

# Procedure file

Basic information	
CNS - Consultation procedure Decision	2005/0232(CNS)  Procedure completed
Access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol	
See also <a href="#">2015/0807(CNS)</a> Amended by <a href="#">2017/0351(COD)</a> Repealed by <a href="#">2018/0152A(COD)</a>	
Subject 7.10.04 External borders crossing and controls, visas 7.30.05.01 Europol, CEPOL 7.30.20 Action to combat terrorism	

Key players			
European Parliament	Committee responsible	Rapporteur	Appointed
	<b>LIBE</b> Civil Liberties, Justice and Home Affairs	ALDE <a href="#">LUDFORD Baroness Sarah</a>	23/01/2006
Council of the European Union	Council configuration	Meeting	Date
	<a href="#">Justice and Home Affairs (JHA)</a>	<a href="#">2807</a>	12/06/2007
	<a href="#">Justice and Home Affairs (JHA)</a>	<a href="#">2794</a>	19/04/2007
	<a href="#">Justice and Home Affairs (JHA)</a>	<a href="#">2696</a>	01/12/2005
European Commission	Commission DG <a href="#">Justice and Consumers</a>	Commissioner BARROT Jacques	

Key events			
24/11/2005	Legislative proposal published	COM(2005)0600	Summary
01/12/2005	Debate in Council	<a href="#">2696</a>	
16/02/2006	Committee referral announced in Parliament		
19/04/2007	Debate in Council	<a href="#">2794</a>	Summary
14/05/2007	Vote in committee		Summary
21/05/2007	Committee report tabled for plenary, 1st reading/single reading	<a href="#">A6-0195/2007</a>	
06/06/2007	Debate in Parliament		

07/06/2007	Results of vote in Parliament		
07/06/2007	Decision by Parliament	<a href="#">T6-0229/2007</a>	Summary
12/06/2007	Act adopted by Council after consultation of Parliament		Summary
12/06/2007	End of procedure in Parliament		
13/08/2008	Final act published in Official Journal		

### Technical information

Procedure reference	2005/0232(CNS)
Procedure type	CNS - Consultation procedure
Procedure subtype	Legislation
Legislative instrument	Decision
	See also <a href="#">2015/0807(CNS)</a> Amended by <a href="#">2017/0351(COD)</a> Repealed by <a href="#">2018/0152A(COD)</a>
Legal basis	Treaty on the European Union (after Amsterdam) M 034-p2c; Treaty on the European Union (after Amsterdam) M 030-p1
Stage reached in procedure	Procedure completed
Committee dossier	LIBE/6/32176

### Documentation gateway

Legislative proposal		COM(2005)0600	24/11/2005	EC	Summary
Document attached to the procedure		N6-0058/2006 <a href="#">OJ C 097 25.04.2006, p. 0006-0010</a>	20/01/2006	EDPS	Summary
Committee draft report		<a href="#">PE370.254</a>	10/03/2006	EP	
Amendments tabled in committee		<a href="#">PE372.109</a>	10/05/2007	EP	
Committee report tabled for plenary, 1st reading/single reading		<a href="#">A6-0195/2007</a>	21/05/2007	EP	
Text adopted by Parliament, 1st reading/single reading		<a href="#">T6-0229/2007</a>	07/06/2007	EP	Summary

### Additional information

European Commission	<a href="#">EUR-Lex</a>
---------------------	-------------------------

### Final act

<a href="#">Decision 2008/633</a> <a href="#">OJ L 218 13.08.2008, p. 0129</a> Summary
---

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

PURPOSE : to create a legal framework establishing the conditions under which Member States' internal security bodies and Europol may

access the Visa Information System (VIS).

PROPOSED ACT: Council Decision.

CONTENT: this proposal complements Council Decision 2004/512, which establishes the Visa information System (VIS). The fight against terrorism is a priority for all Member States. The European Union is committed to combating terrorism and organised crime, hence the creation of the VIS. Access to information stored on the VIS could help Member State authorities as well as Europol to both prevent and combat terrorist acts. This present proposal has been prepared in order to clarify how and when Member States' internal security bodies as well as Europol, can access VIS information for the dual purposes of preventing and combating terrorism and/or organised crime.

The present initiative does not go beyond what is necessary to achieve its objectives. Importantly, the scope is limited to terrorist offences and to crimes for which Europol is responsible. In addition, the proposed provisions restrict the use of VIS data to specific cases only in order to exclude routine access. Only those national authorities responsible for the prevention, detection or investigation of criminal offences will have access to the VIS. Moreover, those authorities will be obliged to go through a central access point which will consult the VIS on their behalf, on a case-by-case basis and after receipt of a duly motivated request. Furthermore, the Authorities responsible for internal security are clearly listed in the Annex to this Decision, as are the Central Access Points.

