**COUNCIL OF THE EUROPEAN UNION**

**Brussels, 23 April 2007**

**8711/07**

**CATS 34**
**ENFOPOL 72**
**EUROPOL 40**
**VISA 136**
**COMIX 399**

**NOTE**

| | |
|---|---|
| from : | Presidency |
| to : | delegations |
| No. prev. doc. : | 8540/07 VISA 129 CODEC 356 CATS 31 ENFOPOL 68 EUROPOL 39 COMIX 335<br>5456/1/07 CATS 4 ENFOPOL 7 EUROPOL 9 VISA 21 COMIX 59<br>14196/1/06 REV 1 CATS 157 ENFOPOL 175 EUROPOL 90 VISA 267 COMIX 861<br>10627/06 CATS 126 ENFOPOL 129 EUROPOL 53 VISA 159 COMIX 558<br>9641/06 CATS 105 ENFOPOL 103 EUROPOL 48 VISA 136 COMIX 481<br>15142/05 CATS 83 ENFOPOL 174 EUROPOL 38 VISA 300 COMIX 803 |
| Subject : | Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences |

The Presidency presents in annex a redrafting of the above-mentioned draft Council Decision, taking into account the outcome of the Council meeting of 20 April 2007 regarding the outstanding questions with regard to further discussions with the European Parliament.

The issue of access by UK and IE will be dealt with by the appropriate bodies of the Council.

**ANNEX**

Proposal for a

**COUNCIL DECISION**[1]

**concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences**

THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the Commission[2],

Having regard to the opinion of the European Parliament[3],

Whereas:

*(recitals will be issued later)*

1 Parliamentary reservation DK, FR, IE, NL, SE, UK.
2 OJ C , , p. .
3 OJ C , , p. .

HAS DECIDED AS FOLLOWS:

*Article 1*

**Subject matter and scope**

This Decision lays down the conditions under which Member States' designated authorities and the European Police Office (Europol) may obtain access for consultation of the Visa Information System for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences.

*Article 2*

**Definitions**

1. For the purposes of this Decision, the following definitions shall apply:

   (a) 'Visa Information System (VIS)' means the Visa Information System as established by Council Decision 2004/512/EC;

   (b) 'Europol' means the European Police Office as established by the Convention of 26 July 1995 on the Establishment of a European Police Office ("the Europol Convention");

   (c) 'terrorist offences' means the offences under national law which correspond or are equivalent to the offences in Articles 1 to 4 of Council Framework Decision 2002/475/JHA on combating terrorism[4];

   (d) 'serious criminal offences' means the forms of crime which correspond or are equivalent to those referred to in Article 2(2) of the Framework Decision of 13 June 2002 on the European Arrest Warrant;

   (e) 'designated authorities' means authorities which are responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences and designated by the Member States ~~in accordance with~~ **pursuant to** Article 3 of this Decision.

2. The definitions in the VIS Regulation shall also apply.

[4] OJ L 164, 22.6.2002, p.3.

*Article 3*

**Designated authorities and central access points**

1. Member States shall designate the authorities referred to in Article 2(1)(e) which are authorised to ~~directly~~ access VIS data pursuant to this Decision.

1a. Every Member State shall keep a list of the designated authorities and, within three months after this Decision enters into force, notify it in a declaration to the Commission and the General Secretariat of the Council and may at any time amend or replace its declaration by another declaration.

2. The Commission shall publish the declarations in the *Official Journal of the European Union.*

3. At national level, each Member State shall keep a list of the units within the designated authorities that **are authorised to** ~~shall directly~~ access ~~to~~ the VIS **as well as a list of the central access points through which this access is done**. Such access shall be exercised by the duly empowered staff as referred to in Article 10 of this Decision.

***Article 4a***

**Process for access to the VIS**

**1. Where the conditions of Article 5 are fulfilled the units referred to in Article 3(3) shall submit a request to their central access points referred to in Article 3(3) to access the VIS. Upon receipt of a request for access the central access points shall verify whether the conditions for access are fulfilled. If all conditions for access are fulfilled the requests shall be processed to the VIS by the central access points. The VIS data accessed shall be transmitted to the units referred to in Article 3(3) in such a way as not to compromise the security of the data.**

**2. In case of urgency the central access points may receive written, electronic or oral requests. In such a case, the central access points shall process the request immediately and only verify ex-post whether all the conditions of Article 5 are fulfilled.**

*Article 5*

**Conditions for access to VIS data by designated authorities of Member States to which the VIS Regulation applies**

1. Access to the VIS for consultation by designated authorities shall take place within the scope of their powers and if the following conditions are met:

   (a) (deleted**)**

   (b) access for consultation must be necessary for the purpose of the prevention, detection or investigation of terrorist offences or other serious criminal offences ~~and~~;

   (c) access for consultation must be ~~linked to~~ **necessary in** a specific case ~~and~~; **a specific case exists in particular when the access for consultation is connected to a specific event or to a danger associated with serious crime, or to (a) specific person(s) in respect of whom there are serious grounds for believing that he/she (they) will commit terrorist offences or other serious criminal offences or that he/she (they) has (have) a relevant connection with such a person(s);**

   (d) if there are reasonable grounds**, based on substantive indications,** to consider that consultation of VIS data will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question.

