COUNCIL OF THE EUROPEAN UNION

Brussels, 19 September 2006

12924/06

Interinstitutional File: 2005/0202 (CNS)

LIMITE

CRIMORG 138
DROIPEN 58
ENFOPOL 156
DATAPROTECT 31
COMIX 762

NOTE

From :	Presidency
To :	Multidisciplinary Group on Organised Crime
No. prev. doc. :	11547/2/06 REV 2 CRIMORG 124 DROIPEN 44 ENFOPOL 146 DATAPROTECT 26 COMIX 642 12432/06 CRIMORG 135 DROIPEN 54 ENFOPOL 152 DATAPROTECT 30 COMIX 715
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 - Issues paper

Background

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.

   As the MDG is expected to complete the first reading of the entire proposal at its meeting on 21 and 22 September 2006, the Presidency deems it appropriate to discuss some central questions on the draft Framework Decision, before starting the second, article-by-article, reading of it.

As the questions mentioned under 1.2, 1.3. and 1.4. were already discussed at the CATS meeting on 12 September 2006, the Presidency proposes not to discuss them again until other issues have been resolved.

DE, DK, LV, NL, PT and SI have a general scrutiny reservation on the proposal. DK, FR, IE, NL, SE, SI and UK have a parliamentary reservation. AT, ES, FI, IT and SE have a linguistic scrutiny reservation.

1. Scope of the draft Framework Decision?

1.1. Data held by which authorities ?

2. The 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)). Is it therefore necessary to define the authorities with which this cooperation takes place in more detail than is provided for in the current Article 2(j), as these are the authorities that will need to comply with the DPFD?

3. The current text of Article 1(2) states that the DPFD shall apply to "the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data (....) by a competent authority for the purpose of the prevention, investigation, detection or prosecution of criminal offences". There seems to be no valid reason why the DPFD should not apply to law enforcement authorities in the execution of penalties (e.g. various decision-making processes with regard to (conversion of) imprisonment sentences or the enforcement of pecuniary sanctions).
This would necessitate a change in the references to competent authorities (in Articles 1(1) and 2(j), as well as in Article 5(2) and (3)) to include the wording “or the execution of a penalty imposed for a criminal offence”.

Do delegations agree that there is a need to include the execution of penalties in the concept of law enforcement?

1.2. Only international or also domestic processing of data?

4. 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)). This raises the question of whether the scope of the DPFD should be confined to the cross-border transmission of information and the processing of data thus transmitted or whether it should also – as provided for in the Commission's proposal – encompass data gathered and used in a purely domestic context. A number of delegations had previously expressed doubts against the inclusion of data processed in a purely domestic context. One of the reasons put forward were 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[1].

5. Another argument was that the inclusion of purely domestic data would be contrary to the proportionality and the subsidiarity principle. 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. Whilst the Commission proposal is aimed at ensuring data protection in the context of police and judicial co-operation between the Member States, in the Commission's view this inevitably has consequences for the purely domestic processing of data as well. The concrete impact of the Commission proposal on the purely domestic handling of data is primarily based on a number of general data protection principles laid down in Chapter II of the DPFS. The Commission has pointed out that all existing international instruments on data protection already contain these principles. The Commission approach was supported by a majority of delegations and by the European Data Protection Supervisor (EDPS)[2].

---

[1] 7215/06 JUR 102 CRIMORG 46 DROIPEN 20 ENFOPOL 45 DATAPROTECT 7 COMIX 251.

[2] 16050/05 CRIMORG 160 DROIPEN 64 ENFOPOL 185 DATAPROTECT 8 COMIX 864.

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. Data gathered in the context of an internal investigation could, at a later stage, possibly be exchanged with foreign authorities. It was also pointed out that 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.

Do delegations agree that a number of general data protection principles to be provided for in Chapter II of the DPFD should apply to all data processing by competent authorities, including purely domestic data processing?

1.3. Exchange of data with third countries

6. The Commission proposed that the information exchange with third countries which would be subject to the DPFD be limited to data received from other Member States. The Member States' response to this part of the Commission proposal has been very mixed[3]. One may take the view that, if there is agreement on the principle that a number of general data protection principles from Chapter II of the DPFD apply also to purely domestic data processing (see question 2), this should also condition the possibility of transferring data to third countries. Tempting though that view may be from a theoretical point of view, it needs to be adjusted by taking account of the fact that existing bilateral or multilateral agreements between Member States and third countries will not be affected by the DPFD. This necessarily implies that the impact of any DPFD requirements for exchange with third countries is limited to those cases where the exchange takes place in the absence of a treaty basis.

