Request for an Opinion by the European Parliament, draft EU-Canada PNR agreement (**Opinion 1/15**)

Hearing of 5 April 2016

Pleading notes of the European Data Protection Supervisor (EDPS)

Mr President, Ladies and Gentlemen Members of the Court, Mr Advocate General.

Thank you for inviting the European Data Protection Supervisor today.

As a preliminary remark, we should keep in mind that this draft agreement with Canada is only one piece of a complex patchwork of bilateral exchanges of personal data, put in place in the name of public safety and security. Similar PNR agreements are already in place with the United States and Australia, and an agreement with Mexico is under negotiation.

But other countries have also demanded PNR data from Europe, from Russia to Saudi Arabia[1]. Those states might soon want to negotiate their own PNR agreements. We therefore need this Opinion to set a true "gold standard" for the future.

We have already had the opportunity to answer questions from the Court in writing. Today, I would like to bring the following three points to your attention:

First, the guarantees required under Article 8 of the Charter must be respected. An international agreement that governs data transfers cannot lower the level of protection of that fundamental right.

My second point is that the processing of PNR data is systematic and particularly intrusive in nature. Therefore, the review of EU legislature's discretion must be strict.

[1] Study for the Council of Europe T-PD committee "*Passenger Name Records, data mining and data protection: the need for stronger safeguards*" by Prof. Douwe Korff, 15 June 2015, p. 73.

And finally my third point: the draft agreement -- in its present form -- does not ensure a level of protection required under Article 8 of the Charter.

As to my first point:

As a principle, data transfers from the territory of the Union to a third country can take place only when that country ensures an adequate level of protection. When the third country has not been declared as adequate, transfers are possible as long as additional safeguards are present. In the absence of rules covering personal data once it has left the territory of the Union, there would be no effective protection under Article 8 of the Charter.

In *Schrems* this Court set a number of criteria, derived directly from Articles 7, 8 and 47 of the Charter, with which a finding of adequacy must comply.

Contrary to what the Commission maintains, it is clear that the legal effects of the draft agreement would be very similar to an adequacy decision within the meaning of Directive 95/46. I refer here to Article 5 that would create a presumption of legality of all PNR transfers without the need to provide any additional safeguards.

Therefore, the criteria which apply to adequacy findings must also be fulfilled by an international agreement such as the one at issue today. If it were not the case, the legal framework for adequacy could be easily circumvented by creating a parallel system of international transfer arrangements with lesser protection.

One key requirement identified in *Schrems* is -- that the third country in question must give individuals the right to pursue effective legal remedies, for example in order to have access to personal data related to them (para. 95).

We submit that such remedy does not effectively exist under the draft agreement.

First, Article 14(2) of the draft agreement implies that some "other remedy" might be provided instead of judicial redress.

Second, and more importantly, the Canadian Privacy Act excludes individuals who are not Canadian citizens or permanent residents from the right of access to their personal data (Article 12). As a result, it would seem that, at present, there

is no effective legal remedy that EU citizens outside Canada could pursue before Canadian courts, since they would not be able to invoke any right of access on the basis of the Canadian legislation currently in force.

The second point I would like to make today is that the processing of PNR data constitutes a very serious interference with fundamental rights.

It is important to dispel the myth that PNR data processing is somehow less intrusive than, for example, retention of communications traffic and location data.

Admittedly, Passenger Name Records may disclose fewer details about private lives than communications metadata, especially when one does not travel by airplane very often. Nevertheless, PNR can reveal one's travel habits, the relationship between two (or more) people, the fact that they shared the same flight as well as the same hotel, the person or company who paid for your ticket, and so on. Dietary information (such as requests for kosher or hala'l meals) typically serves as a *proxy* for sensitive information about religious beliefs.

It is also clear that PNR data processing does not require a connection to a specific threat to public security. On the contrary, the draft agreement obliges air carriers to transfer the data solely based on the fact that a person is taking a flight to or from Canada. Given that over 62 million of passengers travelled between the EU and North America in 2014, many millions of individuals are affected.

However, it is not only the scale of the collection of PNR data that matters in this case. What matters -- is the way in which PNR data are actually and potentially being used.

Mr President,

The draft agreement is very vague in defining how PNR data will be used in practice. It does not go beyond general statements that it "*has proven to be a very important tool in the fight against terrorism and serious crime*"[2].

[2] Explanatory memorandum to the draft Agreement

Some of the processing described by the Commission and others appear rather uncontroversial, such as checking against other databases of criminal suspects, stolen passports or credit cards etc.

