

EU: Survey on police powers to exchange personal data across member states

- **most police forces in member states have extensive powers to "autonomously" access and exchange data on individuals**
 - **no data protection provision on individuals rights in draft Framework Decision**
-

Responses to a survey by 22 EU member states (including Norway, Iceland and Switzerland who take part in the Schengen *acquis*), show that most police forces can access and exchange personal data with agencies in other member states without a judicial authorisation. The survey covers police forces but would apply to all law enforcement agencies (ie: immigration and customs) under the *"Draft Framework Decision on simplifying the exchange of information and intelligence between law enforcement agencies of the member states of the European Union, in particular as regards serious offences including terrorist acts."*

An essential criteria in the gathering and exchange of data on an individual requested by an agency in another EU state is whether a judicial decision or authority is required or whether the agencies are *self-regulating* (that is, not subject to any external authorisation).

The responses to the first general question looks at two stages: "pre-investigations" (ie, prior to establishing concrete evidence that a crime has or is about to be committed) and where an investigation is underway in the requesting state. In most EU states the police can access information "autonomously". In both categories only eleven out of 22 police forces would require "authorisation of a judicial authority" to get access to information in the pre-investigation stage and in only nine would this be a requirement if the information was not held and had to be obtained.

The second question lists 47 categories of information and intelligence and asks whether police can access these categories "autonomously" or whether they *"can access but only with the authorisation of a judicial authority"* or *"cannot obtain without a decision of the judicial authority to use coercive measures"*.

Most police forces can access information and intelligence "autonomously" in many of the 47 categories. The categories include basic information which it might be expected that police forces would hold or get access to, for example, people convicted of an offence, wanted and missing persons, stolen vehicles and goods and firearms. Nearly all of the 19 police forces can access and exchange "autonomously" information on people suspected of a "concrete" crime and those "suspected" of criminal activity (who are under surveillance). Only

Switzerland would need to get authorisation to hand over fingerprints, only Portugal, Switzerland and Belgium for DNA, only Luxembourg and Poland for driving licence and passport details, only Luxembourg, Netherlands and Latvia for permits details and fingerprints of foreign nationals, and only Luxembourg for passport data.

There are some categories which many forces can "autonomously" access and exchange data which might come as a surprise. Seventeen police forces can "autonomously" access "*transport companies' passenger lists*" only five have to get authorisation. Fifteen police forces can "autonomously" accessing "*observation reports*" (surveillance and background checks and interviews). Fifteen forces can "autonomously" accessing statements by "*undercover agents*". And fourteen police forces can "autonomously" access and pass over information on the documented questioning of suspects and witnesses without the need for authorisation.

It is on more intrusive forms of intervention or surveillance that a real divide in the powers of access emerges. When it comes to "autonomously" accessing the "*the documentation of telephone tapping*" nine police forces can do this without authorisation (Denmark, Estonia, France, Finland, Lithuania, Poland, Slovakia, Sweden and Norway) - everywhere else judicial authorisation is required. For "autonomously" accessing and exchanging the "*documentation of room bugging*" nine police forces can do this without external authorisation (Denmark, Estonia, France, Finland, Lithuania, Poland, Slovakia, Slovenia and the UK).

Five police forces can "autonomously" access and exchange real-time "*telecommunications monitoring*" interception products (Estonia, Poland, Slovakia, Sweden and UK) - sixteen police forces cannot obtain this information without a decision of a judicial authority. Four police forces can "autonomously" access the "*storage and production of telecom traffic (communication data) generated by various information technology systems and handled by telecom operators and Internet Service Providers*" (Estonia, Latvia, Hungary and Sweden). These figures are interesting in the context of the proposal for the mandatory retention of telecommunications data currently being discussed in the Justice and Home Affairs Council's working parties because in 16 states judicial authorisation is required.

Details of "*unusual or suspicious (money) transactions*" can be "autonomously" accessed in nine police forces. Personal financial information like bank statements, insurance policies and credit cards can be "autonomously" accessed in six states (Estonia, Finland, France, Lithuania, Hungary and Poland).

Draft Framework Decision

On the initiative of Sweden a "Draft Framework Decision on simplifying the exchange of information and intelligence between law enforcement agencies of the member states of the European Union, in particular as regards serious offences including terrorist acts" is being discussed in the Council's Multidisciplinary Group on Organised Crime. Its objective is the exchanging of *"existing information and intelligence for the purpose of conducting crime investigations or crime intelligence operations"*. There is no "obligation" on the requested member state to "gather" information to meet the request and the information and intelligence passed over can only be used in evidence in court with the "consent" of the originating member state (Article 1). The threshold for making a request is for offences which could bring a custodial sentence at at least 12 months, which embraces many, many offences (Article 3).

Article 4a lists 37 offences to which the Framework Decision would apply. These include infringing traffic regulations, infringement of intellectual property rights, and public order - threats of acts of violence at international events such as meetings of the European Council (the 25 prime ministers).

Article 9 is entitled "Data Protection" contains no mention at all of the individual's rights (eg: the right to be informed that data from police and other sources has been given to an agency in another EU state or the right to see and correct the information).

The UK Information Commissioner, in a submission to the House of Commons Select Committee on European Scrutiny, questioned whether infringing traffic regulations and the infringement of intellectual property rights: "really fall within the area of serious crime". The Commissioner also said: "personal data obtained in the course of one set of proceedings cannot necessarily be used in another set of proceedings".

The role of judicial authorities in authorising access to certain categories of information by police forces has not been resolved. A Note from the Netherlands Presidency said in November 2004:

"The practical problems that the proposal tries to tackle, can be illustrated as follows. If one takes the example of a secret telephone number that is found on a "red list", police authorities in some Member States do not have access to such lists, but have to make requests to a judicial authority. If the request comes from a foreign police authority, it seems that the practice is to ask the foreign police authority for a letter rogatory. It may also be that the law of the requested State provides that information may not be provided unless the request has been made by a (foreign) judicial authority (in the context of a criminal investigation or proceedings). It is then that the question arises that a judicial authority in the requesting

State may not be involved in the criminal investigation since the intelligence and information gathering is at such an early stage that the judicial authorities are not, under the law of the requesting State, involved in the pre-investigation phase and therefore the requesting State's police authorities cannot legally obtain a letter rogatory. The situation may also be such that the pre-investigation phase may be held up while awaiting an answer to the letter rogatory.

It would seem to the Presidency that here rules for judicial cooperation to some extent interfere with rules for police cooperation. The reason would be that when the information is of a particularly sensitive nature ("red list" telephone numbers, DNA evidence, holders of bank accounts, criminal records, tax information, etc), the legislation in at least some Member States

seem to require that a judicial authorisation be sought. When a request for such information comes from abroad, a letter rogatory is asked for since the type of information is considered to be "judicial".

A report from the Luxembourg Presidency of the Council, dated 28 January 2005, says that there is "a major problem" with the proposal because in some member states data is "freely accessible" to police forces while "it is not in others". In the former data is directly accessible and can be exchanged under rules on police cooperation, while in the latter the legal system lays down judicial authorisation at different stages of police work (ie: between a "criminal intelligence operation" which has not reached the stage of establishing whether a concrete criminal act has been or may be committed and a "crime investigation" regarding a concrete criminal act).

It is clear from the survey that when it comes to "special investigative techniques" (such a phone-tapping, the bugging or rooms or the interception of communications) many member states currently require authorisation from a judicial authority.

How current police and judicial powers in member states can be squared with the "Hague Programme" (adopted on 5 November 2004) is not at all clear. It says that there should be "common standards of access to data" and that this should be exchangeable between member states under the so-called "principle of availability" - which suggests there may be an attempt to lower the standards of authorisation.

Tony Bunyan, Statewatch editor, comments:

"It is crucial that the powers of law enforcement agencies to exchange information and intelligence are subject to external control and authorisation. The alternative is that "self-regulation" - with all the dangers of abuse and misuse - will become the norm.

Equally, it cannot be right that information collected for one purpose by the requested state can be used, amended and added to by the requesting state for a different purpose and without individuals having the right to correct or amend it."