In presenting this proposal, the Commission emphasises that the Decision seeks to ensure full respect for the right to liberty and security, the right to respect for private and family life, the right to the protection of personal data and the principles of legality and proportionality of criminal offences and penalties.

The Commission points out that the proposal fulfils both the subsidiarity and proportionality principles. The subsidiarity principle applies in this instance in that the VIS database is established under an EU framework thereby hindering individual Member States from authorising, on their own, access to it. In other words, the objectives of the Decision could not be sufficiently achieved by the Member States acting on their own. As far as the proportionality principle is concerned the initiative does not go beyond what is necessary to achieve its objective. The Decision seeks to ensure full respect for the fundamental rights and the conditions set out for access to VIS data is restricted to specific cases only? in other words routine access is not a possibility.

Given that Ireland and the United Kingdom do not participate in the common visa policy and that they are not a party to the VIS Regulation, the internal security bodies of these Member States do not have direct access to the VIS. However, it is appropriate that VIS data be made available to the Irish and UK authorities. The provisions of the Decision apply to Iceland and Norway.

The proposal has implications for the Community budget in so far as the additional number of access to the VIS generated by the authorities responsible for internal security via the central access points has to be taken into account when setting up and maintaining the system. The implementation of the proposed Decision would entail only a small amount of additional expenditure, to be charged to the budget of the European Communities for meetings of the secretarial services for the new committee set up by this Decision.

#### FINANCIAL IMPLICATIONS:

- Policy sector concerned : Justice and Home Affairs; 1806 ? Establishing a genuine area of freedom, security and justice in criminal and civil matters.
- Human resources and associated expenditure: EUR 1 134 000.
- Administrative costs, other than human resources and associated costs not included in reference amount: EUR 246 000.
- Total indicative financial costs for intervention (commitment/payment and including human resources): EUR 1 382 640.
- Period of application: From 2006.
- Over all total number of human resources: 1,75.
- Financial cost of human resources and associated costs not included in the reference amount: EUR 189 000 per year from 2006-2011.
- Other administrative expenditure not included in reference amount: EUR 41 440 per year from 2006-2011, totalling over the entire period EUR 248 640.

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

---

#### OPINION OF THE EUROPEAN DATA PROTECTION SUPERVISOR

The European Data Protection Supervisor (EDPS) was asked by the Commission to give its opinion on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences.

The EDPS deems it important to deliver an opinion on this sensitive subject because this proposal follows directly from the establishment of the VIS, which will be subject to his supervision.

Overall, the Data Protection Supervisor underlines the crucial importance of granting access to authorities in charge of internal security and Europol, only on a case by case basis, and under strict safeguards. This aim is achieved by the proposal in a globally satisfactory way, although some improvements can be made, as proposed in this opinion:

- it should be a condition for access to the VIS according to Article 5 that consultation will ?substantially? contribute to the prevention, detection or investigation of a serious crime, and the records required in Article 10 should allow an evaluation of this condition in each individual case;
- two search keys for access in the VIS mentioned in Article 5(2), namely ?purpose of travel? and ?photographs?, should be reconsidered and made available as supplementary information in the case of a hit;
- the level of data protection applying beyond consultation should be equivalent, regardless of the authorities consulting the VIS data. Article 8 and 10 should also apply to Member States to which the VIS Regulation does not apply;

- a coordinated approach to supervision should be ensured, also with regard to access to the VIS as envisaged in this proposal;
- provisions on monitoring systems should also ensure self-auditing of compliance with data protection requirements.

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

---

The Mixed Committee took note of the main results of the Triologue held between the Council, the European Parliament and the Commission on 28 March 2007 regarding a draft Regulation concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay visas.

The outcome of the Triologue was encouraging and the Council Presidency informed that a first reading agreement with Parliament on the VIS Regulation would be a realistic possibility. The Presidency also informed the Council about the state of play concerning a draft 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 Mixed Committee agreed on a compromise package for further negotiations with the European Parliament with a view to reaching an agreement with this institution on the two instruments as soon as possible.