However, the real reason why PNR data is so valuable to law enforcement authorities is that, thanks to complex computer algorithms, it allows them to *identify* previously unknown individuals. PNR makes possible what is known as "predictive policing".

As the Commission explains in its replies to question II.3.b, what we are talking about here is policing based on abstract definitions of what a potential criminal or otherwise suspicious behaviour might look like. These definitions are created on the basis of an analysis of PNR data over long periods of time[3] and are subsequently applied to every individual passenger in order to pinpoint those who "fit the profile".

[3] COM(2010) 492 final, Communication from the Commission on the global approach to transfers of PNR data to third countries.

In this respect, it is interesting to read the last annual report from the Privacy Commissioner of Canada. He underlines (on p. 43) that in the past, the Canadian Border Security Agency used an individual risk scoring method that analysed specific passengers and gave them a risk value based on their own distinct data elements. Passengers with a high risk score would be flagged for further review.

By contrast, "*[t]he new scenario-based method uses Big Data analytics to evaluate all data collected from air carriers against a set of conditions or scenarios*" and has been designed to harmonize with the system used by the United States.

The Privacy Commissioner is particularly concerned that passengers may be targeted on the basis of their age, gender, nationality, birthplace, or racial or ethnic origin. He observes that the system "*could allow the operator to, for example, search for all males aged between the ages of 18-20 who are Egyptian nationals and who have visited both Paris and New York*."

We note that such criteria are reminiscent of the *Rasterfahndung* or "pattern searches" system used by the German police after the terrorist attacks of 11 September 2001. This was declared unconstitutional by the German Constitutional Court in 2006.

We touch here on one crucial aspect of PNR data processing that is different from the retention of communications data which was at stake in *Digital Rights Ireland*. The communications metadata was basically passively stored by the provider until it was accessed and used in a specific case, usually in search of evidence of past wrongdoing of a person identified as a suspect of serious crime. In most cases, it would not have been accessed or used at all. By contrast, practically all of the PNR data transferred by air carriers is systematically analysed in order to make assumptions about who is or is not a high-risk traveller.

What is more, as clearly stated by the Commission and other parties, PNR are in fact unverified information. In other words, they are neither complete, nor necessarily accurate. Vast amounts of such unverified information about millions of passengers over extended periods of time are pooled together and analysed. On this basis, decisions are then taken with potentially very serious

consequences for individual passengers, such as denying them entry on board of an aircraft, additional security searches, limitations of liberty for further questioning on arrival etc. It is obviously very difficult, if not outright impossible, for those concerned to defend themselves against such decisions. This, in our view, compounds the intrusiveness of this processing.

As to my third and final point.

Article 8(3) of the Charter requires that processing be subject to control by an independent supervisory authority, which according to this Court is an essential component of the right to the protection of personal data.

It is fairly obvious, I think, that the draft agreement, in its present formulation, does not guarantee supervision by an independent authority.

Structurally integrated within the Canadian Border Security Agency, the Recourse Directorate is in essence an internal review mechanism and could at best be compared with the function of the internal Data Protection Officer. This is a function mandatory for EU institutions and it also exists in certain Member

States. But it is clearly not an independent Data Protection Authority in the meaning of the case law of this Court.

The draft agreement does not guarantee independent control by a European supervisory authority, either. Such independent control cannot exist without the power to examine, with complete independence, whether the transfer of data complies with the law (*Schrems*, paras. 57-58) and to take the necessary enforcement action when the transfer does not comply.

Mr President,

The draft agreement renders independent control by European authorities meaningless. It clearly lays down a commitment of the EU "*to not prevent the transfer of PNR data from the EU carriers to Canada*" (Article 4(1)).

This provision would effectively deprive supervisory authorities of the power to suspend or terminate a transfer of PNR data to Canada, even in cases where basic requirements of data protection law are breached.

Finally, if -- as we submit in our written responses -- the draft agreement were correctly based on Article 16 of the Treaty, the need for independent control would have been even more evident, because as clearly follows from paragraph 2 thereof, legislation based on Article 16 must fully ensure independent control.

This brings me to my conclusions.

Firstly, the draft agreement does not guarantee effective judicial remedy.

Secondly, PNR data processing for "predictive policing" purposes is systematic and particularly intrusive.

And finally, independent supervision required by Article 8(3) of the Charter is not guaranteed.

Thank you for your attention.

Anna Buchta

Agent of the EDPS