Procedure file

Basic information

CNS - Consultation procedure JHA act	2005/0207(CNS)	Procedure lapsed or withdrawn
Fight against crime: general availability of information for Member States' law enforcement authorities and for Europol officers Subject 7.30.05 Police cooperation 7.30.30 Action to combat crime		

Key players

European Parliament	Committee responsible	Rapporteur	Appointed
	LIBE Civil Liberties, Justice and Home Affairs	ALDE PICKART ALVARO Alexander Nuno	22/07/2009
	Former committee responsible		
	LIBE Civil Liberties, Justice and Home Affairs		
Council of the European Union			
European Commission	Commission DG	Commissioner	
	Justice and Consumers	BARROT Jacques	

Key events

12/10/2005	Legislative proposal published	COM(2005)0490	Summary
13/12/2005	Committee referral announced in Parliament		
19/10/2009	Committee referral announced in Parliament		

Technical information

Procedure reference	2005/0207(CNS)
Procedure type	CNS - Consultation procedure
Procedure subtype	Legislation
Legislative instrument	JHA act
Legal basis	Treaty on the European Union (after Amsterdam) M 034-p2b; Treaty on the European Union (after Amsterdam) M 030-p1
Stage reached in procedure	Procedure lapsed or withdrawn
Committee dossier	LIBE/7/00072

Documentation gateway

Legislative proposal		COM(2005)0490	12/10/2005	EC	Summary
Document attached to the procedure		SEC(2005)1270	12/10/2005	EC	Summary
Document attached to the procedure		N6-0057/2006 OJ C 116 17.05.2006, p. 0008-0017	28/03/2006	EDPS	Summary

Additional information

European Commission	EUR-Lex

Fight against crime: general availability of information for Member States' law enforcement authorities and for Europol officers

PURPOSE: to determine the conditions and modalities under which certain types of information, that are available to competent authorities of a Member State, shall be provided to equivalent competent authorities of other Member States and Europol, in order to assist them in the execution of their lawful tasks for the prevention, detection or investigation of criminal offences.

LEGISLATIVE ACT: Council Framework Decision.

CONTENT: The Hague programme invited the Commission to present legislation by the end of 2005 at the latest to implement a "principle of availability". From an analytical perspective, seven main obstacles exist to information to be generally available throughout the EU, that is relevant to make possible, facilitate, or accelerate the prevention, detection or investigation of criminal offences:

-Bi- and multilateral agreements between Member States are either geographically restricted or do not oblige Member States to provide information, making the exchange of data dependent on discretionary factors.

-Current forms of law enforcement cooperation usually require intervention of national units or of central contact points. Direct information exchange between authorities is still the exception.

-No standardised procedure exists yet at EU level to request and obtain information.

-No efficient mechanism exists at EU level to establish whether and where information is available.

-Differences in the conditions to access and exchange information, as well as in distinctions between police, customs and judicial cooperation interfere with an efficient exchange of information.

-Differences in protection standards hinder the exchange of confidential information.

-Absence of common rules to control the lawful use of information that has been obtained from another Member State and few possibilities to trace the source and original purpose of the information.

This Framework Decision obliges Member States to ensure that relevant information, i.e. information able to make possible, facilitate, or accelerate the prevention, detection or investigation of criminal offences, controlled by authorities or by private parties designated for this purpose, is shared with equivalent competent authorities of other Member States if they need the information to carry out their lawful tasks. The information is also to be shared with Europol, insofar as the access to the information by Europol is necessary for the performance of its legitimate tasks, and complies with the Europol Convention and its Protocols. Available information is shared either by online access, or by transfer based on an 'information demand' after matching solicited information with index data that Member States shall provide for information that is not accessible online.

No obligation exists to collect information by means of coercive measures.

Where national law requires that transfer of information requires authorisation from an authority other than the one that controls it, the authority that controls or handles this information (the ?designated authority?) shall obtain this authorisation on behalf of the law enforcement body in the other Member State that needs the information.

Refusal of transfer further to an information demand is limited to grounds fixed by the Framework Decision that, moreover, only apply if less restrictive options have proven to be of no avail. The Framework Decision applies to information exchange prior to the commencement of a prosecution, and does not affect mutual legal assistance mechanisms.

The provisions of the Framework Decision go beyond the exchange of information provided for by the Schengen Convention and constitute a new form of cooperation which did not previously exist. For this reason, this Framework Decision is not a development of the Schengen Acquis.

