

Therefore, we would welcome a general solution for EU-U.S. transfers provided that it is comprehensive and solid enough. This requires robust improvements in order to ensure sustainable long term respect for our fundamental rights and freedoms. Where adopted, upon the first assessment by the European Commission, the decision has to be timely reviewed to identify relevant steps for longer term solutions to replace a Privacy Shield with a more robust and stable legal framework to boost transatlantic relations.

The EDPS also notes from the draft decision and its annexes that, notwithstanding recent trends to move from indiscriminate surveillance on a general basis to more targeted and

selected approaches, the scale of signals intelligence and the volume of data transferred from the EU subject to potential collection once transferred and notably when in transit, is likely to be still high and thus open to question.

Although these practices may also relate to intelligence in other countries, and while we welcome the transparency of the U.S. authorities on this new reality, the current draft decision may be interpreted as legitimising this routine. The issue requires serious public democratic scrutiny. We therefore encourage the European Commission to give a stronger signal: given the obligations incumbent on the EU under the Lisbon Treaty, access and use by public authorities of data transferred for commercial purposes, including when in transit, should only take place as an exception and where indispensable for specified public interest purposes.

Moreover, we note that essential representations relevant for the private lives of individuals in the EU appear to be only elaborated in important details in letters internal to U.S. authorities (for instance, statements concerning signals intelligence activities over transatlantic cables, if any)[13]. Although we do not question the authority of their distinguished authors, and understand that once published in the Official Journal and the Federal Register these representations will be considered as "written assurances" on the basis of which the EU assessment is made, we note on a general basis that the importance of some of them would deserve a higher legal value.

Besides legislative change and international agreements[14], additional practical solutions may be explored. Our Opinion aims at providing pragmatic advice in this regard.

II. MAIN RECOMMENDATIONS

1. Integrating all main data protection principles

The draft decision states that the Privacy Shield as a whole ensures a level of protection that is essentially equivalent to the one guaranteed by the substantive basic principles of the Directive[15]. However, the current draft omits substantive details of some of these principles, relating in particular to **data retention** and **automated processing**. Other essential elements, such as the **purpose limitation** principle should be better clarified. The **exceptions** to the Privacy Shield requirements are also to be better specified. The draft decision does not fully explain how, even if taken as a whole, the Privacy Shield or the U.S. legal order could fill these gaps. As mentioned above, the Privacy Shield should therefore be amended to better integrate all main EU data protection principles[16], as will be developed in section III.1 of this Opinion. In addition, the provisions addressing **onward transfers**, the **right to access** and the **right to object** should be improved. The EDPS would like to underline the WP29 recommendations in this regard.

2. Limiting derogations

According to Annex II.I.5(a), the Privacy Shield principles can be limited to the extent necessary to meet national security, law enforcement or any public interest requirement. Annex II.I.5(b) also allows limitations of the principles if a statute, regulation or case law creates conflicting obligations or explicit authorisations, without any limitation on the purpose of such access. **The purposes for which exceptions are allowed and the**

requirement of a legal basis should be more precise in both (a) and (b). The EDPS notes that one of the reasons of the invalidation of the Safe Harbour Decision[17] was the absence of findings on rules limiting interferences by U.S. authorities with the rights of the persons whose data are transferred from the EU. The Court has also required clear and precise rules limiting the scope and application of any interference with fundamental rights[18]. **For the same reasons, Annex II.I.5(c) should better specify the purposes for which derogations are possible or be deleted**.

The EDPS welcomes the efforts towards increased transparency in the information provided by the Office of the Director of National Intelligence on access to data by U.S. authorities[19]. The EDPS also notes significant guidance in the Presidential Policy Directive 28 (hereafter: "PPD 28") against mass collection. However, PPD 28 allows the further processing of data collected in bulk to "facilitate targeted collection" and for at least six other purposes. In addition, while the draft decision states that signals intelligence may be collected exclusively where there is a foreign intelligence or counterintelligence purpose, the term "foreign intelligence" is broadly defined[20]. In addition, we assume that the conditions for access by U.S. authorities to personal data that "has been transferred"[21] are different to those relating to access to personal data "to be transferred"[22]. We recommend nuancing recital 55 of the draft decision, which states that limitations on the access and use of personal data transferred under the EU-U.S. Privacy Shield for national security purposes are "clear"[23].