Sources

- 1. Replies to questionnaire on Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the EU, in particular as regards serious offences including terrorist acts** (doc no 5815/1/05, 2.2.05, pdf)
- 2. Draft Framework Decision on simplifying the exchange of information and intelligence between law enforcement agencies of the member states of the European Union, in particular as regards serious offences including terrorist acts** (doc no: 13869/04, 4.11.04, pdf)
- 3. Note from Presidency to the Article 36 Committee** (doc no: 13867, 4.11.04, pdf)

[Statewatch News online](#) | [Join Statewatch news e-mail list](#) | [Search Statewatch database](#)

Statewatch does not have a corporate view, nor does it seek to create one, the views expressed are those of the author. Statewatch is not responsible for the content of external websites and inclusion of a link does not constitute an endorsement.

13869/04

LIMITE

**CRIMORG 116
ENFOPOL 152
COMIX 658
ENFOCUSTOM 75**

OUTCOME OF PROCEEDINGS

of : Multidisciplinary Group on Organised Crime

on : 21-22 October 2004

No. prev. doc. : 10215/04 CRIMORG 46 ENFOPOL 69 ENFOCUSTOM 49 COMIX 382 +
ADD1 + COR1 (en) + COR2 (es) + COR3 + ADD1 COR1 + ADD1 REV1 (en)
11725/04 CRIMORG 67 ENFOPOL 104 ENFOCUSTOM 52 COMIX 489
13178/04 CRIMORG 94 ENFOPOL 130 COMIX 596 ENFOCUSTOM 65

Subject : Draft Framework Decision on simplifying the exchange of information and
intelligence between law enforcement authorities of the member States of the
European Union, in particular as regards serious offences including terrorist acts.

On 21 October 2004, the MDG discussed the above mentioned Framework Decision on the basis of document 13178/04 CRIMORG 94 ENFOPOL 130 COMIX 596 ENFOCUSTOM 65.

The following delegations have entered a general scrutiny reservations: AT, CY, DE, DK, GR, FI, IT, PL, COM. Parliamentary reservations have been laid down by: FR, UK, IRL, DK.

The discussion in the MDG focused on the precise areas of law enforcement cooperation that will be covered and in particular the delineation between law enforcement cooperation and judicial cooperation. A number of delegations (AT, CZ, DE and FR) argued against the inclusion of cooperation with judicial authorities within the scope of the draft Framework decision. The Swedish delegation explained that, in its opinion, it was necessary to maintain judicial authorities within the scope of the draft instrument in order to attain the main aim of making bilateral exchange of

information more fluid. Otherwise, important pieces of information, which in some Member States are accessible pursuant to a judicial authorisation only, would be excluded. The Swedish delegation also reminded the Group that it was for every Member State to determine which authorities, police or judicial, can access information. A separate paper on this issue is found in doc 13867/04 CRIMORG 115 CATS 47.

The detailed comments made by delegations at last and previous meetings are included in the text below. Where appropriate, the Presidency has included suggestions to amend the text, so as to enable delegations to consider them in view of the next meeting of the MDG.

DRAFT FRAMEWORK DECISION

on simplifying the exchange of information and intelligence between law enforcement authorities of the member States of the European Union, in particular as regards serious offences including terrorist acts.

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Articles 30(1) (a) – (b) and 34(2) (b) thereof,

Having regard to the initiative of the Kingdom of Sweden,

Having regard to the Opinion of the European Parliament,

Whereas:

1. One of the Union's core objectives is to provide its citizens with a high level of security within an area of freedom, security and justice;
2. That objective is to be achieved by preventing and combating crime through closer co-operation between law enforcement authorities in the Member States, while respecting the principles and rules relating to human rights, fundamental freedoms and the rule of law on which the Union is founded and which are common to the Member States;
3. Exchange of information and intelligence on crime and criminal activities is the basis for law enforcement co-operation in the Union serving the overall objective of improving the safety of the Union's citizens;

4. The timely access to accurate and up to date information and intelligence is a crucial element for the possibility of law enforcement authorities to successfully detect, prevent and investigate crime or criminal activity, in particular within an area where internal border controls have been abolished. As terrorists and other serious criminals' activities are carried out clandestinely, they need to be controlled, and information relating to suspected terrorists, need to be exchanged in a particularly rapid manner;
5. It is important that the possibilities for law enforcement authorities to obtain information and intelligence concerning serious crime and terrorist acts from other Member States be viewed horizontally and not in terms of differences with regard to types of crime or division of competencies between law enforcement or judicial authorities;
6. Currently, effective and expeditious exchange of information and intelligence between law enforcement authorities is seriously hampered by formal procedures, administrative structures and legal obstacles laid down in Member States' legislation; such a state of affairs is unacceptable to the citizens of the European Union which call for greater security and more efficient law enforcement while protecting human rights;
7. It is necessary for law enforcement authorities to be able to request and obtain information and intelligence from other Member States at different stages of investigation, from a phase of criminal intelligence gathering to a phase of criminal investigation. The Member State's systems are different in that respect, but this Framework Decision does not purport to change these systems. However, it intends, as regards certain types of information and intelligence, to ensure that certain information vital for law enforcement authorities is exchanged in a rapid manner within the Union, so as not to hamper investigations into serious crime and terrorism acts.
8. The absence of a common legal framework for the effective and expeditious exchange of information and intelligence between the law enforcement authorities of the Member States is a deficiency that will have to be remedied; the Council therefore deems it necessary to adopt a legally binding instrument on simplifying the exchange of information and intelligence;

9. The Member States' common interest to fight crime of a cross-border nature must strike the appropriate balance between a fast and efficient law enforcement co-operation and agreed principles and rules on data protection, fundamental freedoms, human rights and individual liberties; the present text achieves that balance;
10. In the declaration on combating terrorism as adopted by the European Council at its meeting on 25 March 2004, the European Council instructs the Council to examine measures regarding simplifying the exchange of information and intelligence between law enforcement authorities of the Member States. The present Framework Decision fulfils that instruction.
11. As regards Iceland and Norway, this Framework Decision constitutes a development of the provisions of the Schengen acquis which falls within the area referred to in Article 1 of Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis¹. The procedures set out in that Agreement have been followed in respect of this Framework Decision.
12. The personal data processed in the context of the implementation of this Framework Decision will be protected in accordance with the principles of the Council of Europe Convention of 28 January 1981 for the protection of individuals with regards to the automatic processing of personal data.
13. This Framework Decision respects the fundamental rights and observes the principles recognised by Article 6 of the Treaty on European Union and reflected by the Charter of Fundamental Rights of the European Union.

¹ OJ L 176, 10.7.1999, p 31.

HAS ADOPTED THE PRESENT DECISION:

TITLE I

SCOPE AND DEFINITIONS

Article 1

Objective and scope

1. The purpose of this Framework Decision is to establish the rules under which Member States' law enforcement authorities effectively and expeditiously can exchange existing information and intelligence for the purpose of conducting crime investigations or crime intelligence operations and in particular as regards serious offences, including terrorist acts. It shall not affect more favourable provisions in national law¹, bilateral or multilateral agreements or arrangements between the Member States or between Member States and third countries and shall be without prejudice to instruments of the European Union on mutual legal assistance or mutual recognition of decisions regarding criminal matters².
2. This Framework decision does not imply any obligation on the part of the Member States to gather and store information and intelligence only for the purpose of providing it to the competent law enforcement authorities of other Member States.
3. This Framework Decision does not imply any obligation on the part of the Member States to provide information and intelligence to be used before a judicial authority as evidence, nor does it give any right to use such information or intelligence for that purpose. Where a Member State has obtained information or intelligence in accordance with this Framework

¹ UK remarked that care should be taken so as to ensure that this could not be construed so as to mean provisions with a lower level of data protection.

² DE, AT considered that the relationship between this instrument and judicial cooperation needed to be clarified.

Decision, and wants to use it as evidence in a criminal proceeding, it has to obtain consent¹ from the Member State that provided the information or intelligence, where necessary through use of instruments regarding judicial cooperation in force between the Member States².

4. This Framework Decision does not imply any obligation to obtain information or intelligence by means of coercive measures³ in the State receiving the request for information or intelligence.⁴

¹ FI considered that the current situation with regard to the use of information or evidence should be maintained. SE, AT were opposed to this idea.

² UK suggested that the last sentence could be replaced by the text of the Schengen Implementing Convention, Article 39:2, and that Article 13:1 could be deleted. Other delegations considered that the relationship between the Framework Decision and Articles 39 and 46 of that Convention needed to be studied further. COM opined that Article 39 is wider than the scope of the current draft Framework decision and should therefore be maintained. The Presidency proposes to deal with this issue by amending the text of Article 13(1) in such a manner that the text of Article 39(2) of the Schengen Implementing Convention is not repealed in its entirety, but only to the extent that the Framework Decision covers areas contemplated in Article 39.

