

OPINION OF THE  
EUROPOL, EUROJUST, SCHENGEN AND CUSTOMS  
JOINT SUPERVISORY AUTHORITIES

presented to the

HOUSE OF LORDS  
SELECT COMMITTEE ON THE EUROPEAN UNION  
SUB-COMMITTEE F

for their inquiry into EU counter-terrorism activities

Brussels, 28 September 2004

## **I. Introduction**

Sub-Committee F of the House of Lords Select Committee on the European Union is undertaking an inquiry into EU counter-terrorism activities. This opinion has been drafted in response to the Committee's invitation to submit evidence and, specifically, it seeks to answer the following questions, which the Select Committee addressed to the third-pillar joint supervisory authorities:

- Would current data protection arrangements continue to provide an adequate level of protection for the individual if the collection and exchange of data were increased on the scale envisaged? Is there a need for a common EU data protection legal framework for the Third Pillar, as advocated by the Commission?
  
- Should there be common standards for the transfer of personal data from the EU bodies and the Member States to third countries/bodies, including Interpol?

## II. Data Protection under the Third Pillar

- 1 The joint supervisory authorities are those bodies established by the Europol Convention, the Council Decision setting up Eurojust, the Convention implementing the Schengen Agreement and the Convention on the use of Information Technology for Customs Purposes. This opinion should therefore be regarded as the evidence of these four joint supervisory authorities.
- 2 In addition to the right to respect for private and family life guaranteed by Article 8 of the ECHR and reaffirmed by Article 7 of the Charter of Fundamental Rights of the European Union, the new fundamental right to data protection is enshrined in Article 8 of the Charter. The draft Treaty Establishing a Constitution for Europe that includes the Charter, also guarantees in Article I-51 the right to data protection and states that compliance with data protection rules shall be subject to the control of an independent authority.
- 3 The ECHR allows interference with the right to privacy if necessary for the interests referred to in the second paragraph of Article 8 and when justified by those interests; such interference must take account of the principle of proportionality. Article 8 of the Charter of Fundamental Rights expands on this, stipulating that personal data must be processed fairly for specified purposes, and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. This legitimate basis has also to fulfil the conditions of proportionality.
- 4 The 1981 Council of Europe Convention for the Protection of Individuals to Automatic Processing of Personal Data (Convention 108) provides more specific principles for data protection also applicable in the Third Pillar. There is also a Recommendation with specific data protection provisions for the use of personal data in the police sector, which was adopted in 1987 by the Committee of Ministers to Member States regulating the use of personal data in the police sector.<sup>1</sup>

---

<sup>1</sup> Recommendation No. R (87) 15, of 17 September 1987

### III. EU counter-terrorism activities

- 5 The establishment of an area of freedom, security and justice was a new objective set for the European Union by the Treaty of Amsterdam. The Tampere European Council in October 1999 placed this objective as a priority for the Union and set an ambitious agenda. In its assessment of the Tampere programme, the Commission recently reiterated the need to give the fight against terrorism priority status.<sup>2</sup> Although the Tampere programme already included activities to create an area of security, the terrorist atrocities of September 2001 resulted in a period of extensive activities in the field of counter-terrorism activities. The Madrid bombings of March 2004 further accelerated this process.
- 6 Various Council declarations and many initiatives followed. A horizontal assessment of these initiatives reveals three general developments in combating terrorism: closer co-operation, more processing of personal data (particularly the exchange of such data), and attempts to highlight the links between combating terrorism **and** tackling other forms of serious crime. Apart from these EU initiatives, many Member States are in the process of extending the competencies of law enforcement agencies and intelligence services.

---

<sup>2</sup> Communication from the Commission, Com (2004) 401, 2 June 2004.