Although PPD 28 constitutes a positive development, it remains to be seen how **further policy and legislative amendments**, e.g. as regards Executive Order 12333, **could help meet the adequacy requirements**. The 2017 review of Section 702 FISA, which presently does not appear to require the government to identify particular targets or give the Foreign Intelligence Surveillance Court a rationale for individual targeting[24], could also be a good opportunity in this regard.

3. Improving redress and oversight mechanisms

As stated by the WP29, in order to improve the redress mechanism proposed in the national security area, the role of the **Ombudsperson** should also be further developed, so that she is able to act **independently** not only from the intelligence community but also from any other authority[25]. In practical terms, the possibility of reporting directly to Congress could be one option in this regard.

We recommend that the European Commission seek more **specific commitments that the requests for information and cooperation from the Ombudsperson, as well as her decisions and recommendations, will be effectively respected and implemented by all competent agencies and bodies**. Further commitments from U.S. authorities ensuring increased **cooperation between the different oversight layers** would also be welcome. The appropriate oversight bodies, in particular the Inspectors-General concerned, could commit to prioritise coordination with the Ombudsperson. Her case-by-case analysis of complaints could better take into account the on-going assessment by the PCLOB of the U.S. legal bases for surveillance and its recommendations.

The EDPS notes that these bodies have the role of overseeing compliance with U.S. statutes, rules and case law, which leads to differences in the level of protection to U.S. and non U.S. persons and which allow processing by U.S. authorities; this appears not to be "essentially equivalent" to the derogations provided in the EU data protection framework[26]. We would

encourage the European Commission to explore the feasibility of **involving EU representatives in (a) the assessment of the results of the oversight system** for processing by U.S. authorities of personal data that have been transferred from the EU and **(b) notification of certain categories of personal data to be processed** by U.S. authorities, in particular where such processing may raise fundamental rights concerns. This involvement could even take the form of a panel including trusted third party high level representatives from one or more EU parliamentary committees and/or national oversight mechanisms on intelligence, and/or EU or national high courts and/or data protection authorities (hereafter: DPA).

The solutions proposed by the Commission under the EU-U.S. agreement on the processing and transfer of financial messaging data (hereafter: "TFTP") have been a precedent; in particular, as regards **authorisation by a judicial authority** before certain requests by U.S. authorities may be responded to[27]. The initial TFTP arrangement also included **supervision by an EU judge** of the further processing of the data[28]. **EU DPAs** are also currently involved in the oversight of the way U.S. requests are handled[29]. Useful examples can also be found in some EU Member States where national intelligence activities are subject to DPA jurisdiction[30]. In this regard, the **notification of the categories of personal data to be processed** by U.S. authorities to a panel including an independent authority from the EU, in particular where the processing may raise concerns according to EU standards, could help alleviating concerns.

III. ADDITIONAL RECOMMENDATIONS

1. Provisions on transfers for commercial purposes

Fully integrating the data minimisation and data retention principles

The EDPS recommends modifying Annex II to more clearly **prohibit keeping personal data in a form which permits identification of data subjects for longer than necessary** for the purposes for which the data were collected or further processed. Such an obligation is an essential principle of data protection law, since it ensures that no personal data are processed for longer than needed and thus would require certified organisations to establish a data retention policy[31].

Annex II.II.5 of the draft decision states that "personal information must be limited to the information that is *relevant* for the purposes of processing". The EDPS recommends, in compliance with the data minimisation principle adding the requirement that **personal information be *adequate and not excessive*** or ***limited to the information that is necessary* for the purposes for which they are collected and/or further processed**[32].

Adding safeguards as regards automated processing

In Annex II a principle should be added containing measures to safeguard the legitimate interests of individuals where they are subject to a decision which produces legal effects concerning them or significantly affects them and which is **based solely on automated processing** of data intended to evaluate certain personal aspects relating to them, such as their performance at work, creditworthiness, reliability, conduct, etc. Such safeguards could include allowing them to obtain human intervention on the part of the controller, to express their point of view and to contest the decision, and to obtain information about the logic

underpinning the processing. Inspiration could also be drawn from Article 15 of the Umbrella agreement[33].