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

---

The committee adopted the report by Baroness Sarah LUDFORD (ALDE, UK) amending - under the consultation procedure - the proposed Council decision on access for consultation of the VIS by the authorities of the Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences:

- in the list of definitions, 'serious criminal offences' shall mean 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";
- designated authorities of the Member States may access data contained in the VIS in specific cases and following a substantiated written or electronic request via central access points which will have to check that all the relevant conditions for accessing the data are complied with. In exceptional cases of urgency, the request may be received orally and the required checks can be made afterwards;
- at national level, each Member State should keep a list of the operating units within the designated authorities that are authorised to access the VIS through the central access points;
- the committee adopted a series of amendments aimed at ensuring adequate data protection. It stipulated inter alia that "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". Personal data obtained from the VIS should not be transferred or made available 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", in which case Member States shall ensure that records are kept of such transfers and make them available to national data protection authorities on request;
- a new article provided for penalties, "including administrative and/or criminal penalties, that are effective, proportionate and dissuasive", in the event of any misuse of VIS data;
- any person has the right to have factually inaccurate data relating to him/her corrected or unlawfully stored data relating to him/her deleted;
- three years after the VIS is brought into operation and every four years thereafter, the Commission shall produce an overall evaluation of the VIS, including an assessment of the application of the Decision in respect of the VIS;
- whereas the Commission's proposal stated that both Ireland and the United Kingdom are taking part in the Decision, in accordance with Article 5 of the Protocol integrating the Schengen acquis, the committee pointed out that the Decision "constitutes a development of provisions of the Schengen acquis" in which neither the UK nor Ireland take part, and that these two countries were therefore not taking part in the Decision and were not bound by it or subject to its application. However, it added that, "in accordance with Framework Decision 2006/960/JHA, information contained in the VIS can be provided to the United Kingdom and Ireland by the competent authorities of the Member States whose designated authorities have access to the VIS pursuant to this Decision and information held in the national visa registers of the United Kingdom and Ireland can be provided to the competent law enforcement authorities of the other Member States. Any form of direct access for central authorities of the United Kingdom and Ireland to the VIS would, under the present state of their participation in the Schengen acquis, require an Agreement between the Community and those Member States, possibly to be supplemented by other rules specifying the conditions and procedures for such access."

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

---

The European Parliament adopted a resolution drafted by Baroness Sarah LUDFORD (ALDE, UK) amending - under the consultation procedure - the proposed Council decision on access for consultation of the VIS by the authorities of the Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences. The main amendments were as follows:

- in the list of definitions, 'serious criminal offences' shall mean 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";

- every Member State shall keep a list of the designated authorities. Within three months after the Decision enters into force every Member State shall notify in a declaration to the Commission and the General Secretariat of the Council their designated authorities. Every Member State shall designate the central access point(s) through which the access is done;
- 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 in accordance with the Article on the process for access to the VIS. The central access points should process the requests to the VIS following verification whether all conditions for access are fulfilled. In an exceptional case of urgency the central access points shall process the request immediately and only do the verification afterwards;
- Parliament adopted a series of amendments aimed at ensuring adequate data protection. 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;
- personal data obtained 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;
- personal data obtained from the VIS should not be transferred or made available 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, in which case Member States shall ensure that records are kept of such transfers and make them available to national data protection authorities on request;
- the competent body or bodies, which in accordance with national law are charged with the supervision of the processing of personal data by the designated shall monitor the lawfulness of the processing of personal data and. Member States shall ensure that these bodies have sufficient resources to fulfil the tasks entrusted to them;
- Parliament expanded Article 8 to include provisions on the following: data security; liability; self-monitoring; penalties; keeping of VIS data in national files; and right of access, correction and deletion. Any person has the right to have factually inaccurate data relating to him corrected or unlawfully stored data relating to him deleted;
- Parliament inserted a detailed list of records that must be kept;
- three years after the VIS is brought into operation and every four years thereafter, the Commission shall produce an overall evaluation of the VIS;
- the Commission's proposal states that both Ireland and the United Kingdom are taking part in this Decision, in accordance with Article 5 of the Protocol integrating the Schengen acquis. However, Parliament adopted an amendment stating that neither the UK nor Ireland are taking part and are not bound by it or subject to its application. It further stated that in accordance with Framework Decision 2006/960/JHA, information contained in the VIS can be provided to the United Kingdom and Ireland by the competent authorities of the Member States whose designated authorities have access to the VIS and information held in the national visa registers of the United Kingdom and Ireland can be provided to the competent law enforcement authorities of the other Member States. Any form of direct access for central authorities of the United Kingdom and Ireland to the VIS would, under the present state of their participation in the Schengen acquis, require an Agreement between the Community and those Member States, possibly to be supplemented by other rules specifying the conditions and procedures for such access.

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

---

The Council agreed on a Decision concerning access for consultation of the 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.

It also welcomed the agreement reached in first reading with the European Parliament on a Regulation concerning the VIS and the exchange of data between Member States on short-stay visas (see [COD/2004/0287](#)).

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

---

**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.