³ Instead of defining coercive measures, the UK suggested to give some examples, for instance "such as body searches, house searches, formal questioning of persons, interception of telecommunications" (see explanatory memorandum). NO thought that this should be left to each country to decide. BE concurred in that, but stated that also the interference in the private life was an important element.

⁴ AT thought that information that had been obtained through use of coercive measures previously should be excluded even if it was available ("existing") in a file. FI, NO and SE opposed to this idea. BE, FR and LU thought that this information can only be exchanged on the basis of a judicial request for mutual assistance. DE has a scrutiny reservation. The Presidency decided to revert to the question whether such information should be excluded from the scope of application, at a later stage.

Article 2

Definitions

For the purposes of this Framework Decision:

- (a) ‘competent law enforcement authority’: a national police, customs or other authority¹, that is authorised by national law to detect, prevent or investigate offences or criminal activities and to exercise authority and take coercive measures in the context of such activities. [A judicial authority is regarded as competent law enforcement authority if the information or intelligence, according to national law, is only held by or accessible to that judicial authority]²;
- (b) ‘crime investigation’: a legal framework within which measures are taken by competent law enforcement or judicial authorities, including public prosecutors, with a view to establishing and identifying facts, suspects and circumstances regarding one or several identified concrete criminal acts;
- (c) ‘criminal intelligence operation’: a legal framework, having not yet reached the stage of a criminal investigation supervised and controlled by judicial authorities including public prosecutors, within which a competent law enforcement authority is entitled by national law to collect, process and analyse information about crime or criminal activities with the view to establishing if concrete criminal acts has been or may be committed;

¹ PL suggested to include FIUs. FR was opposed to this suggestion, as the FIUs were not always involved in the proper investigative phase. Several delegations considered that the reference to "other authorities" was too vague. It was pointed out however that it is only those authorities that are authorised by national law to detect, prevent or investigate offences or criminal activities and to exercise authority and take coercive measures that are covered. Following a suggestion made by one delegation, it was decided that this question be solved through a system of designation to the General Secretariat and the Commission.

² AT, PL, DE, BE and HUN had certain queries about the last sentence. It was however agreed to seek to redraft the sentence with the limited scope indicated in the cover note. AT laid down a scrutiny reservation. The COM suggested to include the meaning of this sentence in another Article.

(d) 'information and intelligence'¹; any type of existing information or data; appraised, processed and analysed or not, that could be used² in a crime investigation or a criminal intelligence operation to detect, prevent or investigate a crime or a criminal activity. Such information or intelligence includes^{3 4}:

- (i) information and intelligence in records or files kept by competent law enforcement authorities,
- (ii) information kept in records or files by other authorities, to which competent law enforcement authorities have access, either directly or indirectly,
- (iii) information on holders, ex-directory and listed respectively, of telephone-, cell-phone, telex-, fax-, e-mail or web-site subscriptions or addresses kept by telecom operators,
- (iv) information on persons and freight kept by transport companies,
- (v) any other information or intelligence or data; appraised, processed and analysed or not, that has been obtained within the framework of a criminal investigation or a criminal intelligence operation or that may be obtained without the use of coercive powers.

Article 3

Offences

Exchange of information and intelligence under this Framework Decision may take place concerning offences punishable by the law of the requesting Member State by a custodial sentence or a detention order for a maximum period of at least 12 months. Member States may agree on a bilateral basis to make the procedures applicable under this Framework Decision applicable on a broader basis.

¹ The COM considered that intelligence and information could not be put on the same footing.

² AT considered the wording too broad and suggested that a criterion on "necessary" or "required" information should be used.

³ DK suggested that the list could be made more precise. FI wondered if the list was needed. AT and CZ had queries about in particular iv and v and considered that they went too far as access to some of the information mentioned would require a judicial authorisation. AT and COM also wanted to exclude criminal records which would become the subject of a specific system.

⁴ BE and UK stated this list could not cover intelligence held by intelligence services.

TITLE II

EXCHANGE OF INFORMATION AND INTELLIGENCE

Article 4

Provision of information and intelligence

1. Member States shall ensure that information and intelligence, held by or accessible without the use of coercive means to competent law enforcement agencies, can be provided to the competent law enforcement authorities of other Member States in accordance with this Framework Decision.
2. Member States shall ensure that conditions not stricter than those applicable at national level for providing and requesting information and intelligence are applied for providing information and intelligence to competent law enforcement authorities of other Member States.
3. Information and intelligence shall be provided on request by a competent law enforcement authority, acting within the limits conferred upon it by national law, conducting a crime investigation or a criminal intelligence operation.

Article 4a

Time limits for provision of information and intelligence

1. Information and intelligence shall be provided without delay and to the furthest possible extent within the timeframe requested. If information or intelligence cannot be provided within the requested timeframe, the competent law enforcement authority having received a request for information or intelligence shall indicate the timeframe within which it can be provided. Such an indication shall be made immediately.

2. Member States shall ensure that they have procedures in place so that they may respond within at most 12 hours¹ to requests for information and intelligence where the requesting State indicates that it is carrying out a crime investigation or a criminal intelligence operation as regards the following offences, as defined by the law of the requesting State:

- participation in a criminal organisation,
- terrorism
- trafficking in human beings,
- sexual exploitation of children and child pornography,
- illicit trafficking in narcotic drugs and psychotropic substances,
- illicit trafficking in weapons, munitions and explosives,
- corruption,
- fraud, including that affecting the financial interests of the European Communities within the meaning of the Convention of 26 July 1995 on the protection of the European Communities' financial interests,
- laundering of the proceeds of crime,
- counterfeiting currency, including of the euro,
- computer-related crime,
- environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties,
- facilitation of unauthorised entry and residence,
- murder, grievous bodily injury,
- illicit trade in human organs and tissue,
- kidnapping, illegal restraint and hostage-taking,
- racism and xenophobia,
- organised or armed robbery,
- illicit trafficking in cultural goods, including antiques and works of art,
- swindling,
- racketeering and extortion,
- counterfeiting and piracy of products,
- forgery of administrative documents and trafficking therein,

¹ Several delegations (LV, IRL, I) suggested that a more flexible time limit could be inserted.

- forgery of means of payment,
- illicit trafficking in hormonal substances and other growth promoters,
- illicit trafficking in nuclear or radioactive materials,
- trafficking in stolen vehicles,
- rape,
- arson,
- crimes within the jurisdiction of the International Criminal Court,
- unlawful seizure of aircraft/ships,
- sabotage,
- conduct, which infringes road traffic regulations, including breaches of regulations pertaining to driving hours and rest periods and regulations on hazardous goods,
- smuggling of goods,
- infringements of intellectual property rights,
- threats and acts of violence against persons and property, in particular violence during sports events or international events such as meetings of The European Council,
- torture

Where the requesting State indicates that it wishes to have the information more rapidly, the requested State shall use its best endeavours to respond quickly to the request.

Article 5

Requests for information and intelligence

1. Information and intelligence may be requested for the purpose of detection, prevention or investigation of an offence or a criminal activity involving the offences referred to in Article 3 where there are reasons to believe that relevant information and intelligence is available in another Member States.
2. The requesting competent law enforcement authority shall refrain from requesting more information or intelligence or setting more narrow timeframes than necessary for the underlying purpose of the request.

3. Requests for information or intelligence shall contain at least the information contained in the Annex to this Framework Decision (*to be prepared*).

Article 6

Categories of persons regarding which information or intelligence may be exchanged

1. Exchange of information and intelligence under this Framework Decision may relate to persons who, in accordance with the national law of the requesting Member State:
 - a) are suspected of having committed or taken part in a offence or a criminal activity involving the offences specified in Article 3, or
 - b) may, according to criminal intelligence or other evidentiary circumstances, commit or take part in an offence or a criminal activity involving the offences specified in Article 3, or
 - c) are not falling under category a) or b), but there are factual reasons to believe that an exchange of information and intelligence, as a necessary part of a criminal investigation or criminal intelligence operation, could assist in detecting, preventing or investigating a crime or a criminal activity involving the offences specified in Article 4a.
2. Exchange of information and intelligence may also take place with a view to identifying persons falling under categories 1 a) – c).