The Framework Decision seeks to ensure full respect for the right to to protection of personal data and the principles of legality and proportionality of criminal offences and penalties. It does so by authorising only national authorities competent for the investigation of criminal offences to obtain information, and by obliging the authorities involved to verify the necessity and the quality of the information. Furthermore a committee will establish ex ante that information is only available for the equivalent competent authority.

The processing of personal data pursuant to this Framework Decision will be done in accordance with the Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters and the Europol Convention respectively.

FINANCIAL IMPLICATIONS: A committee, composed of the representatives of the Member States and chaired by a representative of the Commission, shall assist the Commission in order to determine the equivalence between competent authorities of the Member States and to develop, where necessary, technical details of the exchange of information. This Committee will probably meet regularly, estimated three times a year, whenever necessary. One participant per Member State will have to be reimbursed.

Period of application: starting 2006.

Overall financial impact of human resources and other administrative expenditure: total EUR 2,172 million (EUR 0.362 million per year for six years.)

Total staff: 1.75

Overall financial impact of human resources: EUR 189,000 per year

Other administrative expenditure deriving from the action: EUR 55.000 per year.

Fight against crime: general availability of information for Member States' law enforcement authorities and for Europol officers

COMMISSION?S IMPACT ASSESSMENT

For further information regarding the context of this issue, please refer to the summary of the Commission?s initial proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM(2005)0490).

1- POLICY OPTIONS AND IMPACTSThe Commission?s impact assessment examined the following four policy options.

1.1- Option 1 - No legislative initiative:the first option departs from the situation where the principle of availability would not be established or no additional legislation would be considered. However, the following developments in the current situation which have potential to contribute towards the political objectives should be noted:

- Establishment of the second generation of the Schengen Information System (SIS) with its gateway the SIRENE-bureaux. The information that is exchanged in that context is limited to what is explicitly foreseen in the relevant Acts of the Parliament and Council, or ? in the case of SIRENE - data supporting action on the basis of SIS information. The SIS is presently conceived as a hit/no-hit control system, not to prevent or investigate criminal offences.

- Some Member States are in the process of setting up direct online access to certain national databases (Schengen II, Schengen III). These multilateral processes are taking place outside the mechanisms and cooperation structures foreseen in the Union treaties, and disregard the European dimension of law enforcement and security issues, and the interdependence of law enforcement authorities. This approach risks jeopardising the solidarity of EU Member States.

- The legislative revision of the fundamental rules on law enforcement information exchange laid down in Arts 39 and 46 of the Schengen Convention working rules will lead to significantly improved conditions and infrastructures for law enforcement cooperation and information exchange. The situation will be improved inter alia by speeding up response times. However, it contains a number of new limitations that curb its applicability, and does neither eliminate the unpredictability inherent to such conditions nor the differentiated treatment between national and non-national requests for information.

- Bilateral agreements will continue to determine the information exchange landscape in order to respond to the specific needs that are not catered for by common agreement or covered in the context of a general legal framework.

1.2- Option 2 - Access to information based on the principle of equivalence: at present, law enforcement authorities can search databases that are nationally accessible. However, accessing information held by law enforcement services from other Member States poses challenges that make it inaccessible in practice. A ?right of equivalent access? would make this information practically accessible to competent law enforcement authorities in the Member States under the condition of respecting the rules that apply in the requested country. This right would imply a correspondent obligation for the requested Member State to provide information to the law enforcement authorities of another Member State that are entitled to obtain it under the law of the former.

1.3- Option 3 - Mutual recognition mitigated by a condition of equivalent access in conjunction with a mechanism to appraise the equivalence of the authorities that are competent to obtain information: the problem arising from the application of a right of equivalent access is that the conditions to meet can be different in the Member States, which hinders the full deployment of the law enforcement potential of the Union. Harmonisation would be a means to address this discrepancy.

However, the Commission does not have the intention and has not been invited to bring about such harmonisation. For that reason, mutual recognition of the competencies of the authorities in one Member State to obtain information under their national law is the best means of facilitating the information flow. Mutual recognition implies a corresponding obligation for the requested Member State to provide information to the law enforcement authorities of another Member State that are entitled to obtain it under the law of the latter. Mutual recognition constitutes a higher level of cooperation, because of the trust and confidence that is necessary to operate the law enforcement mechanism. However, because of the diversity in legal traditions and organisational idiosyncrasies in the Member States, the straightforward application of mutual recognition will inevitably run into questions of asymmetry of competencies.

