

Comments of the EDPS on different international agreements, notably the EU-US and EU-AUS PNR agreements, the EU-US TFTP agreement, and the need of a comprehensive approach to international data exchange agreements

I. The PNR agreements

The EDPS has expressed comments at several occasions with regard to the **EU-US PNR agreement**, notably in his interventions before the Court of Justice¹ and in opinions² adopted together with the Article 29 Working Party.

A number of these comments have not been taken into account in the definitive version of the agreement and are still valid. Since then, the agreement has provisionally entered into force, although it has not yet officially been concluded, and some opportunities have arisen to evaluate its effectiveness. The level of protection afforded by the agreement should therefore be assessed also in the light of these practical aspects of its implementation. The points below summarise our previous findings in this perspective.

Besides the question of the legal basis of the agreement, the main issue under analysis was the level of adequacy provided by the agreement, in accordance with Article 25 of Directive 95/46/EC³ and Article 8 of the European Convention on Human Rights.

- *Purpose limitation*: The scope of the agreement is not limited to the specific purpose of fighting terrorism. Among the possible purposes listed is the vital interest of any person, or a requirement by law; such a broad purpose raises legal certainty issues, and also has an influence on the appreciation of the balance between the intrusiveness and the necessity of the measures.
- *Quality and proportionality of data*: the list of personal data to be collected is extensive, and includes even sensitive data in exceptional cases, as well as data of third parties - thus not only those of passengers involved in the flight. The duration of storage (15 years) is considered as excessive;
- *Legitimacy of the processing*: the collection of data is not focused on persons presenting a risk: the agreement allows for a bulk collection of personal data and risk assessment applying in an undifferentiated way to all individuals, including therefore a processing of personal data on a great majority of

¹ Cases C-317/04 and C-318/04.

² See the different opinions of the Working Party on US PNR at the following link:

http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/index_en.htm#data_transfers

³ The analysis of adequacy is based on criteria listed in a working document (WP12) of the Article 29 Working Party. This Working Document "on the transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive", adopted on 24 July 1998 can be found at:

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf.

innocent people. Such a wide scale collection, analysis and storage of personal data could raise legitimacy and proportionality issues in relation to the jurisprudence of the European Court of Human Rights (see especially the S. and Marper case⁴);

- Legal certainty: The binding character of CBP's commitments is not clear, as some decisive elements of the agreement are included in a side letter. This could raise a risk of unilateral interpretation by the US of their obligations;
- Onward transfers: the agreement offers wide possibilities of onward transfers, with unclear exceptions to data protection principles: this is the case for instance with regard to "emergency circumstances" allowing for such transfers;
- Rights of individuals: although redress possibilities are foreseen in the agreement, the exercise of rights by the individual in practice, and especially the right to access personal data, remains a challenge: exceptions linked with security reasons could prevent effective exercise of rights.
- Push/pull: the transition from pull to push, in order for airlines to be in control of the data they transmit to the US, is far from satisfactory in practice. Investigations led by the passengers' subgroup of the Article 29 Working Party confirm this important shortcoming⁵.
- Effectiveness of implementation and review: adequacy will be met only if there are guarantees that the principles will be applied and violations are sanctioned in an effective, proportionate and dissuasive manner. The conditions of the review raise practical questions: Data Protection Authorities are not mentioned in the agreement as taking part in the review. They might be involved in practice but there is no legal certainty as to their role and their autonomy with regard to the practical conditions and conclusions of the review.

To conclude on this point, the EU-US agreement should be evaluated from a perspective including not only shortcomings identified at the moment of the negotiation of the agreement, but also taking into account the global context of its implementation. The possible organisation of a review in the coming weeks or months would certainly bring useful elements to complement the present picture.