Article 7

Communication channels

1. Exchange of information and intelligence under this Framework Decision may take place via the SIRENE Bureaux or in accordance with Article 4 (4) and 5 (4) of the Convention on the establishment of a European Police Office (the Europol Convention) or in customs matters via the central units as defined in Article 5 (1) of the Convention on mutual assistance and

cooperation between customs administrations or within any other framework established at bilateral or multilateral level among the Member States of the European Union. Any such framework shall be notified to the General Secretariat of the Council within 3 months of the entry in to force of this Framework Decision and subsequently notified to the other Member States. The notification shall be published in the Official Journal

2. Member States may agree, on a case-by-case basis or in general, that other channels may be used for the exchange of information and intelligence under this Framework Decision, for instance through liaison officers or directly between national or local law enforcement authorities.
3. Information or intelligence not exchanged by virtue of Article 4 (4) and 5 (4) of the Europol Convention shall be communicated also with Europol in accordance with the Europol Convention insofar as the exchange refers to an offence or criminal activity within the Europol mandate.

Article 8

Spontaneous exchange of information and intelligence

1. Without prejudice to Article 11 a) – c), the competent law enforcement authorities shall, without being so requested, provide to the competent law enforcement authorities of other Member States concerned information and intelligence in case there are factual reasons to believe that the information and intelligence could assist in the detection, prevention or investigation of offences or a criminal activities involving the offences referred to in Article 4a.
2. The provision of information and intelligence shall be limited to what is deemed relevant and necessary for the successful detection, prevention or investigation of the crime or criminal activity in question.

Article 9

Data protection

1. Each Member State shall ensure that the established rules and standards on data protection provided for when using the communication channels referred to in Article 7(1) are applied also within the procedure on exchange of information and intelligence provided for by this Framework Decision.
2. Each Member State shall ensure that where a communication channel referred to in Article 7(2) is used, the equivalent standards of data protection as referred to in paragraph 1, are applied within the simplified procedure for exchange of information and intelligence provided for by this Framework Decision.
3. Information and intelligence, including personal data, provided under this Framework Decision may be used by the competent law enforcement authorities of the Member State to which it has been provided for the purpose of:
 - a) proceedings to which this Framework Decision applies;
 - b) other law enforcement proceedings directly related to the one referred to under a);
 - c) for preventing an immediate and serious threat to public security;
 - d) for any other purpose including prosecution or administrative proceedings only with the explicit prior consent of the competent law enforcement authority having provided the information or intelligence.

4. When providing information and intelligence in accordance with this Framework Decision, the providing competent law enforcement authority may pursuant to its national law impose conditions on the use of information and intelligence by the receiving competent law enforcement authority. Conditions may also be imposed on reporting the result of the criminal investigation or criminal intelligence operation within which the exchange of information and intelligence has taken place. The receiving competent law enforcement authority shall be bound by such conditions.

Article 10

Confidentiality

The competent law enforcement authorities shall take due account, in each specific case of exchange of information or intelligence, of the requirements of investigation secrecy. To that end the competent law enforcement authorities shall, in accordance with their national law, guarantee the confidentiality of all provided information and intelligence determined as confidential.

Article 11

Reasons to withhold information or intelligence

A competent law enforcement authority may refuse to provide information or intelligence only if there are factual reasons to assume that the provision of the information or intelligence would:

- (a) harm essential national security interests of the requested Member State or;
- (b) jeopardise the success of a current investigation or a criminal intelligence operation or;
- (c) in case the requested information and intelligence is clearly disproportionate or irrelevant with regard to the purposes for which it has been requested.

TITLE III

FINAL PROVISIONS

Article 12

Implementation

1. Member States shall take the necessary measures to comply with the provisions of this Framework Decision 2 years after the entry into force of this Framework Decision.
2. Member States shall transmit to the General Secretariat of the Council and the Commission the text of any provisions transposing into their national laws the obligations imposed on them under this Framework Decision. On the basis of this and other information, the Commission shall, 2 years after the date in paragraph 1., submit a report to the Council on the operation of this Framework Decision. The Council shall no later than 1 year after that date assess the extent to which the Member States have complied with this Framework Decision.

Article 13

Relation to other instruments

1. Article 39, paragraphs 1 and 2 of the Schengen Implementation Convention are hereby repealed to the extent this Framework decision covers matters that are contained therein.
2. Member States may continue to apply bilateral or multilateral agreements or arrangements in force when this Framework Decision is adopted in so far as such agreements or arrangements allow the objectives of this Framework Decision to be extended or enlarged and help to simplify or facilitate further the procedures for exchanging information and intelligence falling within the scope of this Framework Decision.

3. Member States may conclude bilateral or multilateral agreements or arrangements after this Framework Decision has come into force in so far as such agreements or arrangements allow the objectives of this Framework Decision to be extended or enlarged and help to simplify or facilitate further the procedures for exchanging information falling within the scope of this Framework Decision.
4. The agreements and arrangements referred to in paragraphs 2 and 3 may in no case affect relations with Member States which are not parties to them.
5. Member States shall, within three months from the entry into force of this Framework Decision, notify the Council and the Commission of the existing agreements and arrangements referred to in paragraph 2 which they wish to continue applying.
6. Member States shall also notify the Council and the Commission of any new agreement or arrangement as referred to in paragraph 3, within three months of signing it.

Article 14

Entry into force

This Framework Decision shall enter into force on the day after its publication in the Official Journal.

Done at

For the Council
The President

Brussels, 2 February 2005

**5815/1/05
REV 1**

LIMITE

**CRIMORG 7
COMIX 69**

NOTE

From :	General Secretariat
To :	Multidisciplinary Group on Organised Crime
No. prev. doc. :	15654/1/04 REV 1 CRIMORG 146 COMIX 752 + COR 1
Subject :	Replies to questionnaire on Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the member States of the European Union, in particular as regards serious offences including terrorist acts

Delegations will find hereafter a comparative overview of the replies received to the questionnaire set out in doc. 15654/1/04 REV 1 CRIMORG 146. Up to date, 22 replies have been received. In so far as possible, the comments that were provided to the replies have also been reproduced, either in the table of general comments, or as footnotes to the answers to the questions. For the sake of conciseness, some comments have, however, not been reproduced. This is the case for comments that merely explain which authorities are competent under national law to access and/or provide information or comments that explain why a Member State has not filled out the questionnaire with regard to certain types of information. Regarding the latter, this may be because the question is too vague or the reply would vary according to the type of information sought. It may also be the case that the Member State concerned does not have the legal powers to access the information or that the information is classified and cannot be exchanged through police channels (and only through judicial channels). In some Member States the type of information concerned, may not exist (e.g. some Member States do not issue national identity cards) or the information is not recorded in a systematic way (e.g. lack of DNA register).

General comments

BE: The Belgian position hereafter referred to in the table is subject to the following requirements :

- the possibility to exchange information via police cooperation channel shall not prevent Member States to require prior authorisation by judicial authorities to transmit the information to the requesting authority via such channels when this information is under judicial control in the requested State
- the pre-investigation phase shall be defined in precise terms and shall not have a wider definition than the one contained in art. 2 (c) of the proposal. In particular, such a pre-investigation shall always concern a concrete criminal act.

Furthermore, the Belgian position is subject to the discussion which needs to be further developed regarding grounds for refusal to transmit information (art. 11 of the proposal).

CZ: In regard to the first table, the Czech Republic has put into whole line B) and C) as an answer NO. This is, however, not necessarily connected to the problems of distinction between police and judicial cooperation (concerning only the cases when the information is already in the files of the police), but rather to the problems relating to the character of information. For example, phone tapping can be done only with previous approval of judicial authority. However, once this information is already in criminal file it could, theoretically, be given to another states without another (second) approval from judicial authority. It will, however, not be exchanged due to the fact that such information is subject to regime of classified information. In the Czech Republic it is the problem of classified information and protection of personal data (sensitive data), rather than the problem of second approval of judicial authority, in cases when the information is already in the files of the police, which is at the origin of the difficulty to exchange information. Information that is not yet in files of police and has to be acquired with the approval of judicial authority, can be obtained only via mutual assistance.

DK: It should be noted that Denmark has a distinctive criminal legal system in which the head of the police district is not only chief of police but also chief prosecutor in the district court. Each Danish police district has a legal branch, which handles the prosecution of offenders in the district courts and overlooks the work carried out by the regular police force, including the handling and exchange of information. Accordingly, when Denmark in table 2 indicates that the police autonomously may access and exchange an extensive amount of information this does not imply that there is no judicial authority overseeing the handling of such information.