Clarifying the purpose limitation principle

As the WP29 has noted, terms such as "different purposes", "materially different" purposes, or "a use that is not consistent with" which recur in the draft decision are not clear and may cause misunderstandings[34]. The EDPS recommends **streamlining the concepts used around the notion of "purpose"**. Preferably, the term "(in)compatible purpose" should be used throughout the document. In any case, it should be specified that "materially different" purposes for which data may be further processed should be compatible with the purposes for which the data were initially collected.

Further use for **marketing purposes** of personal data initially processed for medical or pharmaceutical research or for human resources purposes should in any case not be considered as compatible with the initial purpose. Therefore, the references to such possibility in supplemental principles 9(b)(i) and 14(b)(i) should be deleted.

Limiting exceptions

The numerous exceptions to the Privacy Shield principles[35] may make it difficult for organisations, data subjects and DPAs to determine whether specific types of processing are covered. This is particularly important as commercial transfers not covered by the draft decision will need to be covered by other tools (e.g. BCRs, SCCs). The scope of these exceptions should therefore be clearly stated in detail in the draft decision to ensure legal certainty. In addition, some of them can be problematic since they may **contradict the key requirements of the EU data protection legislation**.

This also applies to "**journalistic material**"[36], which is completely exempted from the requirements of the Privacy Shield principles. However there is an obligation to balance the right of freedom of expression with the rights of privacy and data protection, both under the Charter and in accordance with the Directive as interpreted by the CJEU, in particular the Google Spain[37] and the Satamedia[38] rulings[39]. We therefore recommend replacing this general exemption by particular derogations to certain requirements[40] only where they are necessary to reconcile the rights to privacy and data protection with the rules governing freedom of expression and where this "journalistic material" is to be used for journalistic purposes.

Improving redress and oversight

As regards oversight of the transfers for commercial purposes, despite positive changes, we still **recommend an outcome where U.S. authorities will systematically and effectively monitor compliance with the Privacy Shield principles**. For instance, the draft decision could be complemented to highlight how on-site visits or inspections on the premises of self-certified organisations to investigate compliance with the Privacy Shield principles will be conducted [41]. Regarding the "Operation of DPA Panels"[42], the text should be more precise on the manner this panel will function compared to the panel established by the Safe Harbour. We assume that the positive elements of previous experiences may be preserved. In the light of recent developments on U.S. enforcement, we also recommend clarification of the respective roles of the FCC and the FTC over broadband internet service providers.

The draft decision should also assess the means which are effective in practice for individuals whose data have been transferred under the Privacy Shield to bring cases to U.S. Courts. Whilst the plurality of avenues for individuals to seek redress at federal and State level demonstrates the willingness to offer effective redress mechanisms for individuals, this is offset by the complexity of the system. In order to facilitate direct access for individuals to independent redress, and taking into account the complexity of the mechanisms proposed, we recommend improving the system building on the voluntary option for certified organisations insofar as they process data which has been transferred in accordance with the Privacy Shield, to be **subject to supervision by DPAs,** so as to benefit from their expertise with regard to processing of personal data. In this regard, the WP29 has also recommended that privacy policies include the possibility for EU individuals to bring claims for damages in the EU[43].

2. Recommendations regarding access by U.S. authorities

The draft decision states that taken as a whole, the oversight and recourse mechanisms provided offer legal remedies to the data subject to gain access to his/her personal data and to request their rectification or erasure[44]. However, the draft decision does not fully assess the possibilities for individuals to exercise their **rights of access, rectification or erasure** concerning data collected or accessed by public authorities **for purposes other than national security** (e.g. law enforcement or other "public interest" purposes)[45]. This require precise clarifications in the decision. In this regard, the EDPS notes that the recently adopted Judicial Redress Act[46] only applies to "records" transferred from public or private entities of the covered countries (i.e. the EU) directly to U.S. public authorities[47]. This excludes personal data transferred between private entities under the Privacy Shield and subsequently requested or accessed by U.S. authorities.

