COUNCIL OF THE EUROPEAN UNION

Brussels, 31 October 2006

Interinstitutional File: 2005/0202 (CNS)

13918/1/06 REV 1

LIMITE

CRIMORG 150
DROIPEN 64
ENFOPOL 168
DATAPROTECT 39
COMIX 825

NOTE

From :	Presidency
To :	Coreper
No. prev. doc. :	7215/06 JUR 102 CRIMORG 46 DROIPEN 20 ENFOPOL 45 DATAPROTECT 7 COMIX 251 3246/2/06 REV 2 CRIMORG 143 DROIPEN 61 ENFOPOL 161 DATAPROTECT 33 COMIX 780
Subject :	Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters - Question on scope

1. The above Commission Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (DPFD) has been discussed extensively in the Multidisciplinary group on organised crime (MDG) - Mixed Committee. At the MDG meeting on 3-4 October 2006 delegations commenced the second reading. (...) As the discussions of the DPFD have advanced, a solution for the question on scope, which has been discussed by the Article 36 Committee (CATS) at its meetings of 12-13 September and 23 October 2006, has become more urgent.

2. The draft DPFD aims to provide common standards to ensure the protection of individuals with regard to the processing of personal data in the framework of police and judicial co-operation in criminal matters, provided for by Title VI of the Treaty on European Union (Article 1(1)). At first sight, it might therefore seem logical to restrict the scope of the DPFD to the cross-border transmission of information and the processing of data thus transmitted. A number of delegations[1] has expressed doubts against the inclusion of data processed in a purely domestic context. Four delegations[2] have expressed doubts as to whether there was a TEU legal basis to regulate data protection in purely domestic cases. On 9 March 2006, the Council Legal Service delivered an Opinion on whether there was a legal basis for the inclusion of data gathered and used in a purely domestic context in the scope of the draft Framework Decision[3].

3. The Commission proposes that the DPFD applies to the processing of data in the field of Justice and Home Affairs also in a purely domestic context. The Commission approach was supported by a majority of delegations, by the European Parliament in its opinion on the proposal[4] and by the European Data Protection Supervisor (EDPS) [5]. Whilst the Commission proposal is aimed at ensuring data protection in the context of police and judicial co-operation between the Member States, this inevitably must have certain consequences for purely domestic processing of data as well. It is indeed difficult to see how the Union could put in place an effective data protection regime for police and judicial co-operation if there are not a number of general data protection principles which apply to all, including purely domestic, data processing by competent law enforcement authorities.

---

1 CH, CZ, DK, IE, IS, MT, SE and UK.
2 CZ, IE, MT and UK.
3 7215/06 JUR 102 CRIMORG 46 DROIPEN 20 ENFOPOL 45 DATAPROTECT 7 COMIX 251.
4 European Parliament legislative resolution on the proposal for a Council framework decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (COM(2005)0475 - C6-0436/2005 - 2005/0202(CNS)).
5 16050/05 CRIMORG 160 DROIPEN 64 ENFOPOL 185 DATAPROTECT 8 COMIX 864.

Data gathered in the context of an internal investigation could, at a later stage, possibly be exchanged with foreign authorities. From a practical point of view, data which have been gathered in a purely domestic context may be difficult to distinguish from data that have been subject to cross-border transmission. It would seem difficult and at any rate very costly to put in place certain data protection rules solely for the purpose of applying these rules to data which have been received from another Member State.

4. The Presidency is of the opinion that most provisions of the DPFD, that is all chapters except Chapter III, should apply both to domestic and cross-border data processing. Regarding the general data protection principles laid down in Chapter II of the DPFD, which are already contained in all existing international instruments on data protection, it is difficult to see which reason could justify a restriction of their scope to cross-border data processing. In line with the subsidiarity principle, the concrete implementation of these general principles is left to the Member States. Regarding Chapters IV and V, the Presidency is of the opinion that there are no cogent reasons to restrict the scope of the rights of the data subject (Ch. IV) and the confidentiality measures (Ch. V) to data which have been received from another Member State. To do so would seem to make the data protection system unnecessarily complicated and costly.

   The provisions of Chapter VI on judicial remedies and liability hinge upon the provisions of other chapters, so the question of scope does not apply. The same seems to hold true in respect of Chapter VII as the powers of the supervisory authorities are related to the provisions adopted pursuant to the DPFD. (Chapter VIII deals with final provisions.)

   In the view of the Presidency, only the provisions from Chapter III should apply solely in the context of cross-border, for the reasons set out hereafter:

   - Article 9: the obligation to verify data that are transmitted is triggered by the future transmission of these data. The more general data protection requirement of accuracy, which is also applicable in a purely domestic context, is laid down in Article 4(d), and the implementation thereof is left to the Member States[6].

[6] AT thinks Article 9 should also apply to domestic data processing.

- Article 10: the logging and documenting obligation is triggered by the exchange of data. Discussions in the MDG have clearly demonstrated that there is no willingness to have a general logging obligation for all cases where data are accessed[7].

- Articles 11 and 18: it is the clear wish of delegations to have a specific purpose limitation applicable to data received from another Member State

- Article 15: this provision on the exchange of data to third countries, by its very nature, applies solely in the context of cross-border exchange of data, but the question whether it should apply solely to data received from another Member State or to all data is still open.

5. Some delegations[8] have indicated that they cannot accept the principle to apply the provisions of the DPFD (except those of Chapter III) to domestic data processing, as long as the exact nature and extent of the obligations contained in the DPFD is not clear. Concerns that the obligations contained in the current draft of the Framework Decision are far too detailed or do not sufficiently take account of law enforcement concerns have been expressed. Whilst the Presidency would like to reassure delegations that accepting the principle that the DPFD's scope extends to domestic data processing does not imply agreement to the content of the substantive details of the DPFD's provisions, it would at the same time like to emphasise that it is of course impossible to conclude the negotiations on the substance of those provisions as long as it has not been decided whether the these provisions should apply to cross-border data processing only or whether to should extend to domestic data processing. It is moreover unclear to the Presidency why delegations would be able to accept certain provisions in a cross-border context, but not in a domestic context.

6. *Do delegations agree that all provisions from the DPFD, with the exception of Articles 9, 10, 11, 15 and 18, should apply to domestic data processing? Should delegations wish to add other provisions to this list, they are invited to present a justification for those articles.*

---

[7] AT and HU think Article 10 should also apply to domestic data processing.

[8] CH, DK and SE. DE, IT and SK have a scrutiny reservation on the question of scope.