COUNCIL OF THE EUROPEAN UNION

Brussels, 26 March 2012

7568/12

Interinstitutional File: 2012/0010 (COD)

LIMITE

DATAPROTECT 35
JAI 175
DAPIX 31
FREMP 33
COMIX 167
CODEC 636

NOTE

from:	Presidency
to:	CATS
No. Cion prop.:	5833/12 DATAPROTECT 6 JAI 41 DAPIX 9 FREMP 8 COMIX 59 CODEC 217
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 - Discussion note

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. The purpose of this Presidency note is to launch a debate in CATS on two questions of a more general and strategic nature surrounding the Commission proposal for a Data Protection Directive.

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 arguments in favour of including domestic processing operations in the scope of a data protection instrument in the framework of police and judicial cooperation in criminal matters are well-known, also at the time of the adoption of the DPFD. One of the main arguments is 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. 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.

5. Article 8 of the EU Charter of Fundamental Rights and Article 16 – of which the latter forms the legal basis for the proposal – of the Treaty on the Functioning of the European Union (TFEU) make no distinction between domestic and cross-border co-operations, but refer to processing activities that fall within the scope of EU law, and the free movement of personal data.[1]

[1] Equally, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No.: 108), and its Additional Protocol (CETS No.: No 181) apply without distinction to the processing of personal data carried out within

6. It is important to keep in mind that the adoption of an EU instrument covering all domestic data processing in the area of justice and home affairs inevitably has a substantial impact on national legislation and practice within the area of criminal procedure. Any investigation and prosecution of a criminal act will involve the processing of personal data. Therefore, any applicable rules on the processing of personal data by the competent authorities will regulate the processing of personal data which forms part of the necessary conditions under which these authorities operate. Indirectly, the harmonisation of such data protection rules will result at least partly in a harmonisation of criminal procedure.

7. At the same time the fundamental right of all individuals to have their personal data protected has to be respected. As highlighted in the recitals of the Council Conclusions of 24-25 February 2011, the European Union is firmly committed to protecting the fundamental rights and freedoms of its citizens as well as protecting their security. Privacy and security are possible and there is no need to choose between being free and being safe and the necessary and appropriate processing of personal data is vital in keeping the public safe. It cannot be forgotten that the activities of the competent authorities in this area involve the processing of highly sensitive personal data on e.g. suspicions of criminal activity and the identity of witnesses.

8. Today, guaranteeing that the fundamental rights – including the right to privacy – of all persons involved in an investigation etc. are respected, form an integral part of each Member State's rules on criminal procedure, police laws etc. These rules are formulated to respect fundamental rights and strike an often delicate balance between many different and sensitive concerns including; preserving the integrity and efficiency of the investigative process, protecting the public, protecting witnesses and ensuring the correct functioning of the national criminal justice system. Any rules on data protection in this area – be they national or EU-wide – must be delimited and formulated in a way that respects this balance.

Member States and when transferred from a Member State to another a Member State or a third country.

9. Section 2.1.1.of the 2012 Commission report on the implementation of the DPFD documents the nexus between data protection and criminal procedure by indicating that in most Member States general data protection legislation applies to the processing of personal data by the police and justice both at national level and in a cross-border context, however often alongside Criminal Procedure Acts and Police (Data) Acts. Of the Member States that replied to the Commission, thirteen Member States (Belgium, Czech Republic, Germany, Estonia, Italy, Luxembourg, Hungary, Malta, the Netherlands, Slovenia, Slovakia, Finland and Sweden) referred to Criminal Procedures Acts or similar legislation, next to the application of their general data protection acts. Seven Member States (Czech Republic, Germany, Hungary, the Netherlands, Slovenia, Finland and Sweden) reported the existence of a specific Police (Data) Act. If the Commission proposal for the Directive were to be adopted, its implementation will in all likelihood also require the amendment of some national criminal procedure acts, and of police legislation.

10. The 2012 Commission implementation report states that "14 Member States indicated that their legislation in force implements the Framework Decision", and 4 "stated that they were still investigating whether there was a need for further implementation measures". Another 9 Member States reported "that implementing legislation still needs to be adopted", and 4 Member States "have either not reacted to the Commission´s request for information (…) or indicated that they have not implemented the Framework Decision"[1]. Irrespective of the state of transposition of the DPFD in Member States' law, it is comprehensible that experience with the rules transposing the DPFD is still limited in some Member States.

11. In light of the above, the Presidency invites delegations to express themselves regarding the scope of the new data protection instrument.

12. Delegations are also invited to point to any specific examples from practice showing that the lack of EU rules on domestic processing of personal data in this area has led to an obstruction of the cooperation between Member States or had detrimental effects for the protection of the rights of individuals.

[1] 5834/12, DATAPROTECT 7 JAI 42 DAPIX 10 FREMP 9 COMIX 60, p. 3.

III. Transfer of personal data to third countries

13. The DPFD's scope is limited to personal data received from, or made available to, a competent authority of another Member State.[1] 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 13 (2) and (3) of the DPFD then provide for derogations from (1), 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.2 The Commission proposal for a Directive seeks to overhaul this system.

14. 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 Commission proposal for the Directive (Article 34) be assessed only by the Commission. This would be done either through an adequacy decision for the particular third country under the General Data Protection Regulation or through a specific decision under the Directive. Under the Directive - in the absence of a Commission decision - the Member States have to assess whether appropriate safeguards exist in the third country, either in a legally binding instrument or on the basis of an assessment of all the circumstances surrounding the data transfer (Article 35). In addition, Article 36 provides for a number of case-based derogations, under which transfer of personal data to third countries are possible

---

[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.

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

in individual cases in the absence of a Commission adequacy decision or appropriate safeguards, including "where the transfer is necessary in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties" (Article 36 (d)). It is no requirement that the Member State from which the data were obtained has given its consent to the transfer in compliance with its national law.

15. The main difference between the DPFD and the Directive therefore appears to be between a system under which the data controller, i.e. the competent authority processing the personal data, assesses the adequacy of the data protection in the third country or, in the absence of such adequacy, makes use of the derogations provided for, and a system where the competence to assess the adequacy is in the hands of the Commission or, in the absence of such adequacy, the competent authority processing the personal data either ensures that appropriate safeguards exist or makes use of the derogations provided for. .

16. 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 renegotiate" international agreements concluded by Member States prior to the entry force of this Directive" , and amend them, where necessary, in order to bring them into line with the requirements of the Directive. The deadline for this is set at five years after the entry into force of the Directive.

17. This clause begs a number of questions: Why are Agreements concluded by the EU excluded from this requirement? How is this rule to be applied regarding multilateral agreements to which many other states are party and in regard to which Member States may not have the option of insisting on a renegotiation? Is it at all realistic that 27 Member States review numerous agreements which provide for the exchange of personal data which are concluded by them with third countries around the world on time?

18. In view of the above, Member States are invited to express themselves on the proposed directive’s approach to international agreements, as well as on the questions outlined in paragraph 17.