The EDPS notes that several levels of oversight and redress are available in the U.S., but even taken as a whole they do not appear to cover adequately all instances where government may access personal data. Furthermore, non U.S. persons do not always enjoy the same rights as U.S. persons under U.S. Constitution, laws and regulations. The actual relevance of these oversight and redress mechanisms for the Privacy Shield is therefore limited. **Additional safeguards for independent supervision and redress** are therefore needed in the case of access for law enforcement and other public interests purposes.

3. Assessing the impact of other relevant statutes and rules

All rules applicable to data transferred from the EU to the U.S. under the draft decision should be assessed in the light of the many exceptions from the application of the Privacy Shield principles applying to processing for commercial purposes or where other rules may interfere with these principles. This assessment should include **U.S. federal and state laws** allowing **access for public interest purposes** other than national security and law enforcement, and other laws and regulations with an impact on the protection of personal data[48]. The assessment should also include relevant **international commitments** in particular those providing for access to or transfers by public authorities of personal data initially processed for commercial purposes.

4. A meaningful review

As required by the WP29, the joint review of the application of the Privacy Shield should not only include meetings with public and private entities but also **on-the-spot verifications**. The review should not be limited to the commercial part of the draft decision, but should also cover **access by U.S. authorities to the data transferred under the Privacy Shield**. This should be specified in the draft decision. The draft decision should also mention that the **conclusions and findings at least of EU DPAs will be reflected in the report** of the joint review.

5. Interaction with the GDPR

As mentioned above, any solution for transfers between the EU and the U.S. affording some stability should take into account the new EU data protection framework. This is essential to provide a consistent level of protection and legal certainty with regard to the main principles of the EU data protection framework, not only in the short term but also in the medium and long term. In particular, the draft decision should also consider new elements of the GDPR which are not present in the Directive, such as the principles of **privacy by design, privacy by default, or data portability.** The EDPS notes that the GDPR also provides clearer and more detailed criteria for adequacy decisions, including the existence and effective functioning of **independent supervisory authorities** in the third country in question[49].

Finally, the GDPR innovates the scope of application of the EU data protection framework. Controllers or processors not established in the EU will be subject to EU rules as long as their processing activities are related to the offering of goods and services to individuals in the EU or the monitoring of their behaviour. In those cases, certification under the Privacy Shield will not exempt certified organisations from the application of the EU data protection legal framework if they fall within its new scope. In such case, the EU legal framework will prevail over the Privacy Shield principles and such organisations will be required to comply directly with the GDPR.

IV. CONCLUSION

The EDPS welcomes the efforts shown by the parties to find a solution for transfers of personal data from the EU to the U.S. for commercial purposes under a system of self-certification. However, robust improvements are needed in order to achieve a solid framework, stable in the long term.

Done in Brussels, 30 May 2016

(signed)