FR: A titre préliminaire, il convient de rappeler qu'en France, l'activité judiciaire de la police est dirigée par l'autorité judiciaire, et que les investigations réalisées dans ce cadre le sont sous le

contrôle du magistrat compétent, conformément aux dispositions des articles 12 et 13 du code de procédure pénale. Ces dispositions font écho à l'article 41 du code de procédure pénale qui dispose que « le procureur de la République procède ou fait procéder à tous les actes nécessaires à la recherche et à la poursuite des infractions pénales », et qu'à cette fin, « il dirige l'activité des officiers et agents de la police judiciaire dans le ressort de son tribunal. »

A cet égard, la proposition de décision-cadre initiée par la Suède est susceptible de se heurter en France à des difficultés majeures en ce qu'elle vise à organiser la communication directe entre services de police en dehors de tout contrôle judiciaire.

Le premier tableau cherche à distinguer les règles applicables à l'échange d'informations d'une part selon la possibilité d'accès à l'information par les services de police, d'autre part selon qu'une enquête judiciaire à caractère pénal est ou non en cours. Cette dichotomie est réductrice, et ne suffit pas à rendre compte des spécificités de l'approche française et de la complexité des questions posées. En effet, au-delà de ce premier critère, il est nécessaire de considérer le type d'information concerné.

1) Situation si aucune enquête judiciaire n'est en cours dans l'Etat requérant

S'agissant de la France, une telle hypothèse est extrêmement marginale puisque l'article 75 du code de procédure pénale dispose que la police judiciaire procède à des enquêtes préliminaires « soit sur les instructions du procureur de la République, soit d'office. »

La notion de « pré-investigations » que met en avant le questionnaire est donc peu pertinente pour rendre compte de la situation que connaît la France s'agissant d'enquêtes judiciaires. Cette étape pré-judiciaire est sans doute plus proche, en ce qui concerne la France, des activités de renseignement, qui ne relèvent pas de l'autorité judiciaire.

En outre, il convient de préciser que si une enquête judiciaire a eu lieu, mais est terminée, les règles de transmission des informations recueillies au cours de la procédure judiciaire sont strictes. En effet, l'article R.156 du code de procédure pénale dispose qu'aucune pièce de la procédure autre que les décisions juridictionnelles (arrêts, jugements, ordonnances) ne peut être délivrée à des tiers sans l'autorisation préalable, selon les cas, du Procureur de la République ou du Procureur Général.

L'accès de la police à une telle information suppose toutefois l'existence d'une procédure judiciaire à caractère pénal. La transmission de telles informations, qui est susceptible de rentrer dans le champ de l'entraide judiciaire en matière pénale, requiert donc l'autorisation de l'autorité judiciaire compétente. Cette remarque vaut pour toutes les réponses où le sigle de la France est indiqué en italiques (*FR*).

La transmission de tels procès verbaux à l'étranger relève incontestablement de l'article 39-2 de la Convention Schengen, et requiert donc une autorisation de la part du magistrat compétent. La

détention d'archives par les forces de police ne les autorise pas à les utiliser dans le cadre d'autres procédures, plus particulièrement avec l'étranger (Convention Schengen Art. 39 - 2.)

LT: According to the national legislation there are two types of investigations. First type of investigation is implemented according to the Law on Operational Activity. Another type of investigation is carried out according to the Criminal Procedure Code. In the latter case, information exchange is executed through the Ministry of Justice or Prosecutors General Office on the basis of rogatory letters. This means that police have no rights to decide what information can be delivered and what cannot. In the first case, it is usually police (or other law enforcement institutions) that decide which data can be provided to the authorities of the requesting countries.

Information exchange always depends on the character of the request of the foreign state, the content of requested information and the legal regulation as well as the concrete situation connected with related investigations that are carried out in Lithuania.

LU: For Luxembourg, as long as the information exchange is requested through a police channel, the status of the investigation in the requesting country is not relevant as we assume that the request is legally possible in the requesting state. The important question for Luxembourg is whether the information request is of a general nature or if it is linked to an ongoing investigation in Luxembourg (requested state) and what is the status of this investigation. If there is an ongoing investigation in Luxembourg and if the information request addressed to the police through a police cooperation channel is linked to this investigation, or if the police owns the information only because of its involvement in an investigation, then the exchange through a police cooperation channel is not possible, or submitted to the prior authorisation of the judicial authorities.

A distinction has to be made with regard to the answers provided by Luxembourg. An unconditional "yes" can be given to information that in every situation is freely accessible to the police (for instance car registration, company register information...). However in a considerable number of situations, the police has "de facto" access to a piece of information as the police was involved in the collecting process (example: witness record...) but as the information was collected during a criminal investigation on request of a judicial authority, the police is not the owner of the information and cannot freely share it.

NL: The replies to question 1 are only partially possible as the distinctions made do not completely correspond to the Dutch procedural system. Regarding question 2, the relevant box has been ticked when the police has access to the information and can exchange it with other Member States. However, this does not mean that police would be able to do so within 12 hours.

SE: The answers are by necessity given as general statements. Please note therefore that the release of a few types of information may be released only if certain conditions are met, for instance that

the investigation or pre-investigation at hand involves an offence on which a certain penalty can be imposed. The release of other types of information may also be preceded by an assessment if the information can be released. However, neither of these two factors will in practice pose any problem as to the transmission of information or intelligence to foreign law enforcement bodies.

CH: The Swiss position referred to in the table has been defined in the understanding that:

- the scope of the proposed Framework Decision shall be restricted to police cooperation;
- the possibility to exchange information through police cooperation shall be without prejudice to the competence of national judicial authorities and the legal instruments on mutual legal assistance;
- the proposed Framework Decision shall not relate to information which is only accessible or has been previously obtained by means of coercive measures;

NO: The Norwegian delegation would first like to point out that in Norway, the (lower) prosecuting authority is integrated into the police. This means that an investigation conducted by the police is always led by a police prosecutor. But since the prosecuting authority is integrated into the police, the police can act autonomously unless a decision of the court to use a coercive measure is necessary. The column/row “can access but only with authorisation of a judicial authority” is therefore irrelevant for the Norwegian answers. We understand column C and the third row to mean decision of the court to use a coercive measure.

Question 1: Do your national legislation and internal procedures allow to exchange the following information under the draft Framework decision?

INFORMATION WHICH THE POLICE IN THE REQUESTED STATE	PRE-INVESTIGATION IN THE REQUESTING STATE		INVESTIGATION IN THE REQUESTING STATE	
	The information has been obtained already in the requested state ¹	The information has not yet been obtained in the requested state	The information has been obtained already in the requested state ²	The information has not yet been obtained in the requested state
A) can access autonomously	BE ³ - CZ- DK- EE- FR- CY- LV- LT- LU- HU- AT- PL- SI- SK- FI - SE- UK- CH- NO-	BE- CZ- FR- LV- LT- LU- HU- AT- PL- SI- SK- FI - SE- UK- CH- NO-	BE-CZ- DK- EE- CY- LV- LT- LU- HU- PL- SI- SK- FI - SE- UK- CH- NO- IS-	CZ- LV- LT- LU- HU- PL- SI- SK- FI - SE- UK- CH- NO-
B) can access but only with authorisation of a judicial authority	BE- FR ⁴ - LV- LT- SI- SK- SE- CH- IS-	DK- FR ⁵ - LT- PL- SI- SE ⁶ - CH-	BE- LV- LT- PL- SI- SK- FI - SE- CH-	DK- LT- PL- SI- SE ⁷ - CH-
C) can not obtain without a decision of the judicial authority to use a coercive measure	BE- FR ⁸ - LV- LT- FI- SE-	DK- LT- PL- SE ⁹ - IS-	BE- LV- LT- SE-	DK- LT- PL- FI- SE ¹⁰ - IS-

¹ This means that the information is already in the files of the police.

² This means that the information is already in the files of the police.

³ BE: Some legal conditions are required (only for judicial police officers,...)

⁴ FR: Cet accès dépend toutefois de la nature de l'information, et du cadre juridique dans lequel elle est collectée. En outre seule l'information peut être transmise, et non pas les pièces qui l'établissent.

⁵ FR: Selon les circonstances: Toutefois, cet accès ne sera pas possible si l'information relève de l'emploi de moyens dont la mise en œuvre obéit à une procédure réglementée par la loi (sonorisation d'un lieu ou écoutes téléphoniques), et qui peuvent parfois être réservées au cadre d'une procédure pénale judiciaire.

⁶ SE: When obtained subsequent to a decision by a judicial authority it can be exchanged through police channels.

⁷ SE: See previous footnote.