2. Consultation of the VIS shall be limited to searching with any of the following VIS data in the application file:

   (a) surname, surname at birth (earlier surname(s)); first names; sex; date, place and country of birth;

   (b) current nationality of the applicant; nationality at birth;

   (c) type and number of the travel document, the authority which issued it and the date of issue and of expiry;

   (d) main destination and duration of the intended stay;

   (e) purpose of travel;

   (f) date of arrival and departure;

   (g) border of first entry or transit route;

   (h) residence;

(i) (deleted)

(j) fingerprints;

(k) type of visa and the number of the visa sticker

(l) details of the person issuing an invitation and/or liable to pay costs of living during the stay

and shall, in case of a hit, give access to all of the above data as well as to

(a) any other data taken from the application form;

(b) the data entered in respect of any visa issued, refused, annulled, revoked or extended.

*Article 6*

**Conditions for access to VIS data by designated authorities of a Member State to which the VIS Regulation does not apply**

1. Access to the VIS for consultation by designated authorities of a Member State to which the VIS Regulation does not apply shall take place within the scope of their powers and

(a) subject to the same conditions as referred to in Article 5 (1) (b) to (d); and

(b) by a duly motivated written or electronic request to a designated authority of a Member State to which the VIS Regulation applies; that authority shall then request its national central access point to consult the VIS.

2. A Member State to which the VIS Regulation does not apply shall make its visa information available to Member States to which the VIS Regulation applies, on the basis of a duly reasoned written or electronic request, subject to compliance with the conditions laid down in Article 5 (1) (b) to (d).

**2a. Article 8 to 10 of this Decision apply accordingly.**

*Article 7*

**Conditions for access to VIS data by Europol**

1. Access to the VIS for consultation by Europol shall take place within the limits of its mandate and

(a) when necessary for the performance of its tasks pursuant to Article 3(1), point 2 of the Europol Convention and for the purposes of a specific analysis as referred to in Article 10 of the Europol Convention ; or

(b) when necessary for the performance of its tasks pursuant to Article 3(1), point 2 of the Europol Convention and for an analysis of a general nature and of a strategic type, as referred to in Article 10 of the Europol Convention, provided that VIS data is rendered anonymous by Europol prior to such processing and retained in a form in which identification of the data subjects is no longer possible.

2. Article 5 (2) of this Decision applies accordingly.

3. Europol shall designate a specialised unit for the purpose of this Decision with duly empowered Europol officials to act as the central access point to access the VIS for consultation.

4. Processing of information obtained by Europol from access to the VIS shall be subject to the consent of the Member State which has entered that data in the VIS. Such consent shall be obtained via the Europol national unit of that Member State.

*Article 8*

**Protection of personal data**

1. The processing of personal data consulted under this Decision shall be subject to the following rules and to the national law of the consulting Member State. With regard to the processing of personal data consulted under this Decision, each Member State shall ensure an adequate data protection level in its national law which at least corresponds to that resulting from the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data and, for those Member States which have ratified it, the Additional Protocol of 8 November 2001 to that Convention, and shall take into account Recommendation No. R (87) 15 of 17 September 1987 of the Committee of Ministers of the Council of Europe Regulating the Use of Personal Data in the Police Sector.

2. The processing of personal data by Europol pursuant to this Decision shall be in accordance with the Europol Convention and the rules adopted in implementation thereof and supervised by the independent joint supervisory body established by Article 24 of the Convention.

2a. Personal data obtained pursuant to this Decision from the VIS shall only be processed for the purposes of the prevention, detection, investigation and prosecution of terrorist offences or other serious criminal offences.

3. (deleted)

4. (deleted)

5. Notwithstanding paragraphs 1 and 2, personal data obtained pursuant to this Decision from the VIS shall not be transferred or made available to a third country or to an international organisation. By way of exception, such data may be transferred or made available to a third country or an international **body in case of urgency**, exclusively for the purposes and under the conditions set out in Article 5(1) of this Decision, subject to the consent of the Member State having entered the data into the VIS and in accordance with the national law of the Member State transferring the data or making them available. **The transfer of national VIS data is subject to national law of the Member State that entered the data in the VIS according to the Regulation.**

6. The competent body or bodies, which in accordance with national law are charged with the supervision of the processing of personal data by the authorities designated under this Decision shall monitor the lawfulness of the processing of personal data pursuant to this Decision. **The Member States shall ensure that these bodies have sufficient resources to fulfil the tasks entrusted to them under this Decision.**

6a. The bodies referred to in paragraph 6 shall ensure that at least every four years an audit of the processing of personal data pursuant to this Decision is carried out, where applicable according to international auditing standards.