#### **IV. Data protection and combating terrorism**

- 7 The EU-wide processing of large quantities of personal data, with access for intelligence and law enforcement agencies, is a significant development in the fight against terrorism and serious crime.
- 8 Recent proposals anticipate the processing of personal data from different sources on an unprecedented scale. The proposal to require the retention of communications data, and the recent agreement with the US concerning personal information on airline passengers are both examples of a new trend involving the collection of information on individuals (and not only suspects) with a view to aiding the prevention, investigation, detection and prosecution of crimes and terrorism.
- 9 There is a requirement to assess these developments in the light of the principles of data protection. However, the existing joint supervisory authorities (Europol, Eurojust, Schengen and Customs) have a specific mandate, and there is no existing framework or forum in the Third Pillar with the task of advising and assessing initiatives involving the use of personal data. The Conference of European Data Protection Authorities recently issued a resolution calling on the EU institutions to create an appropriate forum in the Third Pillar to allow for scrutiny of new initiatives involving the use of personal data.
- 10 Apart from an assessment of the necessity of the proposals referred to in paragraph 8, there is the question whether the current data protection arrangements continue to provide an adequate level of protection for the individual. This question covers two different aspects of data protection.
- 11 The first is the impact the different proposals may have on individuals. The fight against terrorism and other serious forms of crime is not an isolated activity of one or two law enforcement agencies; it involves a huge number of agencies throughout the European Union. Personal data are processed and analysed with the latest technology and made available to other authorities whenever considered necessary.

The experience of the Europol Joint Supervisory Body in assessing the agreement between Europol and the United States of America demonstrates that limiting the number of law enforcement authorities allowed to process the exchanged data is difficult. In the United States some 1500 authorities on Federal, State and community level are involved in dealing with criminal offences including terrorism.

- 12 The processing of personal data on the scale proposed (often involving the processing of information on those who are not suspected of any crime) requires adequate legal safeguards such as purpose restriction, with supervision to ensure that there is compliance with legal instruments.
- 13 Convention 108 is perhaps too general in its nature to provide for an adequate set of data protection provisions dealing with the new dimension in processing personal data as set out in the different EU initiatives. Furthermore, there are significant differences in the way this Convention has been implemented by Member States in national law.
- 14 A more specific set of data protection rules for police and intelligence authorities should be developed to enhance the level of data protection. The European Parliament already urged for a binding set of rules. In the recent past initiatives within the Council of the European Union and with the participation of the national Data Protection Authorities to set up a harmonized legal framework failed.  
A new legal framework for the Third Pillar, as advocated by the Commission, could provide for this but only if that legal framework provides for a tailor-made set of rules applicable to law enforcement activities. Simply reaffirming general principles of data protection shall not be sufficient. This legal framework could perhaps further elaborate on the principles set out in the Recommendation of the Committee of Ministers to Member States regulating the use of personal data in the police sector including the results of the three evaluations of that recommendation. Any moves in this direction would, of course, have to take account of the existing legislation (particularly the different national approaches to dealing with data protection in the area of law enforcement), the fundamental right of data protection guaranteed in Article I-51 of the Draft Treaty establishing a Constitution for Europe and the increasing convergence of the First and Third Pillars.

15 The second aspect concerns the supervision of the processing of personal data under the Third Pillar. At present the existing national data protection authorities have different competences in the field of law enforcement. This supervision by independent authorities in the Member States should be organised in a way to ensure that these authorities have a common legal basis as referred to in paragraph 14, equivalent powers, and sufficient funds and capacity.

## **V. Transfer of personal data to third states and bodies**

16 The Europol Convention contains specific rules governing the exchange of personal data to third states or bodies. The basic requirement is that the receiving state or body should have an adequate level of data protection, and that once this has been confirmed a formal agreement should be drawn up. The Protocol to Convention 108 also introduces the adequacy rule but allows derogation if domestic law provides for it because of specific interests of the data subject or legitimate prevailing interests, especially important public interests.<sup>3</sup> Most of the EU Member States have not ratified this Protocol yet.

17 At present there is no uniform Third Pillar instrument regulating the transfer of personal data to third states or bodies. In practice this leads to a situation where Europol cannot transfer data to a particular third state if that state is deemed not to have an adequate level of data protection, but where there is nothing to prevent an EU Member State from doing so by means of a bilateral agreement - there is a need to address this discrepancy.

---

<sup>3</sup> Additional Protocol regarding supervisory bodies and transborder data flows, Strasbourg 8 November 2001