The **EU-AUS PNR agreement** raises less concerns than the EU-US agreement, and a great part of the issues mentioned at the moment of negotiation of the agreement have been taken into account. Improvements would however be welcome on the following points:

- the duration of storage, which is shorter than in the US agreement (5,5 years) but is still considered as excessive;
- the amount of data transferred, including sensitive data;
- the conditions of the review of the agreement.

With regard to the effective implementation of the agreement, the main elements at stake today are the implementation of a functioning push system and the amount of data required by the Australian Customs.

⁴ S. and Marper v. the United Kingdom, 4 December 2008, nos. 30562/04 and 30566/04.

⁵ See also the reply of the President of the Article 29 Working Party to your letter, relating to the PNR agreements.

The Travellers Data Subgroup of the Article 29 Working Party, in which the EDPS takes part, is following closely the developments relating to the implementation of the Australian and the US PNR agreements. In this respect, reference should be made to the complementary information provided by the President of the Article 29 Working Party in reply to your letter.

II. The EU/US TFTP agreement

The EDPS has closely followed the developments concerning the transfers of financial data from SWIFT to US authorities, and issued last July comments on the negotiating mandate proposed by the Commission for a EU-US agreement. Lately, the EDPS has actively contributed to the joint letter prepared by the Article 29 Working Party and the Working Party on Police and Justice.

Against this background the comments here below will provide, on top of the comments put forward by WP29/WPPJ, some additional elements, mainly focussed on the questions you raise in your letter.

The principle of necessity, proportionality and legal certainty. The measures envisaged in the TFTP agreement are very privacy-intrusive, since they interfere with the private life of all Europeans, also in the light of the increasing use of (trans-border) bank transfers in the European area. Pursuant to Article 8 of the ECHR and the EU legal framework, such an interference must be laid down by law and be foreseeable, as well as necessary to achieve the public interest pursued.

In this perspective, there must be very strong evidence that such an intrusive measure is necessary and proportionate. This also entails demonstrating that these measures present a concrete added value, especially with respect to other less privacy-intrusive EU instruments aimed at combating the misuse of the financial system for the purpose of money laundering and terrorist financing (i.e. anti-money laundering Directive 2005/60 and Regulation 1781/2006 on information on the payer accompanying transfers of funds).

The evidence provided so far to the EDPS does not entirely show this necessity and the real added value with respect to more targeted existing instruments (including the specific instruments for exchange of information between Europol and Eurojust and the US, as well as the EU-US agreement on mutual legal assistance). In the TFTP agreement, as opposed to the PNR agreement, there is no element of connection between the data being processed and the US: the controller is established in Europe, the databases are in Europe, and the data transferred to the US relate to any kind of financial transaction worldwide (such as, in the majority of cases, intra-European payments and payments from Europe to third countries).

With regard to legal certainty and foreseeability, many important data protection elements are still absent or not clearly defined in the agreement (see comments below).

Purpose limitation and data quality (including the aspect of data retention). As the EDPS has expressed at several other occasions, the processing of commercial data for law enforcement purposes is a derogation from the purpose limitation principle, and shall thus be limited and targeted. In this perspective, the EDPS stresses the crucial role of independent judicial oversight in assessing the lawfulness of the US subpoenas requesting for data, and acknowledges that the mechanism laid down by Article 4 of the agreement goes in the right direction.

However, the bulk transfers envisaged by Article 4(6) of the agreement as an exception raise concerns, since recourse to them is not clearly limited and may well develop into a common practice.

The definition of the purpose for which data can be transferred is broader than the one contained in Article 1 of the Council Framework Decision 2002/475/JHA on Combating Terrorism.

The storage of non-extracted data for 5 years is not supported by evidence that this period is to be considered proportionate. Furthermore, the agreement does not clarify for how long extracted data will be stored. It does not provide either for mechanisms ensuring that both extracted and non-extracted data are deleted as soon as they are no longer necessary for a specific terrorist investigation.

Furthermore, sharing of personal data with other national authorities as well as third countries is neither clearly defined nor subject to appropriate guarantees, as both Convention 108 and Framework Decision 2008/977 standards would require.

