EDPS comments on the Communication COM (2010) 311 final from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports

As a preliminary comment, the EDPS expresses support for the idea of a European approach to security scanners, provided that the necessity test is met, and the best possible safeguards are included. A European approach would contribute to ensure legal certainty and the best and most consistent protection of EU-citizen.

The need for a global picture

The Communication starts by listing the numerous security initiatives which have followed the different attacks or terrorist attempts since 2001. The EDPS fully supports the considerations developed in points 23 and 24 of the Communication, which question "whether adding new security layers after every incident is an effective means to improve aviation security". The need for a more holistic approach, as defined further in the text, has been advocated by the EDPS in a number of his previous opinions in relation to new measures in the field of law enforcement and fight against terrorism. He is therefore looking forward to further developments and to a comprehensive and in depth analysis of the specific needs and possible solutions with regard to airport security, to be assessed in a privacy and data protection perspective.

Security scanners and Best Available Techniques.

The EDPS would like to reiterate the recommendation made in previous opinions[1] regarding the need for the Commission to define and promote together with industry stakeholders Best Available Techniques following the same procedure adopted by the Commission in the environmental field[2]. In the case of security scanners, "Best Available Techniques" would mean the most effective and advanced stage in the development of activities and their methods of operation which indicate the practical suitability of particular techniques for providing, in compliance with the privacy and data protection EU framework, a defined detection threshold. These BATs will be designed to prevent and, where that is not practicable, to mitigate to an appropriate level the security risks related to airport and minimize as much as possible their impact on privacy.

This process is intended to provide reference documents on Best Available Technique which will offer very useful guidance and greater legal certainty for EU airports management organisations and their related security operators. It will also enhance the harmonisation of such measures throughout EU airports. Last but not least, the definition of privacy and security friendly BATs will facilitate the supervisory role of Data Protection Authorities by providing them privacy and data protection compliant technical references adopted by data controllers.

Possibility for opt-out

As it was already underlined in the joint WP29/EDPS consultation paper of February 2009, and in the light of the last paragraph of points 55 and 87 of the Communication, the EDPS would like to stress again that consent should not be used to legitimise a process of personal data if there is no legal basis for that processing. In other words, the legal need to legitimise the use of security scanners should not be transferred on the consumer through a "choice" option. Although choice might be considered at

[1] EDPS opinion on Intelligent Transport systems, July 2009, EDPS opinion on the RFID communication December 2007, EDPS annual Report 2006 p.48-49.

[2] http://eippcb.jrc.es/

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

first sight as a more balanced solution, it puts into question the effective necessity and efficiency of security scanners. It also raises the question of effective choice: if refusing to use a scanner results in longer waiting lines and a presumption that the passenger has something to hide, there is no real consent. The introduction of a legal obligation, subject to certain modalities and conditions, with scope for some individual "choice", where appropriate, would therefore still seem to be unavoidable in the light of Article 8 ECHR and Articles 7-8 EU Charter.

Identifiability of individuals

The application of EU legislation to images captured by security scanners is developed especially in Chapter 5.2 of the Communication. In point 51, the text mentions that "the capture and processing of the image of an identified *or unidentifiable* person (...) falls under EU legislation on data protection". There seems to be confusion here, maybe due to a typo. We believe that the sentence should read *identified or identifiable*, that is, capable of being identified directly or indirectly. If the individual cannot be identified, even indirectly, then data protection legislation will not be applicable. However, this test should be applied in a holistic fashion and taking account of the circumstances of the case (see also recital 26 of Directive 95/46/EC: *"Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller of by any other person to identify the said person; ..."*

On this issue point 56 last indent might be confusing, as it suggests that images analysed by a human reviewer could have no link to the identity of the screened person and would be 100% anonymous. In such a case we believe that even if no direct link with the individual can be made by the reviewer, there is still an indirect possibility of identification, as there is a connection between the reviewer and other agents, which will take a decision regarding the risks posed by the passenger. This is particularly true in an environment where ID documents and personalised travel documents are readily available. There is therefore no complete anonymity, and the scheme should not be presented as guaranteeing such anonymity. However, it remains less intrusive than a direct viewing (and thus a direct identification) and in that sense it should be preferred to direct viewing.