Access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol

2005/0232(CNS) - 23/06/2008 - Final act

PURPOSE: to enable the authorities of the Member States responsible for internal security and Europol to consult the VIS with a view to preventing and combating terrorism and other serious criminal offences.

LEGISLATIVE ACT: Council Decision 2008/633/JAI 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.

BACKGROUND: in the framework of the gradual establishment of an area of freedom, security and justice, the European Union ensures the free movement of persons but also a high level of security. In this context, absolute priority has been given to the development and establishment of a Visa Information System (VIS) as a system for the exchange of visa data between Member States (see CNS/2004/0029). However, in order to develop and establish the VIS, particularly in the area of internal security, including the fight against terrorism, an overall legal framework must be put in place to complement the existing Regulation, while ensuring strict compliance with the rules governing the protection of personal data. That is why the Council adopted this Decision aimed at granting the authorities of the Member States responsible for internal security access to the VIS, for particular cases specified in the Decision, with a view to enabling them to consult useful information that may help them prevent terrorism and other serious criminal offences. Note that this Decision complements Regulation (EC) No 767/2008 of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) insofar as it provides for a legal base under Title VI of the Treaty on European Union authorising access to the VIS for designated authorities and for Europol (see COD/2004/0287).

CONTENT: the 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 (VIS)** for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences.

Designated authorities and central access points: Member States shall designate the authorities which are authorised to access VIS data. In this context, they shall draw up a list of "**designated authorities**", which may be amended. Member States shall also designate the **central access point(s)** through which access to the VIS is gained. The list of designated authorities and access points shall be sent to the Commission and the General Secretariat of the Council by 2 December 2008 and shall be published in the Official Journal of the European Union. At national level, each Member State shall keep a list of the operating units within the designated authorities that are authorised to access the VIS through the central access point(s). **Only duly empowered staff** of the operational units as well as the central access point(s) shall be **authorised to access the VIS**.

Access to the VIS: the Decision lays down all the technical conditions for access to VIS data:

- **Procedure for access**: in order to access the VIS, the authorised operating units shall submit a reasoned written or electronic request to the central access points. The central access points shall verify whether the conditions for access are fulfilled and grant access. The VIS data shall be

transmitted in such a way as not to compromise the security of the data. In an exceptional case of urgency, the central access point(s) may receive oral requests and process them immediately (verifying ex-post whether all the necessary conditions are fulfilled);

- **Conditions for access to VIS data by designated authorities**: access to the VIS shall only be granted if a certain number of conditions are met, including the existence of reasons to believe that consultation of the VIS data can significantly contribute to the prevention, detection and investigation of the offences in question. In any event, consultation of the VIS shall be restricted to the following information: surname, first name, sex, date, place and country of birth; nationality; type and number of the travel document and the date of issue and of expiry; main destination and duration of the intended stay; purpose of travel; fingerprints; photographs, etc. as well as data entered in respect of any visa issued, refused, annulled, revoked or extended;
- **Specific conditions for access by Member States in respect of which the VIS Regulation has not yet been put into effect**: subject to the same conditions as referred to above, the authorities of Member States which do not normally have access to the VIS shall submit a duly reasoned request to the national designated authorities and central access points to access certain data of the VIS under specific conditions;
- **Conditions for access to VIS data by Europol**: subject to the conditions already laid down in the Decision and provided that access is justified in the context of Europol's competences, Europol may access the VIS data within the limits of its mandate. Processing of information obtained by Europol shall be subject to the consent of the Member State which has entered that data in the VIS.

In any event, any person with access to the VIS data shall receive **appropriate training** about data security and data protection rules before being authorised to process data stored in the VIS.

Data protection: for the purposes of protection of personal data, and in particular to exclude routine access, the processing of VIS data should only be carried out on a case-by-case basis. Such a specific case exists, in particular, when the access for consultation is connected to:

- a specific event;
- a danger associated with serious crime;
- specific person(s) in respect of whom there are serious grounds for believing that the person(s) will commit or has (have) committed terrorist offences or other serious criminal offences or that the person(s) has (have) a relevant connection with such (a) person(s).

To ensure that data is processed adequately, the Decision provides that each Member State should establish, in accordance with national law, **a competent body** responsible for supervising the processing of data by the designated authorities. These bodies shall have sufficient resources to fulfil the tasks entrusted to them and shall ensure that at least every four years an audit of the processing of data is carried out.

Link with the Framework Decision on the protection of personal data processed in the framework of police cooperation: once the proposed Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters has entered into force, it should apply to the personal data which are processed pursuant to this Decision. However, in the meantime and in order to complement these rules, the Decision provides for a series of provisions to ensure the necessary data protection. Each Member State should therefore 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 the corresponding case law, as well as other relevant legal texts.

The transfer of data to third parties: the Decision specifies that personal data obtained from the VIS shall not be transferred to a third country or to an international organisation. However, in an exceptional case of urgency, such data may be transferred exclusively for the purposes of the prevention and detection

of terrorist offences and of other serious criminal offences and under the strict conditions set out in the Decision, subject to the consent of the Member State having entered the data into the VIS. Records of such transfers shall be kept and made available to national data protection authorities.

Data security: Member States are solely responsible for ensuring the security of the data during transmission to the designated authorities. They shall provide for *ad hoc* security measures to ensure maximum security of data when stored and transferred (including preventing any copies of or modifications to the data and any unauthorised processing). Very strict measures for monitoring and self-auditing by the designated authorities are also provided for.

Other technical measures for securing and protecting data: the Decision also provides for a series of measures on:

- **keeping data**: data retrieved from the VIS may be kept only when necessary and in cases duly provided for in the Decision;
- **the right of correction and deletion**: any person has the right to have factually inaccurate data relating to them corrected or unlawfully stored data deleted;
- **records of information sent**: all data processing operations resulting from access to the VIS for 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 of the system, data integrity and security.

Liability and penalties: there are provisions to ensure that any person who, or Member State which, has suffered damage as a result of an unlawful processing operation or of the provisions of the Decision shall be entitled to receive compensation. Measures are also provided for to ensure that any use of VIS data contrary to the provisions of the Decision is punishable by penalties, including administrative and/or criminal penalties, that are effective, proportionate and dissuasive.

Costs: each Member State and Europol shall set up and maintain, at their expense, the technical infrastructure, and be responsible for bearing the costs resulting from access to the VIS.

Monitoring and evaluation: the Decision lays down the procedures for monitoring and evaluating the functioning of the VIS. In accordance with Regulation (EC) No 767/2008, a Management Authority shall be set up to monitor the overall functioning of the VIS. This Management Authority shall also be responsible for assessing the systems established pursuant to this Decision in terms of output, cost-effectiveness, security and quality of service. Moreover, two years after the VIS is brought into operation (and every two years thereafter), the Management Authority shall submit a report to the European Parliament, the Council and the Commission on the technical functioning of the VIS pursuant to this Decision. Furthermore, 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, including thoughts on the future functioning of the system.

Territorial provisions: the Decision lays down the terms for participation in this Decision, for certain Member States that do not normally take part in the common visa policy (UK and Ireland, which shall be associated with the implementation of the Decision under specific conditions) or for countries associated with the implementation of the Schengen acquis (Iceland, Norway and Switzerland).

ENTRY INTO FORCE: the Decision shall enter into force on 02.09.2008. It shall take effect from the date of the full entry into force of Regulation (EC) No 768/2008 on the VIS.