Giovanni BUTTARELLI

European Data Protection Supervisor

[1] Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, 6 October 2015 (hereafter: "*Schrems*").
[2] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the U.S. Department of Commerce (notified under document number C(2000) 2441), (OJ 2000 L 215, p. 7).
[3] Commission Implementing Decision of XXX pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, available on: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf.
[4] See the Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on "Rebuilding Trust in EU-U.S. Data Flows" and on the 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", 20 February 2014, and the EDPS pleading at the hearing of the CJEU in the *Schrems* case, available on: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Court/2015/15-03-24_EDPS_Pleading_Schrems_vs_Data_Commissioner_EN.pdf).
[5] Article 29 Working Party in the Opinion 01/2016 on the EU-U.S. Privacy Shield adequacy decision, (WP 238), available on: http://ec.europa.eu/jus.tice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.
[6] See also the keynote speech by UK Information Commissioner Christopher Graham at the IAPP Europe Data Protection Intensive 2016 Conference in London. Speech available (video) on: https://iapp.org/news/video/iapp-europe-data-protection-intensive-2016-christopher-graham-keynote/.
[7] Letter to Article 29 Working Party and other institutions, signed by Access Now and other 26 NGOs.
[8] European Parliament resolution of 26 May 2016 on transatlantic data flows (2016/2727(RSP)).
[9] *Idem*, para. 14.
[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[11] *Schrems*, para. 71, 73, 74 and 96.
[12] This approach was already considered in one of the earliest WP29 papers on the subject of data transfers (WP12: "Working document on transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive", 24 July 1998).
[13] See for example, clarifications in Annex VI.1. a), that PPD28 would apply to data collected from transatlantic cables by the U.S. Intelligence Community.
[14] At the hearing of the EUCJ in the *Schrems* case, the EDPS stated that "*The only effective solution is the negotiation of an international agreement providing adequate protection against indiscriminate surveillance, including obligations on oversight, transparency, redress and data protection rights*", EDPS pleading at the hearing of the Court of Justice of 24 March 2015 in Case C-362/14 (Schrems v Data Protection Commissioner).
[15] Draft decision, recital 49.
[16] In the *Schrems* judgement, the Court found that Article 1 of the Commission decision on Safe Harbour failed to comply with the requirements of the Directive and was therefore invalid (see para. 98). Therefore, it did not examine the content of the Safe Harbour principles. However, it stated that the Directive seeks to ensure not only effective and complete protection of the fundamental rights and freedoms but also a high level of protection of those rights and freedoms. The objective of its Article 25(6) is to ensure that this level of high protection continues where personal data are transferred to a third country (see para. 72). "Adequate level of protection" must therefore be understood as a level of protection which is "essentially equivalent" to that guaranteed in the EU by the Directive read in the light of the Charter. Otherwise, the objective mentioned above would not be met and the level of protection guaranteed by the Directive could easily be circumvented by transfers to third countries (see para. 73). Although the means used by the third country in question may be different from those used in the EU (e.g., a system of self-certification (see para. 80)), they must prove effective to ensure this essentially equivalent protection (para. 74). The assessment should in any case be strict, taking into account the importance of the protection of personal data in the light of the right to privacy and the large number of persons whose fundamental rights may be infringed (para. 78). Therefore, all the essential elements of the Directive should be considered.
[17] *Schrems*, para. 88.

[18] In the *Schrems* judgment, the CJEU required clear and precise rules limiting the scope and application of any interference with the fundamental rights of the persons whose data were transferred from the EU to the U.S. (para 81). Such rules, which should also lay down safeguards against abuse, are particularly needed in case of automated processing and where there is a significant risk of unlawful access (para. 91). See also Digital Rights Ireland v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others, Court of Justice of the European Union, 8 April 2014, Joined Cases C-293/12 and C-594/12, para. 54-55). In addition, such rules should be based on objective criteria determining the limits of the processing for specific and strictly restricted purposes, which should be capable of justifying the interference (*Schrems*, para. 93).

[19] Draft decision, Annex VI.

[20] It includes not only "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof" and "international terrorists", but also information relating to "foreign organisations" and "foreign persons" (Presidential Policy Directive 28: Signals Activities (PPD-28) (Jan. 17, 2014), footnote 2).

[21] Draft decision, recital 65.

[22] Draft decision, recital 67.

[23] Draft decision, recital 55.

[24] PCLOB Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, 2 July 2014, p. 106.

[25] Draft decision, recitals 53 and 104.

[26] According to the Commission, the reach of U.S. surveillance programmes combined with the unequal treatment of EU citizens brought into question the level of protection afforded by the Safe Harbour arrangement (*Communication on Rebuilding Trust in EU-U.S. Data Flows* (COM(2013) 846 final, p. 4). As regards the significant differences between the safeguards applicable to U.S. persons compared with those applicable non U.S. persons see also *Report on the Findings by the EU Co-chairs of the ad hoc EU-U.S. Working Group on Data Protection* of 27 November 2013, p. 17.

[27] See the European Commission's press release on the Adoption of a proposal for a mandate for negotiating an agreement on bank data transfers with the United States government under the Terrorist Financing Tracking Programme, 24 March 2010. In the final text of the agreement, judicial authorisation was replaced by authorisation by Europol, according to Article 4 of the 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 195/5).