1.4- Option 4 - Mutual recognition mitigated by a condition of equivalent access in conjunction with a mechanism to appraise the equivalence of the authorities that are competent to obtain information, and an index system to identify the information that is not available online: Option 4 actually consists of option 3 plus an additional obligation: the obligation to provide information is complemented with the obligation to know and to show which information exists within a Member State to qualify for exchange under the principle of availability. To supply each other with knowledge about available information, it is proposed that infrastructures are set up by Member States to 1) grant each other direct access to pre-determined, selected databases, allowing for direct consultation of available information and 2) if information cannot or may not be made available online, to establish an obligation to provide an index system of information that is not available online. Online consultation of these

indexes will tell other Member States whether solicited information is available. To be able to comply with this obligation, technical implementation is necessary in order agree on and elaborate technical architecture support. This technical support should be adapted to the nature of the data, the type of access (online or via indexation), and to the level of political ambition vis-à-vis its exchange.

CONCLUSION: As no fundamental rights would benefit from inaction, option 1 must therefore be rejected. Between the three other options, option 4 which allows access to information based on mutual recognition mitigated by a condition of equivalent access in conjunction with a mechanism to appraise the equivalence of the authorities that are competent to obtain information, and an index system to identify the information that is not available online, is the most effective from the point of view of securing the right to life and physical integrity (please refer to CNS/2005/0202).

IMPACT

With regard to the impact on fundamental rights affected by public security, and data protection in particular, the three options (2, 3 and 4) are equivalent. The implementation of equivalent access or mutual recognition would be accompanied by the establishment of common standards on data protection specially adapted to the exchange of information for the purpose of preventing and combating crime. They would constitute a robust and comprehensive system ensuring that the data subject is generally well protected against unlawful processing of personal data.

In spite of the fact that it is an expensive one, option 4 is expected to achieve a far higher level of security. And, as public security and financial costs are not on an equal footing and the rights to life and personal integrity have such weight, important costs should not serve to discourage the implementation of a system if it can be proven to be efficient. An estimation of the cost will be done when the Council decision on how data should be interchanged ? either via direct access or via an indexation system ? is taken.

2- FOLLOW-UP

With regard to the implementation of the proposed option, i.e. a Framework Decision on exchange of information under the principle of availability by Member States, it shall be evaluated in accordance with the usual procedures under Title VI of the Treaty on European Union. 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 before December 2008 assess the extent to which Member States have taken the measures necessary to comply with this Framework Decision, and take all measures necessary to ensure its full application.

Fight against crime: general availability of information for Member States' law enforcement authorities and for Europol officers

This document consists of the European Data Protection Supervisor?s (EDPS) opinion on the proposal for a Council Framework Decision on the exchange of information under the principle of availability.

The EDPS will be available for further consultation at a later stage, following relevant developments in the legislative process on this proposal as well as on other related proposals.

According to the EDPS, the principle of availability should be implemented into a binding legal instrument by way of a more cautious, gradual approach which involves one type of data and to monitor to what extent the principle of availability can effectively support law enforcement, as well as the specific risks for the protection of personal data. This more cautious approach could include starting with the implementation of the availability principle only by way of indirect access, via index data. Based on these experiences, the system could possibly be extended to other types of data and/or modified in order to be more effective.

The EDPS makes the following recommendations aiming to modify the present proposal:

1) clarifying the scope of the principle of availability as follows: adding a clear and precise definition of the data that will be considered available; limiting the scope of the principle of availability to information controlled by competent authorities; in case of a broader scope, ensuring sufficient safeguards for the protection of personal data;

2) direct access to databases by a competent authority of another Member State: the issue has to be properly addressed since, in case of direct access, the designated authorities of the originating Member State have no control over the access and the further use of the data; the proposal may not promote an unconditional interconnection of databases and thus a network of databases which will be hard to supervise;

3) establishment of a system of index data: the proposal should provide for adequate rules, at least on the creation of index data, on the management of the filing systems of index data and on the adequate

organisation of the access to the index data; the definition of index data needs to be clarified; the proposal should clarify the role of national contact points as regards index data; the basic rules for the creation of index data should be included in the Framework Decision itself and not left to implementing legislation in accordance with the comitology-procedure.

4) exchanges of DNA data: clearly limit and define the type of DNA information which may be exchanged (also with regard to the fundamental difference between DNA samples and DNA profiles); set up common technical standards aimed at avoiding that variations in practices on forensic DNA databases in Member States could lead to difficulties and inaccurate results when data are exchanged; provide for appropriate legally binding safeguards aimed at preventing that the developments of science

would result in obtaining from DNA profiles personal data which are not only sensitive, but also unnecessary for the purpose for which they were collected; only be adopted after an impact assessment.

5) limiting the information exchange with Europol to the purposes of Europol itself, as mentioned in Article 2 of the Europol Convention and the Annex thereof.