Rights of persons affected by these measures, accountability and judicial review. The current agreement only addresses the rights of persons affected in its Article 11(1), which refers to the right of having confirmation by the data protection authority "*whether all necessary verifications have taken place within the European Union to ensure that his or her data protection rights have been respected in compliance with this agreement*". Furthermore, Article 11(3) states that effective judicial and administrative redress for possible breaches of the agreement will be available in accordance with the laws of the European Union, its Member States and the United States.

These provisions raise various issues. First of all, Article 11(1) limits the verifications on whether data protection rights have been respected to the European Union and does not provide for similarly guarantees for the United States, where the most delicate part of the processing of European data will take place. Secondly, the same provision allows for possible restrictions to the possibility for data protection authorities to carry out these verifications, with a provision which has no precedent and the logic of which is difficult to understand. Thirdly, and more importantly, many data subjects rights - as for example rectification, information, compensation for unlawful processing, redress - are either disregarded or have no concrete and clear way to be enforced, apart from the very general reference of Article 11(3) to the respective laws of the contracting parties.

In this respect, the EDPS stresses that Article 8 of the Charter of Fundamental Rights clearly states that "*everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified*" and that "*compliance with these rules shall be subject to control by an independent authority*".

Against this background, the joint review laid down by Article 10 cannot be considered as a substitute to the independent supervision required by the EU legal framework.

Furthermore, Article 10(2) sets limits for the number of participating representatives only in the case of data protection authorities.

Article 16 TFEU as a legal basis and the approach to a possible future agreement. The EDPS regrets that, in the latest draft Council decision on the conclusion of the interim agreement (5305/1/10 REV 1 of 21 January), the reference to Article 16 TFEU as one of the relevant legal bases was deleted.

In this respect, the EDPS strongly believes that since this agreement mainly relates to the exchange of personal data, Article 16 is not less relevant as legal basis than the other TFEU provisions relating to law enforcement cooperation. The importance of Article 16 TFEU - which was stressed also by Mrs Reding in her audition before your Committee - is here evident in order to avoid that the international agreement limps on the law enforcement leg.

In the same line, the EDPS welcomes that the current agreement is concluded for a limited duration and clearly states that it will not constitute a precedent. A new agreement will fully be negotiated under this new legal framework and will therefore need a fresh look, which shall comprehensively address all elements required by EU standards of protection of fundamental rights and fully benefit from the new role of the European Parliament in this area. Some issues which have not been properly addressed because of the pressing need to strike a provisional agreement will have to be carefully addressed in the new one.

Conclusion. In conclusion, as to the TFTP agreement, the EDPS considers that not enough elements have been provided so far to justify the necessity and the proportionality of such a privacy-intrusive agreement, which in many aspects overlaps with already existing EU and international instruments in this area.

Furthermore, some elements of the agreement are not defined in such a clear way as to be foreseeable for the Europeans whose data are transferred to the US. While the agreement addresses some issues raised by European data protection authorities - such as the independent judicial oversight mechanism laid down by the current Article 4 - it does not satisfactorily and systematically provide all the safeguards required by the EU data protection legal framework, leaving some dangerous lacunae that should be carefully addressed in the light of Article 16 TFEU and the new legal framework brought by the Lisbon Treaty.

III. The need for a comprehensive approach to international data-exchange agreements

The EDPS would like to emphasise that these diverse agreements with third countries, and especially the United States, do not provide for a harmonised and coherent framework when it comes to trans-border exchange of information.

In this context, the initiative presently discussed for a transatlantic agreement on law enforcement with the United States deserves specific attention. It remains to be seen how this new horizontal tool would apply to already existing agreements. But such a harmonised framework could certainly enhance legal certainty.

The EDPS would support such an initiative, provided that the level of protection offered by the agreement is sufficiently high and strong implementation measures are foreseen.

Brussels, 25 January 2010