[28] See the "TFTP representations" on Processing of EU originating Personal Data by United States Treasury Department for Counter Terrorism Purposes - 'SWIFT' (OJ 2007, C 166/09), which allowed the EU to designate an "eminent European person" to verify if the U.S. was respecting its commitments. In 2008 the European Commission designated judge Bruguière as "eminent person" (Press Release of the European Commission, *EU Review of the United States' "Terrorist Finance Tracking Programme"*, IP/08/400, 7 March 2008).

[29] As part of its supervision tasks, the Europol Joint Supervisory Body, composed of representatives of each EU national data protection authority, monitors the role of Europol in authorising U.S. requests of personal data in the framework of the TFTP agreement. In addition, national EU data protection authorities are involved in the joint review of the agreement, according to Article 13 of the 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 195/5).

[30] See Garante per la protezione dei dati personali, "Summary of key activities by the Italian DPA in 2013", para 1.1, available on: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3205017 (in English) and the Press release (in Italian), "Sicurezza dati personali: Protocollo d'intenti tra l'Autorità Garante e il Direttore Generale del Dis", 11 Novembre 2013, available on: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2746204. See also European Union Agency for Fundamental Rights, "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Mapping Member States' legal frameworks, 2015", available on: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf.

[31] Although Annex VI provides for a retention period of five years for intelligence purposes, it further clarifies that information can be retained for more than five years "if that continued retention is in the national interests of the United States". Furthermore, this principle does not cover data transferred and used for purely commercial purposes.

[32] See Article 6(1)(c) of the Directive.

[33] 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. Draft for

initialling available on: http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf. See also EDPS 1/2016 Opinion of 12 February 2016 on the Umbrella Agreement, para. 44.

[34] Article 29 Working Party in the Opinion 01/2016 on the EU-U.S. Privacy Shield adequacy decision (WP 238), p. 20.

[35] For example, Supplemental principle 3 provides for an exemption of liability for ISPs, telecommunication carriers and "other organisations" under the Privacy Shield when they merely transmit, route, switch, or cache information on behalf of another organisation. Recital 47 of the Directive 95/46 does not exclude that such entities can be processors, and can therefore be subject to the Directive. Moreover, the processing of data by these entities is already covered by the e-privacy Directive. Finally, the derogatory regime of liability of the e-commerce Directive 2000/31 does not apply to data protection law (Article 1(5)(b)). As telecommunications carriers seem to be excluded from the scope of application of the Privacy Shield, their inclusion in this principle creates confusion.

[36] Annex II, III, 2(b) of the draft decision.

[37] Case C-131/12 – Google Spain v. Agencia Española de Protección de Datos and Mario Costeja González, 13 May 2014.

[38] Case C-73/0716 Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy, 16 December 2008.

39 See also the case law of the European Court of Human Rights, in particular Von Hannover v. Germany, no. 59320/00, Von Hannover v. Germany (no. 2) [GC] nos. 40660/08 and 60641/08, and Axel Springer AG v. Germany [GC] no. 39954/08.

[40] See also Article 9 of the Directive.

[41] In *Schrems*, para. 81, the CJEU states regarding the self-certification system that "*the reliability of such a system [...] is founded essentially on the establishment of effective detection and supervision mechanisms enabling any infringements of the rules ensuring the protection of fundamental rights, in particular the right to respect for private life and the right to protection of personal data, to be identified and punished in practice*".

[42] See Supplemental Principles in Privacy Shield Annex II.III.5 (c).

[43] Article 29 Working Party in the Opinion 01/2016 on the EU - U.S. Privacy Shield adequacy decision, (WP 238), p. 27 and Article 29 Working Party, letter to Vice-President Reding on 10 April 2014, p. 5, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf.

[44] Draft decision, para. 50-51.

[45] Draft decision, p.29.

[46] Judicial Redress Act of 2015, Pub.L. 114-126, H.R. 1428.

[47] Sec. 2h4a of the Judicial Redress Act.

[48] Such as the Health Insurance Portability and Accountability Act of 1996, Pub.L., 110 Stat. 1936 (HIPAA) or the Children's Online Privacy Protection Act of 1998, Pub.L. 105-277, 112 Stat. 2681-728 (COPPA).

[49] See Article Art. 45(2)(b) of the GDPR.