**Data protection in the third pillar: in the aftermath of the ECJ decision on PNR data and the data retention directive**

**Fanny Coudert,**
**Eleni Kosta &**
**Prof. Jos Dumortier**
Interdisciplinary Center for Law & ICT (ICRI) – Katholieke Universiteit Leuven, Belgium
Email: fanny.coudert@law.kuleuven.be, eleni.kosta@law.kuleuven.be

**Abstract**

The European Court of Justice with a recent Judgement[1] annulled the Council Decision[2] concerning the conclusion of an agreement between the European Community and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Bureau of Customs and Border Protection (CBP) and the Commission Decision[3] on the adequate protection of those data. The Court ruled that the "transfer of PNR data to CBP constitutes processing operations concerning public security and the activities of the State in areas of criminal law". Although the data have been initially collected for commercial purposes, the Court found that the actual purpose of their transfer falls outside the scope of protection of the data protection directive[4], which only applies to activities falling under Community Law. The Judgment of the European Court created a substantial legal loophole in the protection of PNR data, raising the general problem of protection of personal data that are not covered by the data protection directive.

A few months before the Judgement, the European Union adopted the data retention directive[5], which creates an obligation for communications and internet service providers to retain traffic and location data for the purpose of the investigation, detection and prosecution of serious crime. The directive does not however deal with the actual use of the retained data after they have been accessed by competent authorities in the field of law enforcement. In the aftermath of the PNR Judgment, the legal basis of the data retention directive has been challenged by the Irish Government who claims that it should have been adopted under the third pillar.

The two aforementioned cases illustrate the tendency that gradually more personal data initially collected within commercial activities are processed for national security and law enforcement purposes. Thus, there is a clear and urgent need for the establishment of a legal framework for data protection in the third pillar. To this direction the Council of the European Union has already drafted a Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, which has not been adopted as of now.

In our paper we will critically analyse this Draft Framework Decision in light of the recent judgement of the ECJ on PNR data and the data retention directive. We will examine whether the

---

[1] Judgment of the Court of Justice in Joined Cases C-317/04 and C-318/04 (30 May 2006)
[2] Council Decision of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (2004/496/EC), Official Journal L 183, p. 83 (20 May 2004)
[3] Commission Decision of 14 May on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection, Official Journal L 235, p. 11–22 (06 July 2004)
[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, p. 31–50 (23 November 1995)
[5] Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L105, pp. 54–63 (15 March 2006)

Decision deploys a data protection framework that takes into consideration the particularities in the area of law enforcement and manages to find the right balance with the right to privacy. Finally, based on the findings of our analysis, we will present in which way the data protection principles laid down in the data protection directive can be implemented for the protection of personal data processed under the third pillar.