[3] The Commission's view was supported by a limited number of Member States (CZ, CH, ES, NL and PL). Two Member States argued in favour of an extension of the scope of Article 15 to cover all law enforcement data, including purely domestic data: BE and HU. A number of Member States thought that the Framework Decision should not deal with the transfer of data to third countries (DE, DK, IE, IT, NO, SE, SK and UK).

7. This also has important practical consequences for the adequacy requirement, should it be retained in the Framework Decision as a condition for exchange of data with third countries. As most judicial co-operation as well as a significant portion of police information exchange takes place on the basis of an international arrangement of some kind, there are bound to be situations where the exchange of data with a given third State would not be regulated by the DPFD for some Member States (as they already have an agreement with that third State), but would be for other Member States (which did not have an agreement with that third State). The Presidency submits that the Union would find itself in an awkward situation were there to be cases in which the Union found that the data protection level in a given third State to be inadequate, but a number of Member States were nevertheless able (and possibly obliged) to continue to exchange data with the third State by virtue of their bilateral treaty obligations. It therefore does not seem necessary or appropriate to have a 'European' procedure, which would apply only in some cases and only to some Member States. Because of this and in view of the cumbersome nature of the procedure provided for in Article 16, the Presidency proposes to delete the procedure for assessing the adequacy as proposed in Articles 15(4) and 16. It would hence be for each Member State to decide, in cases where there is no pre-existing bilateral treaty with a third State, to assess whether the data protection of that State is adequate.

Do delegations agree with the proposed limitations of the adequacy requirement?

1.4. National Security

8. There seems to be a broad consensus that processing of personal data in connection with national security purposes should be kept outside the scope of the draft Framework Decision, and that this should be expressed clearly in the instrument. HU made a proposal for a new recital (8ter) to clarify this: "This framework decision is without prejudice to essential national security interests, and it should not jeopardise the success of specific intelligence activities in the field of State security".
Some delegations, however, think that this should be clarified in the text of the Framework Decision itself and the UK delegation has made a proposal that a new paragraph 3a be inserted in Article 1, which would read: "For the avoidance of doubt, this Framework Decision does not apply to national security matters".

Delegations are invited to give a preference for either text proposal or for a combination of both.

2. Further processing (and transmission) of data

2.1. Further processing in a domestic context

9. The current draft text of Article 5(3) allows for the further processing of data with regard to a number of purposes set out in that provision. It has been suggested that this provision be supplemented with a text analogous to that of Article 23(1)(b) of the 2000 Mutual Assistance Convention ("for other judicial and administrative proceedings directly related to the proceedings to which this [Framework Decision] applies"). This makes sense as it would be odd to have a more restrictive provision in a domestic context than in the context of international judicial co-operation. Such an addition would also accommodate the concerns voiced by some delegations that allowance should also be made for the transmission to other authorities currently not covered. Examples of such purposes not currently permitted include regulatory proceedings that do not involve a 'right or freedom'; disciplinary action taken by professional bodies; and police functions such as providing emotional and psychological support to victims.

   The goal of including these purposes might be even better achieved by returning to the wording contained in the original Article 4(1)(b) of the Commission proposal: "or lawful purposes not incompatible with the original purposes including the prevention of threats to public security or to a person...". The phrase "not incompatible" was also used in the original Article 13(b) and is also the limit on data processing in Article 6(1)(b) of the Data Protection Directive. The Presidency thinks it would be appropriate to retain that limit here and not to impose a stricter rule in relation to Title VI processing than in the First Pillar.

   Do delegations agree that Article 5(3)(iii) should be supplemented in the way suggested?

2.2. Further processing in an international context

2.2.1. Do delegations agree to apply the same principle for further processing and transmission of data as in a domestic context?

10. The Presidency has inserted a reference to Article 5(3) in Article 11. It deems it consistent to allow for further processing in the receiving Member State of the already transmitted personal data, in conformity with the general rules on the lawfulness of processing of personal data and for the same purposes as in the transmitting Member State. There is no specialty principle in the 2000 Mutual Assistance Convention, nor in the 1959 Mutual Assistance Convention and it would seem odd to subject the transmission of police data to more stringent rules than those for judicial co-operation.

2.2.2. Do delegations agree that there is no need for a prior consent requirement?

11. Should the above proposals on Articles 5(3) and 11 be accepted, it seems that there is no need for a further provision on consent.

