COUNCIL OF THE EUROPEAN UNION

Brussels, 13 April 2012

8596/12

Interinstitutional File: 2012/0010 (COD)

DATAPROTECT 46
JAI 238
DAPIX 54
FREMP 53
COMIX 229
CODEC 939

NOTE

from:	Presidency
to:	Delegations
No. Cion prop.:	5833/12 DATAPROTECT 6 JAI 41 DAPIX 9 FREMP 8 COMIX 59 CODEC 217 7568/12 DATAPROTECT 35 JAI 175 DAPIX 31 FREMP 33 COMIX 167 CODEC 636
Subject:	Proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data - Outcome of CATS discussion

I. General background

1. On 27 November 2008 the Council adopted the Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (hereinafter referred to as 'DPFD')[1]. It entered into force on 19 January 2009. Under Article 29(1) of the Framework Decision, the Member States were required to take measures to comply with it before 27 November 2010. According to Article 29(2), they were required to transmit to the General Secretariat of the Council and to the Commission the text of the provisions transposing into their national law. In accordance with the same provision, the Commission prepared a report using the information submitted by the Member States, which was received by the Council on 27 January 2012.[2]

[1] OJ L 350, 30.12.2008, p. 60.
[2] 5834/12 DATAPROTECT 7 JAI 42 DAPIX 10 FREMP 9 COMIX 60.

2. This report is part of the comprehensive data protection package which was adopted by the Commission on 25 January 2012. This package comprises two legislative proposals, one for a General Data Protection Regulation, which is intended to replace the 1995 Data Protection Directive, and one for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, which is intended to replace the 2008 DPFD.

3. At the CATS meeting of 3 April 2012 a debate took place on two questions surrounding the Commission proposal for a Data Protection Directive on the basis of the Presidency note set out in 5833/12 DATAPROTECT 6 JAI 41 DAPIX 9 FREMP 8 COMIX 59 CODEC 217.

II. The need for a new JHA data protection instrument which covers domestic processing operations

4. By presenting its proposal for a Data Protection Directive, the Commission has made a policy and principle-based choice to present a new data protection instrument with a scope covering also domestic data processing operations. The Commission defended this choice by arguing that that it was not feasible to distinguish domestic from cross-border data processing operations, which would be contrary to the aim to ensure efficiency and legal certainty for data processing in this area.

5. A number of delegations stated their disagreement with the Commission view and stressed the absence of empirical evidence to the effect that the limited scope of the DPFD had resulted in a lack of confidence between Member State authorities hampering their mutual co-operation. The lack of experience with implementation of the DPFD was also invoked by a number of delegations. Several delegations maintained that the subsidiarity principle was not respected by the Commission proposal.

6. One delegation queried whether the scope of the proposed Data Protection Directive was really broader than that of the DPFD, as the former excludes all data processing operations "in the course of an activity which falls outside the scope of Union law", whereas the latter covered all exchange of personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The DPFD's scope covers personal data received from, or made available to, a competent authority of another Member State[1]. Several delegations queried whether Article 16 TFEU provided a sufficient legal basis for covering all domestic data processing operations in the law enforcement/criminal justice area.

7. Other delegations supported the Commission in its choice, as they were of the opinion that the Union cannot put in place an effective data protection regime for police and judicial co-operation in criminal matters if there are not a number of general data protection principles which apply to all, including purely domestic, data processing activities by competent law enforcement authorities. It was also argued that personal data gathered in the context of a national investigation could, at a later stage, possibly be exchanged with, or made available to, other competent authorities of Member States or of third countries. Reference was made also to the fact that the basic EU provisions (Article 8 of the EU Charter of Fundamental Rights and Article 16 TFEU) and sometimes also national law make no distinction between domestic and cross-border co-operations.

8. At the CATS meeting of 3 April 2012, a few delegations had not yet finalised their internal discussions or still had an open mind on the question of scope, pointing also to the need to tackle first the (question of scope in the) draft Data Protection Regulation.

---

[1] Article 1(2) limits the scope of the Framework Decision to the processing of personal data for the purpose of preventing, investigating, detecting or prosecuting criminal offences or executing criminal penalties of data which are or have been transmitted or made available:
- between Member States,
- by Member States to authorities or information systems established on the basis of Title VI of the Treaty on European Union ('Police and judicial cooperation in criminal matters'); or
- to the competent authorities of the Member States by authorities or information systems established on the basis of the Treaty on European Union or the Treaty establishing the European Community.

III. Transfer of personal data to third countries

9. One of the most intensely negotiated articles of the DPFD, Article 13 sets out four cumulative data protection requirements for transfers of personal data to third States or international bodies, including an adequate level of protection for the intended processing, and the requirement that the Member State from which the data were obtained has given its consent to the transfer in compliance with its national law. Article 26 contains a so-called "grandfather clause" for all existing bilateral and/or multilateral agreements of Member States or the Union existing at the time of adoption.[1]

10. The Commission proposal for a Directive would change this system, as the adequacy requirement which under Article 13(1)(d) DPFD is to be assessed by the competent authority of a Member State that is about to transfer the personal data, would under the future Directive be assessed only by the Commission (Article 34). Unlike the DPFD, the Commission proposal for a Directive as mentioned contains no "grandfather clause" for international bilateral and/or multilateral agreements concluded by Member States. Article 60 would oblige Member States to review "international agreements concluded by Member States prior to the entry force of this Directive" in line with the requirements of the Directive, and, where necessary, renegotiate and amend them. The deadline for this is set at five years after the entry into force of the Directive. The Commission specified that this obligation did not apply to EU Agreements, which have the status of EU primary law and apply uniformly throughout the EU. A Directive by its very nature can impose obligations only on Member States.

11. The Commission defended its proposal by arguing that this would facilitate international exchange of data by streamlining the applicable rules and extending the level of data protection. The Commission also played down the concerns expressed in the Presidency note about the ensuing need to renegotiate bilateral agreements. It specified that this would apply only to international data sharing agreements that are not already in compliance with data protection standards. Moreover, general arrangements with a third country such as the so-called EU-US umbrella data protection Agreement, which was currently being negotiated, could obviate the need to renegotiate bilateral agreements with the third country concerned by complementing them with additional data protection safeguards.

---

[1] Recital 38 of DPFD clarifies that future agreements (after the adoption of the DPFD) should comply with the rules on exchanges with third States.

12. Almost all delegations which intervened stated their opposition to a solution that would oblige them to individually renegotiate existing bilateral agreements. This solution was characterised by many as non-realistic. The practical difficulties in having to renegotiate well-functioning and carefully calibrated existing agreements with third partners (which might not be willing to renegotiate them) were adduced as the main reason, together with the general principle of non-retroactivity of new legislation. The impossibility to renegotiate multilateral agreement was also mentioned. The few delegations which were ready to accept the principle of applying the data protection principles of the future Directive to existing bilateral agreements, also expressed concerns about the feasibility of renegotiating those agreements.