Fight against terrorism: processing and protection of personal data in the framework of police and judicial cooperation in criminal matters. Framework Decision

2005/0202(CNS) - 04/10/2005 - Document attached to the procedure

COMMISSION?S IMPACT ASSESSMENT

For further information concerning the background to this issue, please refer to the summary of the Commission?s initialproposal 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*.

1- POLICY OPTIONS AND IMPACTS

The Commission considered six policy options.

1.1- Option 1 - No legislative initiative: The option of rejecting any legislative initiative would mean recourse to existing legal instruments, in particular Directive 95/46/EC and the Data Protection Convention of the Council of Europe. However, Directive 95/46/EC does not apply to the processing of personal data in the third pillar. Even the disappearance of the pillar architecture would not automatically result in the application of the Directive. Its Art 3 does not only clearly say that it shall not apply to processing of personal data in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union (TEU). It also explicitly excludes the applicability of the Directive in any case for processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.

1.2- Option 2 - Application of Directive 95/46/EC: This would provide for the applicability of Directive 95/46/EC to data processing for the purpose of preventing and combating crime. This option is very close to the first one. Practically, it means transposing the provisions of the Directive (first pillar instrument) into a Framework Decision (third pillar instrument) without any or only slight modifications. However, most Member States also apply the Directive, irrespective of its Art 3, to data processing for the purpose of preventing and combating crime. However, Member States benefit from wide exceptions provided for by Art 13 of the Directive and thus have considerable discretion.

1.3- Option 3 - Legislative initiative once the modalities for the exchange of information under the principle of availability have been defined: The Commission also considered submitting, as a first step, a proposal defining the modalities of exchanging information under the principle of availability and developing appropriate data protection rules as a second step. In principle, it is possible to firstly determine the right modalities for the various types of information and to subsequently define the necessary supplementary rules for data processing and protection. Such approach stresses that data protection provisions can only be developed in view of a very specific purpose, a specific modality of the exchange of information and of a specific type of information.

On the other hand, this approach holds the risk of achieving agreement on (technical) modalities for the exchange of specific types of information (e.g. DNA, fingerprints) without reaching consensus on sufficient supplementary provisions on data processing and data protection. The right to data protection might be at risk in this case.

1.4- Option 4 - Specific provisions in a legal instrument on the exchange of information under the principle of availability: a set of provisions on data processing and protection to be included in a legal instrument on the exchange of information under the principle of availability. Option 4 could be based on the reasons supporting option 3 while avoiding possible disadvantages. A closer link between provisions defining the modalities of exchanging information under the principle of availability and appropriate provisions on data processing and protection could possibly be established. Both types of provisions would be negotiated and adopted by the Council at the same time. Finally, a well balanced chapter on data processing and protection within a legal act on the exchange of information under the principle of availability could probably foster police and judicial cooperation in criminal matters as well as promote proper respect for fundamental rights. On the other hand, option 4 would mean missing an opportunity to provide for a more coherent and consistent legal regime of the Union for data processing and protection. Such a regime could, in the long term, be based on a legal instrument providing for general rules in the area of data processing and protection.

1.5- Option 5 - Framework Decision on common standards for the processing and protection of personal data in the course of activities provided for by Title VI of the TEU:

The fifth option is a Framework Decision setting out common standards for the processing and protection of personal data in the course of activities provided for by Title VI of the TEU. Contrary to Directive 95/46/EC and the instruments adopted within the Council of Europe, a Framework Decision would provide for a complete system of legally binding provisions applicable to the direct exchange of information in the context of police and judicial cooperation in criminal matters while avoiding the weaker points of options 1 to 4. A framework decision setting out general rules for data processing and data protection would not only confirm the fundamental principles already established for the Community and by the Council of Europe but also provide for legally binding rules for all those questions that the various possible modalities of the exchange of information under the principle of availability have in common: not only principles relating to data quality but also more targeted rules for the criteria making data processing legitimate; obligations of the competent authorities when exchanging personal data; rights of the data subject, role of supervisory authorities, advisory body at EU level. This option would cover not only the principle of availability but more specific forms of police co-operation and exchange of information, such as the second generation of the SIS, the so-called ?SIS II?. However, a framework decision setting up common standards would not exclude the necessity of more specific rules where necessary.

1.6- Option 6 - Legislative initiative involving all existing EU information systems or bodies (Europol, Eurojust): The sixth option is a legislative initiative that aims at harmonising the rules for the processing and protection of personal data exchanged through central information systems and bodies (Europol, Eurojust) established at EU level, as well as for the direct exchange between the Member States. This option is the most far reaching one. It avoids the weakness of options 1 to 5 while providing for a high level of harmonisation and simplification regarding data processing and protection under Title VI of the TEU. In principle, this option is the most preferable with regard to the consistency and

coherence of the Union?s policy on data processing and protection, but, as pointed out for option 5, more specific rules would have to be maintained or be set up, where necessary. Secondly, the option would require a comprehensive legislative package containing not only a framework decision setting up general rules for the processing and protection of personal data that are exchanged directly between the Member States but also modifications of the exchange of information through existing EU information systems or bodies. This would go beyond what seems to be immediately necessary in view of the principle of availability. It would require much more consultations and might be confronted with objections from the bodies concerned.

CONCLUSION: While further harmonisation including all information systems and bodies established at EU level is useful, it is less urgent than the rapid introduction of the principle of availability. The latter can be accompanied by an instrument on data processing and protection, which could then serve as the basis for further harmonisation. Such a two step approach would address the short term necessities as well as, in the long term, further harmonisation of the legislation on data processing and data protection under Title VI TEU. Therefore, the Commission recommends option 5.

IMPACT

Option 5 would provide for targeted rules on data processing and data protection for the exchange of information for the purpose of preventing and combating crime in the course of activities provided by Title VI of the TEU. It can ensure an appropriate data protection regime and avoid the disadvantages of options 1, 2 and 3.

A positive impact can also be expected on the respect of fundamental rights. Appropriate and targeted rules of the data protection regime would ensure that the data subject is generally well protected against unlawful processing of personal data. A comprehensive framework decision can be expected to have a more positive impact on the consistency of the Union?s policy on data protection.

Option 5 would not only cover the exchange of information under the principle of availability but also more specific forms of police co-operation and exchange of information, such as the second generation of the SIS, the so-called ?SIS II?. It could therefore be considered at least as a first step towards a less difficult and more transparent legal regime on data protection under Title VI TEU. Moreover, a framework decision could follow as far as possible the example of Directive 95/46/EC and contribute to a more consistent data protection policy ensuring a high level of data protection in both the first and the third pillar. Option 5 is unlikely to result in considerable additional costs. In general, Member States are likely to adapt their legislation. New bodies or systems are most probably not necessary. An advisory body for data protection issues related to police and judicial cooperation in criminal matters including secretarial services would generate costs for a number of meetings per year.

2- FOLLOW-UP

The proposed option shall be evaluated in accordance with the usual procedures under this Title VI. Member States shall transmit to the General Secretariat of the Council and to the Commission the text of the provisions transposing into their national law the obligations imposed on them under this Framework Decision. On the basis of this information and a written report from the Commission, the Council shall assess before December 2007 the extent to which Member States have taken the measures necessary to comply with this Framework Decision.

Furthermore, a working party shall be established according to the Framework Decision. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission. The European Data Protection Supervisor and the chairpersons of the joint supervisory bodies set up under Title VI of the Treaty on European Union shall be entitled to participate or to be represented in meetings of the Working Party.