⁸ FR: Si la coercition est nécessaire, l'information obtenue et conservée l'est alors dans un cadre judiciaire, il faudra donc l'autorisation de l'autorité judiciaire.

⁹ SE: When obtained subsequent to a decision by a judicial authority it can be exchanged through police channels.

¹⁰ SE: See previous footnote.

Question 2: Where do you place every item of this list of doc. 15187/04 CRIMORG 142?

	The Police can access autonomously	The Police can access but only with authorisation of a judicial authority	The Police can not obtain without a decision of the judicial authority to use a coercive measure
Persons convicted of crime (criminal records)	BE- CZ- DK- EE- CY- LV- LT- HU- AT- PL- SI- SE- UK- CH- NO-	NL- PL- PT- SK- FI - IS-	
Persons suspected of (concrete) crime	BE- CZ- DK- EE- FR- CY- LV- LT- LU- HU- NL- AT- PL- PT- SI- SK- FI - SE- UK- CH- NO- IS	FR- LT-	
Persons suspected of criminal activities (criminal intelligence)	BE- CZ- DK- EE- FR- CY- LV- LT- LU- HU- AT- PL- PT- SI- SK- FI - SE- UK- CH- NO- IS	FR- NL-	
Decisions prohibiting entry to premises or restraining orders	BE ¹ - CZ- DK- CY- LT- LU- HU- AT- PL- PT- SI- FI - SE- UK- CH- NO- IS-	BE- LT- NL-	
Wanted/missing persons	BE- CZ- DK- EE- FR ² - CY- LV- LT- LU- HU- NL- AT- PL- PT- SI- SK- FI - SE- UK- CH- NO- IS		
Photographs	BE- CZ- DK- EE- FR ³ CY- LV- LT- LU- HU- NL- AT- PL- PT- SI- SK- FI - SE- UK- CH- NO- IS	PL- CH ⁴ -	
Fingerprints	BE- CZ- DK- EE- FR- CY- LV- LT- LU- HU- NL- AT- PL- PT- SI- SK- FI- SE- UK- CH- NO- IS		CH-
DNA	CZ- DK- EE- FR- CY- LV- LT- HU- AT- PL- SI- SK-	PT-	BE- CH-

¹ DE: Depends on the type of decision. E.g. : the police can autonomously access decisions forbidding entry to a sport stadium.

² FR: Il convient de distinguer les personnes disparues, à l'égard desquelles il est possible qu'aucune procédure judiciaire ne soit en cours, des personnes recherchées, qui le sont en principe dans le cadre d'une procédure judiciaire

³ FR: L'accès de la police à une telle information suppose toutefois l'existence d'une procédure judiciaire à caractère pénal. La transmission de telles informations, qui est susceptible de rentrer dans le champ de l'entraide judiciaire en matière pénale, requiert donc l'autorisation de l'autorité judiciaire compétente. Cette remarque vaut pour toutes les réponses où le sigle de la France est indiqué en italiques (*FR*).

⁴ CH: If obtained undercover.

	FI - SE- UK- CH- NO- IS		
Identification (distinguishing marks or dental records)	BE- CZ- DK ¹ - FR- LV- LT- HU- NL- AT- PL- PT- SI- SK- FI - SE- UK ² - NO-	CY- PL-	BE ³ - DK- PT- IS-
Modus operandi	BE- CZ- DK- EE- FR- CY- LV- LT- LU- HU- NL- AT- PL- PT- SI- SK- FI - SE- UK- CH- NO-		IS-
Other registers that describe crimes committed or types of crime	BE- CZ- DK- EE- FR- CY- LV- LT- HU- NL- AT- PL- PT- SI- SK- FI - SE- UK- CH- NO- IS		
Stolen vehicles or stolen goods	BE- CZ- DK- EE- FR- CY- LV- LT- LU ⁴ - NL- AT- PL- PT- SI- SK- FI - SE- UK- CH- NO- IS	LU ⁵ -	
Firearms tracing	BE- CZ- DK- EE- FR- CY- LV- LT- HU- AT- PL- PT- SI- SK- FI - SE- UK- CH- NO-	LU-	
Reports (complaints) on crimes committed	BE- CZ- DK- EE- FR- CY- LV- LT- LU- HU- NL- AT- PL- PT- SI- SK- FI - SE- UK- CH- NO- IS	PL-	
Driving licences	BE- CZ- DK- EE- FR- CY- LV- LT- HU- NL- AT- PL- PT- SI- SK- FI - SE- UK- CH- NO- IS	LU- PL-	
Passports	BE- CZ- DK- EE- FR- CY- LV- LT- HU- NL- AT- PL- PT- SI- SK- FI - SE- UK- CH- NO- IS	LU- PL-	
National identity cards	BE- CZ- DK- EE- FR- CY- HU- NL- AT- PL- PT- SI- SK- FI - SE- CH- IS	LU-	
Firearms	BE- CZ- DK- EE- CY- LV- LT- HU- NL- AT- PL- PT- SI- SK- FI - SE- UK- CH- IS	LU-	
Information (held by Prison Administration Services) concerning prison inmates.	BE- CZ- DK- EE- FR- LV- LT- HU- NL ⁶ - PL- PT- SI- FI - SE- UK- CH- NO- IS-	LU- AT- SK-	

¹ DK: Access to dental records held by private dentists may require a court order.

² UK: Dental records may require judicial authority, but may be available to the police autonomously in certain circumstances

³ BE: Some marks have to be collected through the use of coercive measures, but not all.

⁴ LU: Goods.

⁵ LU: Vehicles.

⁶ NL: information limited to whether someone has served a term in prison.

Decisions, permits, fingerprints etc concerning foreign nationals.	BE- CZ- DK- EE- FR- CY- LV ¹ - LT- HU- AT- PL- PT- SI- SK- FI - SE- UK- CH- NO- IS-	LU- NL- LV ²	
Vehicle data and vehicle owner (cars)	BE- CZ- DK- EE- FR- CY- LV- LT- HU- NL- AT- PL- PT- SI- SK- FI - SE- UK- CH- NO- IS	LU-	
Data concerning aircraft and owner of aircraft	CZ- DK- EE- FR- CY- LV- LT- HU- NL- AT- PT- SI- FI - SE- UK- CH- NO- IS-	BE- SK-	BE ³ - LU-
Vessel data and owner of vessel or boat.	CZ- DK ⁴ - EE- FR- CY- LV- LT- HU- NL- AT- PL- PT- SI- FI - SE- UK- CH- NO- IS-	BE- SK-	BE ⁵ - LU-
Customs authorities' information on import and export of goods	CZ- DK- EE- FR- CY- LV- LT- HU- AT- PT- SI- FI - SE- UK- CH- NO- IS-	BE- SK-UK ⁶	LU-
Transport companies' passenger and freight lists.	CZ- EE- <i>FR</i> - CY- LV- LT- HU- AT- PL- PT- SI- FI - SE- UK- CH - NO ⁷ - IS-	BE- NL- SK-	BE ⁸ - DK- LU- CH- NO ⁹ -
Administrative registers on persons (census)	BE- CZ- DK- EE- <i>FR</i> - CY- LV- LT- HU- NL- AT- PL- SI- FI - SE- UK ¹⁰ - NO- IS-	LU- PT- SK-	

¹ LV: The police has in its files the information on persons, groups, entities involved in terrorist offences and subject to refusal to entry the territory of Latvia (these lists are made and updated by the Security Police).

² LV: The police have access to visa information system where the information on issued, refused, annulled and cancelled visas is available, also register of nationals and inhabitants, invitation data base and refusal to entry data base.

³ BE: Depends on the voluntary or not voluntary transmission of information by the person concerned.

⁴ DK: Only vessels are registered in Denmark.

⁵ BE: Depends on the voluntary or not voluntary transmission of information by the person concerned.

⁶ UK: H.M. Customs and Excise are party to a number of treaties which would facilitate exchange of this data with requesting states. In the absence of such a treaty the requesting territory may be required to provide an International Letter of Request.

⁷ NO: On domestic lines.

⁸ BE: Depends on the voluntary or not voluntary transmission of information by the person concerned.

⁹ NO: On international lines.

¹⁰ UK: Access to some census information.