7. Member States and Europol shall allow the competent body or bodies referred to in paragraphs 2 and 6 to obtain the necessary information to enable them to carry out their tasks in accordance with this article.

~~7a. Each Member State shall be liable in accordance with its national law for any injury caused to a person as a result of processing of data in violation of the provisions of this Decision.~~

**8. Before being authorised to process data stored in the VIS, the staff of the authorities having a right to access the VIS shall receive appropriate training about data security and data protection rules and shall be informed of any relevant criminal offences and penalties.**

***Article 8a***

**Data security**

**1. The Member State responsible shall ensure the security of the data during the transmission to, and when received by, the designated authorities.**

**2. Each Member State shall adopt the necessary security measures with respect to data to be retrieved from the VIS pursuant to this Decision and to be subsequently stored, in particular in order to:**

**(a) physically protect data, including by making contingency plans for the protection of critical infrastructure;**

**(b) deny unauthorised persons access to national installations in which the Member State store data (checks at entrance to the installation)**

**(c) prevent the unauthorised reading, copying, modification or removal of data media (data media control);**

**(d) prevent the unauthorised inspection, modification or deletion of stored personal data (storage control);**

**(e) prevent the unauthorised processing of data from the VIS (control of data processing);**

**(f) ensure that persons authorised to access the VIS have access only to the data covered by their access authorisation, by means of individual and unique user identities and confidential access modes only (data access control);**

**(g) ensure that all authorities with a right of access to VIS create profiles describing the functions and responsibilities of persons who are authorised to access, enter, update, delete and search the data and make these profiles available to the national supervisory authorities referred to in Article 8(6) without delay upon their request (personnel profiles);**

**(h) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);**

**(i) ensure that it is possible to verify and establish what data has been retrieved from the VIS, when, by whom and for what purpose (control of data recording);**

**(j) prevent the unauthorised reading and copying of personal data during their transmission from the VIS, in particular by means of appropriate encryption techniques (transport control);**

**(k) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Decision (self-auditing).**

***Article 8b***

**Liability**

**1. Any person who, or Member State which, has suffered damage as a result of an unlawful processing operation or any act incompatible with this Decision shall be entitled to receive compensation from the Member State which is responsible for the damage suffered. That State shall be exempted from its liability, in whole or in part, if it proves that it is not responsible for the event giving rise to the damage.**

**2. If any failure of a Member State to comply with its obligations under this Decision causes damage to the VIS, that Member State shall be held liable for such damage, unless and insofar as another Member State participating in VIS failed to take reasonable measures to prevent the damage from occurring or to minimise its impact.**

**3. Claims for compensation against a Member State for the damage referred to in paragraphs 1 and 2 shall be governed by the provisions of national law of the defendant Member State.**

*Article 8c*

**Self-monitoring**

**Member States shall ensure that each authority entitled to access VIS data takes the measures necessary to comply with this Decision and cooperates, where necessary, with the national body or bodies referred to in Article 8(6).**

*Article 8d*

**Penalties**

**Member States shall take the necessary measures to ensure that any use of VIS data contrary to the provisions of this Decision is punishable by penalties, including administrative and/or criminal penalties, that are effective, proportionate and dissuasive.**

*Article 8e*

**Keeping of VIS data in national files**

**1. Data retrieved from the VIS may be kept in national files only when necessary in an individual case in accordance with the purposes set out in this Decision and in accordance with the relevant legal provisions including those concerning data protection and for no longer than it is necessary in the individual case.**

**2. Paragraph 1 shall not prejudice the provisions of national law of a Member State concerning the entry by its designated authorities in their national files of data which that Member State entered in the VIS according to the Regulation.**

**3. Any use of data which does not comply with paragraphs 1 and 2 shall be considered a misuse under the national law of each Member State.**

*Article 8f*

**Right of access, correction and deletion, Legal procedure**

**1. At the request of the data subject or of the competent body under national law, information shall be supplied in compliance with national law to the data subject upon production of proof of his identity, without unreasonable expense, in general comprehensible terms and without unacceptable delays, on the data processed pursuant to this Decision in respect of his person and its origin, the recipient or groups of recipients, the intended purpose of the processing and the legal basis for the processing. A Member State which has not entered the data itself may only provide information about this data if the Member State which has entered the data has had the chance of expressing its opinion.**

**2. Any act the data subject is entitled to according to paragraph 1 may be refused if necessary in the particular case,**