3. Rights of the data subject

3.1. Do delegations want to provide data subjects with the right to be informed whether data relating to them are being processed and/or the obligation for law enforcement to inform data subjects thereof?

12. Articles 19 and 20 of the original Commission proposal sought to impose an obligation on Member States to ensure that data subjects would be informed of the fact that (law enforcement) data were being processed with regard to them, so as to enable them to exercise their right to access these data under Article 21. For obvious operational law enforcement reasons, the provisions also provided for exceptions. Many delegations, however, questioned the appropriateness of establishing a principle which in almost all cases would not be applied because of the exceptions thereto. Some delegations therefore pleaded in favour of the deletion of both articles (in the meantime merged into one article). Before engaging in further redrafting of Article 19, it therefore seems necessary to decide whether there is any need to retain the provision.

Do delegations want to retain, in some form or other, an obligation for law enforcement authorities to inform data subjects that data relating to them are being processed?

4. Relationship to other instruments: lex specialis

13. The DPFD intends to put in place a general data protection framework, with a view to both the protection of data subjects and the facilitation of police and judicial co-operation. Article 1(4) explicitly provides that national data protection provisions "higher" than those established in the Framework Decision may not restrict nor prohibit the disclosure of personal data to the competent authorities of other Member States for reasons connected with the protection of personal data as provided for in this Framework Decision. Member States will be under an obligation to bring their national data protection provisions into line with the DPFD.

4.1. Relationship to other EU legislation ((Framework) Decisions)

14. In that perspective, it seems logical to leave no or as few as possible specific data protection regimes in place. Article 1(3) explicitly exempts the Europol, Eurojust and CIS data protection regimes. As far as any other specific EU legislation (mostly Framework Decisions) on data protection is concerned, the rule is that these data protection provisions will normally be superseded by the DPFD. This flows from the fact that the DPFD is a *lex generalis*, which takes precedence over previous *leges specialis*, as this *lex generalis* is also *lex posterior*.
As far as international exchange of data is concerned, however, Articles 11(3) and 17 make allowance for specific legislation under Title VI of the Treaty on European Union under which the competent authority of the 'originating' Member State may require that data be further processed or further transmitted only under specific conditions. Some delegations thought there was no need for this *lex specialis* principle, which is indeed a derogation from the general rule that the DPFD takes precedence. The EDPS is very much in favour of this (para. 29 of doc. 16050/05). Delegations will need to discuss further whether they want to retain more specific data protection regimes. This would mean that more restrictive data protection regimes (e.g. the one in the 'Swedish' Framework Decision) would be retained. Of course this question can be decided only after delegations have agreed whether the speciality principle should be retained in the DPFD.

Relationship to other EC legislation (Directives/Regulations)

As the DPFD is a third-pillar instrument, it will not affect Community legislation , nor provide any protection to persons on whom data are being held by private entities or administrative authorities pursuant to Community legislation (like the Data Protection Directive). Once these data are transmitted to law enforcement authorities (i.e. competent authorities in the sense of the DPFD), the data will however be subject to the DPFD.

Do delegations want to retain more specific data protection regimes contained in other EU instruments?

4.2. Relationship to international conventions

15. As far as data protection provisions in any international conventions, agreements and MOUs between the Member States are concerned, these will be automatically superseded by the DPFD. Articles 33 and 34(1) explicitly state this in respect of the data protection regimes of the Schengen Implementation Convention and of the 2000 Mutual Assistance Convention. Whilst the same principle will apply to all other bilateral or multilateral arrangements between Member States, it does not seem feasible to list the data protection provisions of all these other international arrangements.

Bilateral or multilateral agreements between Member States and third countries, however, will not be affected by the DPFD and Member States will NOT be under an obligation to amend these.

As far as Agreements concluded by the European Union are concerned, the Union would normally be under an obligation to endeavour to amend these conventions, unless the DPFD explicitly states that they will not be affected by the DPFD. The Presidency which submits the DPFD should indeed state so, for the following reasons. Firstly, it could adversely affect the European Union's credibility as a negotiation partner in reneging on arrangements which have been agreed with third countries. This is all the more valid as the few Agreements which have been/will be concluded on the basis of Article 24/38 TEU are of a very recent nature. As regards the PNR agreement which is soon to be signed between the EU and the USA, it should be noted that it will in any case be reviewed in 2007.

Do delegations agree that more specific data protection regimes contained in Article 24-38 Agreements should be safeguarded?