Address and accommodation	BE- CZ- DK- EE- FR- CY- LV- LT- HU- NL- AT- PL- PT- SI- SK- FI - SE- UK ¹ - CH- NO- IS	LU-	
Company board of directors, operations, share capital etc.	BE- CZ- DK- EE- FR- CY- LV- LT- HU- NL- PL- PT- SI- SK- FI - SE- UK- CH- NO- IS-	BE-	BE ² - LU- AT-
Ownership of real property	BE- CZ- DK- EE- FR- CY- LV- LT- HU- NL- AT- PL- PT- SI- FI - SE- UK- CH- NO- IS	SK-	LU-
Income and wealth information	DK- EE- FR- LV- LT- HU ³ - PL- SI- FI - SE- NO- IS	BE- CZ- CY- PL- PT- SK-	LU- AT- PL- PT- UK- CH-
Registered debts such as taxes, maintenance, fines, debts to individual guarantors etc.	DK ⁴ - EE- FR- LV- LT- PL- SI- FI - SE- UK ⁵ - CH- NO ⁶ - IS	BE- CZ- CY- HU- NL- SK- UK-	DK- LU- AT- NO ⁷ -
Observations or observation reports	DK- EE- FR- LT- LV ⁸ - LU- AT- PL- PT- SI ⁹ - FI - SK- SE- UK - NO-	CZ- LT- HU- NL- AT- PL- SK- UK-	BE- SI- IS-
Photographs	BE- DK ¹⁰ - EE- FR- LV- LT- LU ¹¹ - AT- PL- PT-	CZ- LV- LT- HU- NL- PL- SI- SK-	BE ¹³ - DK- LU ¹ - SI- IS-

¹ UK: Via electoral register information.

² BE: The police can autonomously access company information for which official publication is compulsory under Belgian law. For other kind of information, Depends on the voluntary or not voluntary transmission of information by the person concerned.

³ HU: Only taxes.

⁴ DK: Police may not have autonomously access to certain private debt registers.

⁵ UK: Some debt judgements available. Other information may depend on offence under investigation

⁶ NO: Fines.

⁷ NO: Taxes, maintenance, debts to individual guarantors.

⁸ LV: The police has in its files the information on observations or observation reports as far as investigatory operations are concerned, i.e., investigatory observation.

⁹ SI: Observations are carried out by the decision of judicial authorities. The police can access to observation reports autonomously.

¹⁰ DK: Depending on who is the owner of the photograph, film or video recording a court order may be required.

¹¹ LU: Those where the Police is legally entitled to own.

¹² SI: The police can access autonomously to photographs which have been obtained in the frame of observation only while executing this measure. After the execution of observation has been completed, the police can access to photographs obtained through observation only by the permission of judicial authorities. The police can access autonomously to photographed persons records on the grounds of suspicion that a criminal offence has been committed.

¹³ BE: Depends on how the picture is collected (e.g. through the press, through a surveillance measure, ...).

	SI ¹² - FI - SK- SE- UK- NO-	UK-	
Film or video recordings	BE- DK ² - EE- FR- LV- LT- LU- AT- PL- SI ³ - FI - SK- SE- UK- CH- NO-	CZ- LV- LT- HU- NL- PL- SI- SK- UK- CH ⁴	BE ⁵ - DK- LU- SI- CH ⁶ - IS-
Questioning or other records of conversations with persons who cooperate with crime-fighting authorities	CZ- DK- EE- FR- CY- LT ⁷ - AT- PL- SI- FI - SK- SE- UK- CH- NO-	BE- LT- HU- NL- PL- UK-	PT- IS-
Statements provided by under-cover agents	DK- EE- FR- CY- LV- LT- AT- PL- SI ⁸ - SK- FI - SE- UK- CH- NO-	BE- CZ- LT- HU- NL- IS- UK-	PT- SI-
Other compilations that contain appraised or non-appraised information on crime or criminal activities.	CZ- DK- EE- FR- CY- LV- LT- HU- PL- PT- SI- FI - SE- UK- CH- NO-IS	LT-	
Operational analyses	CZ- DK- EE- FR- LV- LT- HU- AT- PL- PT- SI- SK- FI - SE- UK- CH- NO- IS	LT- NL-	
Documented questioning of suspects, witnesses, plaintiffs, experts etc.	CZ- DK- EE- FR- CY- LV- PL- SI- SK- FI - SE- UK- NO- IS	BE- LT- HU- NL- AT- PL- PT- UK-	BE ⁹ - PT- CH-
Documentation of search of premises including search for communication data, seizures, forfeited	DK- EE- FR- LV- SI ¹⁰ - SK- FI - SE- UK- NO-	LT- HU- NL- PL- SI- UK-	BE- CZ- LU- AT- PT- CH- IS-

- ¹ LU: Photographs where the Police is not legally entitled to own
- ² DK: Depending on who is the owner of the photograph, film or video recording a court order may be required.
- ³ SI: The police can access autonomously to video recordings obtained through observations only while executing this measure. After the execution of observation has been completed, the police can access to video recordings obtained in this way only by the permission of judicial authorities.
- ⁴ CH: If obtained undercover.
- ⁵ BE: Depends on how the picture is collected (e.g. through the press, through a surveillance measure, ...).
- ⁶ CH: If obtained from private persons with coercive measures.
- ⁷ LT: If the investigation is carried out according to the Law on Operational Activity, police can access relevant information autonomously. If the investigation is executed according to the Criminal Procedure Code, police can access data only with authorisation of judicial authorities (see general remark by LT).
- ⁸ SI: The measure of under-cover operation is permitted by judicial authorities. The police have autonomous access to statements provided by under-cover agents.
- ⁹ BE: Depends on the voluntary or not voluntary presence of the person concerned.
- ¹⁰ SI: The police have autonomous access to documentation of search of premises including search for communication data and seizures, while the permission of judicial authorities is needed for documentation related to forfeited property or frozen assets.

property or frozen assets			
Documentation of telephone tapping (including so-called surplus information)	DK- EE- <i>FR</i> - LT- PL- SI ¹ - SK- FI - SE- NO-	CZ- LT- HU- NL- PL- SI-	BE- LU- AT- PL- PT- SI- CH- IS-
Documentation of room bugging	DK- EE- <i>FR</i> - LT- PL- SI ² - SK- FI - UK-	CZ- LT- HU- NL- PL- SI- UK-	BE- LU- AT- PL- PT- SI- CH- IS-
Documentation of crime scene investigations	BE- CZ- DK- EE- <i>FR</i> - CY- LV- LT- NL- PL- SI- FI - SE- UK ³ - CH- NO-IS	LT- HU- AT- PL- PT- UK-	BE ⁴ - PT-
Documentation of medico-legal investigations	CZ- DK- EE- <i>FR</i> - LV- NO-	LT- LU- HU- AT- PL- PT- SI- UK ⁵ -	BE- PT- IS-
Holder, ex-directory and listed respectively, of telephone, cell-phone, fax or telex, e-mail or website subscriptions or addresses.	BE- DK ⁶ - EE- LV- LT- HU- NL- PL- PT ⁷ - SI- SK- FI- SE- UK ⁸ - CH ⁹ - NO ¹⁰ -	BE ¹¹ - CZ- FR- LT- PL- UK-	DK- LU- AT ¹² - PL- CH- NO- IS-
Telecom monitoring	EE- PL- SK- SE- UK ¹³ -	CZ- FR- HU- LV ¹⁴ - UK-	BE- DK- LT- LU- AT- PL- PT- SI- FI - CH- NO- IS-
Storage and production of telecom traffic	EE- LV- HU- SE-	CZ- FR- NL- PT- SI- SK- UK-	BE- DK- LT- LU- AT- PL-

¹ SI: Measures like telephone tapping and room bugging are carried out only by the decision of judicial authorities. While executing these measures, the police can access to documentation (2, 3) autonomously. After the execution of measures has been completed, the permission of judicial authorities is needed for access to documentation.

² SI: See footnote on telephone tapping.

³ UK: Locally held.

⁴ BE: Depends on the type (public or private) of information.

⁵ UK: Unless person is subject to police investigation. Not limited to criminal investigation.

⁶ DK: Police have autonomous access to holders, ex-directory and listed, of telephone, cell-phone, fax and telex, but not e-mail or website subscriptions or addresses.

⁷ PT: If contained in public registers.

⁸ UK: Has enabling legislation allowing the police to require some organisations outside of law enforcement to supply information for law enforcement purposes. These powers are subject to data protection and human rights legislation. In order to exercise these powers the police must ensure that the requirement is lawful, justified, and proportional and that any collateral intrusion has been considered. The information may be obtained for a foreign authority on a police to police basis. However, sufficient details of the investigation, the source of any information and the use to which any results will be put must be provided.

