EUROPEAN DATA PROTECTION SUPERVISOR

Executive summary of the opinion of the European Data Protection Supervisor on the EU-US Privacy Shield draft adequacy decision

(The full text of this opinion can be found in English, French and German on the EDPS website www.edps.europa.eu)

(2016/C 257/05)

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 US 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 US, 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 US side by the US 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 US 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 US 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 US 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.

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 US on 2 February 2016 on a new framework for transfers of personal data called 'the EU-US 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 US 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 US 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 US 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 US 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.

([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 US Department of Commerce (notified under document number C(2000) 2441) (OJ L 215, 25.8.2000, 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-US 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-US 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 1/2016 on the EU-US 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 26 other NGOs.
([8]) European Parliament resolution of 26 May 2016 on transatlantic data flows (2016/2727(RSP)).
([9]) *Idem*, para. 14.

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) ([1]) 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 ([2]). 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 US 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 ([3]). 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-US 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-US 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 US 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 US authorities (for instance, statements concerning signals intelligence

([1]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

([2]) *Schrems*, para. 71, 73, 74 and 96.

([3]) 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).

activities over transatlantic cables, if any) [1]. 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 [2], additional practical solutions may be explored. Our opinion aims at providing pragmatic advice in this regard.

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 US 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.

Giovanni BUTTARELLI

European Data Protection Supervisor

[1] See for example, clarifications in Annex VI.1(a) that PPD28 would apply to data collected from transatlantic cables by the US intelligence community.

[2] 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*).