Giovanni Buttarelli

European Data Protection Supervisor

Towards an Opinion on the EU-US Privacy Shield

LIBE Committee hearing

17 March 2016

Ladies and gentlemen,

Distinguished Members of the European Parliament,

Thank you for the invitation to this preliminary discussion about the EU-US Privacy Shield.

As you know, the EDPS, along with the other independent data protection authorities in the EU, has been following the issue of transatlantic dialogue for a long time.

The EDPS, as an independent advisor to the EU legislator, has - on numerous occasions - expressed a position on personal data transfers between the EU and the U.S, and on the importance of this issue for restoring trust.

Indeed, in our pleading at the hearing before the Court of Justice of the EU in the *Schrems* case, we affirmed our belief in the need for a robust and sustainable solution[1].

We therefore appreciate the commitment to finding such a solution.

And we recognise the efforts made by the negotiators during this first series of negotiations.

It is a positive sign that not only the U.S. Department of Commerce and the Federal Trade Commission, but also the Department of Justice, the Department of State and the Office of the Director of National Intelligence are involved.

[1] "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".

An adequacy decision with a strategic partner like the U.S. addresses the needs of hundreds of companies, in particular SMEs, for whom Binding Corporate Rules or standard contractual clauses may not feasible or appropriate.

But in addressing these needs, a lasting solution must be capable of providing legal certainty. It must be capable of being credibly defended - and upheld! - in case of future scrutiny before the Court.

We are of course at an early stage in our analysis of the complex detail of the draft adequacy decision and its annexes published by the Commission last month.

As the President of the Article 29 Working Party has just said, the community of data protection authorities of Europe intend to speak with one voice on the Privacy Shield.

The EDPS will contribute to that collective opinion as a member of the Working Party.

Shortly afterwards, as the adviser on data protection matters to this Parliament, to the Commission and the Council, we will then issue our own opinion, in full synergy with the position of the Working Party.

We will deliver our advice in good time, so that the Commission and the Article 31 Committee can benefit before the decision is concluded.

I am afraid it is too early today to give you a detailed insight into the main lines of the legal analysis that we started in the last few days.

This is an independent analysis, but of course we are listening attentively to the observations and arguments of experts in this area, whether businesses, civil society or academics.

As you have seen, very conflicting comments have already been made:

- Those that argue that the Privacy Shield does not bring significant changes compared to the Safe Harbor Decision, and in certain respects is even weaker.
- Others say that the Privacy Shield indeed contains improvements, both in the commercial part of the package and in the part that deals with derogations for public security and for law enforcement purposes.

Let me therefore briefly outline just five of the areas which will need to be considered.

First, we have to consider the question of timing.

If the Commission decision is adopted before the entry into force of the GDPR, the decision will have to be based on the current framework of 1995 Data Protection Directive.

Therefore, at this stage, the ongoing legal analysis involves different points, all of which are largely assessed on the basis of the 1995 Directive, interpreted in the light of the EU Charter of Fundamental Rights and the case law of the EU Court of Justice, in particular the *Schrems* case.

Could this have significant consequences in terms of legal formalities.

In any event, a future-oriented approach would be wise, since with the full implementation of the Data Protection Regulation two years from now, all processing operations - not only transfers to the US - will be subject to EU rules for those who will offer goods and services from the US to the EU or will remotely monitor the behaviour of individuals in the EU.

Second, a full assessment should also look into the possible interplay between the Privacy Shield and the EU-US Umbrella Agreement for transfers of data for law enforcement purposes.

I addressed you last month on the Opinion on the Umbrella Agreement.

You may recall that, in that Opinion, the EDPS noted that the provisions of the Agreement also applied to transfers of data from relevant private companies to the US competent authorities, subject to those transfers being based on an international agreement.

Third, as you know, there is the requirement of the 1995 Data Protection Directive that the European Commission, before finding a system to be adequate, must analyse the domestic law and international commitments of the third country in question.

We are all aware that recently the Court of Justice - and indeed also since the 1990s, the Article 29 Working Party in its various opinions - has clarified that it is the **legal order** of the third country that must ensure an adequate level of protection.

Therefore, an assessment is needed of not only **the applicable rules** resulting from domestic law or international commitments, but also **their effectiveness in practice**.

The analysis may also refer to what extent, in the absence of legislative changes limiting the processing of US authorities of personal data transferred from the EU, the terms of the new adequacy decision correspond to the Court requirements.

The analysis needs to consider the privacy shield principles, their legal value, to what extent they are binding, their stability against political changes, the effectiveness of oversight and redress mechanisms, and clarity on derogations.

In other words, what is the effective meaning of "essential equivalence" of a third country's data protection rules?

The means to which the third country has recourse to ensure such a level of protection may be different, but they must prove effective in practice.

The objective, as stated by the Court, is that where the data are transferred to a third country the high level of protection continues to apply.

A fourth question is raised by the derogations for national security and law enforcement purposes. The Court requires clear and precise rules limiting the scope and application of any interference with the fundamental rights of the persons whose data are transferred from the EU to the U.S.[2].

[2] *Idem*, para. 88.

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.[3]

We will soon publish our pleading on the Canadian PNR court case, where significant questions on necessity and proportionality of access by law enforcement bodies are addressed.

Finally, a fifth issue: as the Court has stated, adequacy decisions are 'living instruments', requiring periodic reviews in the light of changing circumstances. So the review provisions also require careful scrutiny.

In conclusion, it is too soon to say to which extent the current Privacy Shield is a a success.

Nevertheless, the need for legal certainty, whether for companies or for individuals, leaves us no room for error. Although it will only be related to Privacy Shield transfers, the adequacy finding will be indirectly relevant for other transfers, such as those based on standard contractual Clauses or Binding Corporate Rules.

Let us not forget that this decision is of major importance not simply for transatlantic relations; it has international resonance: many third countries will be closely following progress against the background of the adoption of the new EU data protection framework.

For that reason we trust that the Commission will take on board the recommendations of independent data protection authorities before finalising the decision.

We remain at the disposal of the institutions for further advice and dialogue on this issue.

Thank you for listening.

[3] *Idem*, para. 91. 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.