⁹ CH: If public.

¹⁰ NO: Unrestricted.

¹¹ BE: Depends on the type (public or private) of information.

¹² AT: Concerning non-listed holders.

¹³ UK: See previous footnote on UK.

¹⁴ LV: In exceptional cases (e.g., where private telecommunication operators are involved) the police may carry out telecom monitoring but with authorisation of a judicial authority.

(communication data) generated by various information technology systems and handled by telecom operators and Internet Service Providers.			PT- FI - UK- CH- NO ¹ - IS-
Unusual or suspicious (money) transactions	EE- LT- HU- NL ² -AT- PL- SK ³ - FI - SE- UK- NO-	BE- CZ- FR- CY- LV NL ⁴ PL- PT- SI- UK-	DK-LU ⁵ - IS-
Information held by banks, financial institutions and insurance companies on balances, transactions, holding of credit cards or insurance policies.	EE- <i>FR</i> - LT- HU- PL- SK ⁶ - FI - UK ⁷ -	BE- CZ- FR- CY- LV- NL- PT- SI- SE- UK-	BE ⁸ - DK- LU- AT- PL- PT- UK- CH- NO- IS-

¹ NO: restricted numbers or e-mail or website subscriptions or addresses.

² NL: Suspicious transactions.

³ SK: Information kept by FIU, which can be exchanged only with other FIUs in accordance with bilateral agreements.

⁴ NL: Unusual transactions.

⁵ LU: This is a particular situation as the anti-money laundering unit of the criminal police is closely associated to the FIU. In this quality, as “members” of the FIU, the police officers of this unit have access to information. Free exchange with other police officers on national or international level is only possible if the information can be linked to a criminal investigation. If this is the case, then it has to be clarified what is the current status of this investigation. In most of the cases (ongoing investigation) exchange of information is then submitted to the prior authorisation of the judicial authorities.

⁶ SK: Information kept by FIU, which can be exchanged only with other FIUs in accordance with bilateral agreements.

⁷ UK: Only limited details without judicial order.

⁸ BE: Depends on the voluntary or not voluntary transmission of information by the company concerned.

13867/04

LIMITE

**CRIMORG 115
CATS 47
COMIX 659**

NOTE

From : Presidency
To: Article 36 Committee

No. prev. doc. : 13869/04 CRIMORG 116 ENFOPOL 152 COMIX 658 ENFOCUSTOM 75

Subject : Draft Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the member States of the European Union, in particular as regards serious offences including terrorist acts.

The Multidisciplinary Group on Organised Crime discussed the initiative of the Kingdom of Sweden at its meeting on 21 and 22 October 2004 on the basis of document 13178/04 CRIMORG 94 ENFOPOL 130 COMIX 596 ENFOCUSTOM 65.

The outcome of proceedings is contained in document 13869/04 CRIMORG 116 ENFOPOL 152 COMIX 658 ENFOCUSTOM 75.

At the meeting, considerable time was devoted to discussion of the limits between police cooperation and judicial cooperation. Attention was focused on Article 2 (a), which in the current text provides that:

"(a) 'competent law enforcement authority': a national police, customs or other authority, that is authorised by national law to detect, prevent or investigate offences or criminal activities and to exercise authority and take coercive measures in the context of such activities. [A judicial authority is regarded as competent law enforcement authority if the information or intelligence, according to national law, is only held by or accessible to that judicial authority];"

and Article 2 (b) which provides that:

"(b) 'crime investigation': a legal framework within which measures are taken by competent law enforcement or judicial authorities, including public prosecutors, with a view to establishing and identifying facts, suspects and circumstances regarding one or several identified concrete criminal acts;"

The Swedish delegation considered that, since the instrument only covered existing information (article 1:1), information and intelligence provided under the Framework Decision could not be used in criminal proceedings (Article 1:3) and no coercive measures could be taken in accordance with the instrument (article 1:4), there could be no confusion with judicial cooperation. It explained that the reference in Article 2 (a) to judicial authorities was only for those cases where a requesting police authority was dealing with a case at such an early stage that a judicial authority had not yet been involved in the requesting country (pre-investigation phase) but in the requested country the judicial authority was the "owner" of the information or intelligence.

Several delegations thought however that the delimitation in the initiative between police and judicial cooperation was not clear and suggested the deletion of all references to judicial authorities.

Under Articles 1 and 3 of the 1959 Convention on Mutual Legal Assistance in criminal matters, assistance is provided in proceedings in respect of offences; letters rogatory are sent for the purpose of procuring evidence or transmitting articles to be produced in evidence, records or documents.

It would therefore seem to the Presidency, at first sight, that judicial cooperation is not contemplated by the initiative, since under Article 1.3 information and intelligence to be used as evidence before a judicial authority is excluded unless consent is given. However, the analysis cannot stop there.

Under Article 39.1 of the Schengen Convention police authorities shall assist each other for the purposes of preventing and detecting criminal offences, insofar as national law does not stipulate that the request has to be made and channelled via the judicial authorities.

On the other hand, article 6, para 5 of the European Union Convention on Mutual Assistance in Criminal Matters (May 2000) mentions that requests for some forms of assistance (controlled delivery, infiltration, joint team) can be done directly from judicial authorities to police- or customs authorities and the other way around, when in one Member State a judicial authority is competent and in the other Member State a police- or customs authority.

The practical problems that the proposal tries to tackle, can be illustrated as follows. If one takes the example of a secret telephone number that is found on a "red list", police authorities in some Member States do not have access to such lists, but have to make requests to a judicial authority. If the request comes from a foreign police authority, it seems that the practice is to ask the foreign police authority for a letter rogatory. It may also be that the law of the requested State provides that information may not be provided unless the request has been made by a (foreign) judicial authority (in the context of a criminal investigation or proceedings). It is then that the question arises that a judicial authority in the requesting State may not be involved in the criminal investigation since the intelligence and information gathering is at such an early stage that the judicial authorities are not, under the law of the requesting State, involved in the pre-investigation phase and therefore the requesting State's police authorities cannot legally obtain a letter rogatory. The situation may also be such that the pre-investigation phase may be held up while awaiting an answer to the letter rogatory.

It would seem to the Presidency that here rules for judicial cooperation to some extent interfere with rules for police cooperation. The reason would be that when the information is of a particularly sensitive nature ("red list" telephone numbers, DNA evidence, holders of bank accounts, criminal records, tax information, etc), the legislation in at least some Member States

seem to require that a judicial authorisation be sought. When a request for such information comes from abroad, a letter rogatory is asked for since the type of information is considered to be "judicial".

In the perception of the Presidency this problem might be dealt with along the following lines:

1. There seems to be a common understanding that a clear distinction should be kept between police cooperation and judicial cooperation. Therefore the scope of the proposal should be restricted to police cooperation, as is reflected by the legal base stated in the preamble (Article 30 (1) (a) and (b) TEU). The purpose should be to improve police cooperation by enhancing and – as the title of the proposal states – simplifying the exchange of information and intelligence between law enforcement authorities.

2. It seems that the proposal broadens the scope of police cooperation *stricto sensu* in two respects. In the perception of the Presidency these extensions are of a limited nature.

a. The proposal not only covers exchange of information between police authorities but also between other ‘competent law enforcement authorities’, that is ‘authorities authorised by national law to detect, prevent or investigate offences or criminal activities’ (Article 2 (a)). This includes amongst others customs authorities.

b. The proposal also aims to make ‘exchangeable’ information which the requesting law enforcement authority needs for investigative purposes but, according to the national law of the requested member state, is only held by or accessible to a *judicial* authority (Article 2 (a) second sentence).

3. In the opinion of the Presidency the elements of the proposal mentioned under a and b above do not change the nature of the proposed instrument. More specifically, they do not make it an instrument of judicial cooperation. In this respect it should be borne in mind that the exchange of information held by or accessible to a judicial authority, is bound by important conditions. First of all, the information exchanged may not be used in criminal proceedings, that is for judicial purposes. Secondly, the proposal does not relate to information which is accessible only by means of coercive measures. Finally, it seems to follow from Article 4 (2) that information held by a judicial authority may only be requested by and provided to for example a police authority, *to the extent* that at the national level such police authorities are entitled to receive the relevant information.

The Article 36 Committee is requested to confirm whether the analysis above is correct. Members are invited to indicate under what conditions they would be prepared to include information held by their judicial authorities in the proposal, with a view to giving guidance to the future work of the MDG on this issue.