**(a) to enable the controller to fulfil its lawful duties properly, or**

**(b) to avoid prejudicing of investigations, inquiries or proceedings, or**

**(c) to protect public security and public order in a Member State, or**

**(d) to protect the rights and freedoms of third parties, or**

**(e) to protect the personal safety of individuals**

**and if the interest of the data subject in being informed is for that reason be overridden.**

**3. The data subject shall be entitled to have inaccurate data corrected. If the designated authorities receive such a request or if they have any other evidence to suggest that data processed in the VIS is inaccurate they shall inform the visa authority of the Member State which has entered the data in the VIS immediately, who shall check the data concerned and, if necessary, correct or delete it immediately, pursuant to Article 21 of the VIS Regulation.**

**4. The Member States shall also ensure that, in order to assert his rights in relation to data protection, the data subject shall be able to lodge a complaint to an independent court or a tribunal within the meaning of Article 6(1) of the European Convention on Human Rights and that the data subject is given the possibility to claim for damages or to seek another form of legal compensation.**

**5. The detailed rules for the procedure to assert these rights and the reasons for limiting the right of access shall be governed by the relevant national legal provisions of the Member State where the data subject asserts his rights.**

*Article 9*

**Costs**

Each Member State and Europol shall set up and maintain at their expense, the technical infrastructure necessary to implement this Decision, and be responsible for bearing the costs resulting from access to the VIS for the purposes of this Decision.

*Article 10*

**Keeping of records**

1. Each Member State and Europol shall ensure that all data processing operations resulting from access to the VIS for consultation pursuant to this Decision are recorded for the purposes of checking whether the search is admissible or not, for the purpose of monitoring the lawfulness of data processing, for self-monitoring, ensuring the proper functioning data integrity and security. Those records shall show the **exact** purpose of the access for consultation referred to in Article 5(1)(b), **including the respective form of crime to be prevented, detected or investigated,** and in Article 7(1)(a) or (b) of this Decision, **the respective file number,** the date and exact time of access, the data used for consultation and the type of data consulted, and the name of the authority accessing and consulting the data. In addition, each Member State and Europol shall, according to national rules or the rules of the Europol Convention **also record the identifying mark of the official who carried out the search and of the official who ordered the search or supply**.

2. Such records containing personal data shall be used only for the data protection monitoring of the legality of data processing as well as to ensure data security. Only such records containing data of a non-personal nature may be used for the monitoring and evaluation referred to in Article 12 of this Decision.

3. These records shall be protected by appropriate measures against unauthorised access and abuse and deleted after a period of one year after the five year retention period referred to in Article 20 (1) of the VIS Regulation has expired, unless they are required for monitoring procedures referred to in paragraph 2 of this Article which have already begun.

*Article 11*

**Advisory Committee**

(deleted)

*Article 12*

**Monitoring and evaluation**

1. The ~~Commission~~ **Management Authority** shall ensure that systems are in place to monitor the functioning of the VIS pursuant to this Decision against objectives, in terms of outputs, cost-effectiveness**, security** and quality of service.

**1a. For the purpose of technical maintenance, the Management Authority shall have access to the necessary information relating to the processing operations performed in the VIS.**

2. Two years after the VIS **is brought into operations** and every two years hereafter, the ~~Commission~~ **Management Authority** shall submit a report to the European Parliament ~~and to~~**,** the Council **and the Commission** on the technical functioning of the VIS pursuant to this Decision. That report shall include information on the performance of the VIS against quantitative indicators predefined by the Commission, **and in particular on the need and use made of Article 4a(2)**.

3. ~~Four~~ **Three** years after the VIS **is brought into operation** and every four years thereafter, the Commission shall produce an overall evaluation of the VIS pursuant to this Decision. This evaluation shall include an examination of the results achieved against objectives and an assessment of the continuing validity of the underlying rationale behind this Decision, **the application of this Decision in respect of the VIS, the security of the VIS** and any implications for future operations. The Commission shall **transmit** the evaluation reports to the European Parliament and the Council.

4. The Member States and Europol shall provide to the ~~Commission~~ **Management Authority and the Commission** the information **necessary** to **draft the reports referred to in paragraph 2 and 3**.

**4a. The Management Authority shall provide the Commission with the information necessary to produce the overall evaluations referred to in paragraph 3.** This information may never jeopardise working methods nor include information that reveals sources, staff members or investigations of the designated authorities.

**4b. During a transitional period before the Management Authority takes up its responsibilities, the Commission shall be responsible for producing and submitting the reports referred to in paragraph 2.**

*Article 13*

**Entry into force and date of application**

1. This Decision shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. This Decision shall apply from the date to be determined by the Council once the Commission has informed the Council that the VIS Regulation has entered into force and is applicable.

The General Secretariat of the Council shall publish that date in the *Official Journal of the European Union.*

Done at Brussels,

*For the Council*

The President