

This text is meant purely as a documentation tool and has no legal effect. The Union's institutions do not assume any liability for its contents. The authentic versions of the relevant acts, including their preambles, are those published in the Official Journal of the European Union and available in EUR-Lex. Those official texts are directly accessible through the links embedded in this document

► **B**

**COUNCIL DECISION 2008/633/JHA**

**of 23 June 2008**

**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**

(OJ L 218, 13.8.2008, p. 129)

Amended by:

Official Journal			
	No	page	date
► <b><u>M1</u></b>	Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019	L 135 27	22.5.2019



## COUNCIL DECISION 2008/633/JHA

of 23 June 2008

**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**

### *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 (VIS) 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 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 of 13 June 2002 on combating terrorism <sup>(1)</sup>;
- (d) 'serious criminal offences' means the forms of crime which correspond or are equivalent to those referred to in Article 2(2) of Framework Decision 2002/584/JHA;
- (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 pursuant to Article 3.

2. The definitions in Regulation (EC) No 767/2008 shall also apply.

### *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 access VIS data pursuant to this Decision.

<sup>(1)</sup> OJ L 164, 22.6.2002, p. 3.

**▼B**

2. Every Member State shall keep a list of the designated authorities. By 2 December 2008 every Member State shall notify in a declaration to the Commission and the General Secretariat of the Council their designated authorities and may at any time amend or replace its declaration by another declaration.

3. Every Member State shall designate the central access point(s) through which the access is done. Member States may designate more than one central access point to reflect their organisational and administrative structure in fulfilment of their constitutional or legal requirements. By 2 December 2008 every Member State shall notify in a declaration to the Commission and the General Secretariat of the Council their central access point(s) and may at any time amend or replace its declaration by another declaration.

4. The Commission shall publish the declarations referred to in paragraphs 2 and 3 in the *Official Journal of the European Union*.

5. 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).

6. 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 Article 4.

#### *Article 4*

#### **Procedure for access to the VIS**

1. Where the conditions of Article 5 are fulfilled the operating units referred to in Article 3(5) shall submit a reasoned written or electronic request to the central access points referred to in Article 3(3) to access the VIS. Upon receipt of a request for access the central access point(s) shall verify whether the conditions for access referred to in Article 5 are fulfilled. If all conditions for access are fulfilled, the duly authorised staff of the central access point(s) shall process the requests. The VIS data accessed shall be transmitted to the operating units referred to in Article 3(5) in such a way as not to compromise the security of the data.

2. In an exceptional case of urgency, the central access point(s) may receive written, electronic or oral requests. In such cases, the central access point(s) shall process the request immediately and only verify *ex-post* whether all the conditions of Article 5 are fulfilled, including whether an exceptional case of urgency existed. The *ex-post* verification shall take place without undue delay after the processing of the request.

**▼B***Article 5***Conditions for access to VIS data by designated authorities of Member States**

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) access for consultation must be necessary for the purpose of the prevention, detection or investigation of terrorist offences or other serious criminal offences;
- (b) access for consultation must be necessary in a specific case;
- (c) there are reasonable grounds to consider that consultation of VIS data will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question.

**▼M1**

1a. In cases where the designated authorities have launched a query of the common identity repository (CIR) in accordance with Article 22 of Regulation (EU) 2019/817 of the European Parliament and of the Council<sup>(1)</sup>, and where the conditions for access laid down in this Article are met, they may access the VIS for consultation where the reply received as referred to in Article 22(2) of that Regulation reveals that data are stored in the VIS.

**▼B**

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 (former surname(s)); first name(s); sex; date, place and country of birth;
- (b) current nationality and 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) intended date of arrival and departure;
- (g) intended border of first entry or transit route;
- (h) residence;
- (i) fingerprints;

<sup>(1)</sup> Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27).

**▼B**

- (j) type of visa and the number of the visa sticker;
- (k) details of the person issuing an invitation and/or liable to pay the applicant's subsistence costs during the stay.

3. Consultation of the VIS shall, in the event of a hit, give access to all of the data listed in paragraph 2 as well as to:

- (a) any other data taken from the application form;
- (b) photographs;
- (c) 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 in respect of which Regulation (EC) No 767/2008 has not yet been put into effect**

1. Access to the VIS for consultation by designated authorities of a Member State in respect of which Regulation (EC) No 767/2008 has not yet been put into effect shall take place within the scope of their powers and

- (a) subject to the same conditions as referred to in Article 5(1); and
- (b) by a duly motivated written or electronic request to a designated authority of a Member State to which Regulation (EC) No 767/2008 applies; that authority shall then request the national central access point(s) to consult the VIS.

2. A Member State in respect of which Regulation (EC) No 767/2008 has not yet been put into effect shall make its visa information available to Member States to which Regulation (EC) No 767/2008 applies, on the basis of a duly reasoned written or electronic request, subject to compliance with the conditions laid down in Article 5(1).

3. Article 8(1) and (3) to (6), Article 9(1), Article 10(1) and (3), Article 12, Article 13(1) and (3) shall 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**

- (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.

**▼M1**

- 1a. In cases where Europol has launched a query of the CIR in accordance with Article 22 of Regulation (EU) 2019/817, and where the conditions for access laid down in this Article are met, Europol may access the VIS for consultation where the reply received as referred to in Article 22(2) of that Regulation reveals that data are stored in the VIS.

**▼B**

- 2. Article 5(2) and (3) shall apply 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.
- 3. 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.

**▼B**

4. 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. However, in an exceptional case of urgency such data may be transferred or made available to a third country or an international organisation, exclusively for the purposes of the prevention and detection of terrorist offences and of other serious criminal offences 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. In accordance with national law, Member States shall ensure that records are kept of such transfers and make them available to national data protection authorities on request. The transfer of data by the Member State that entered the data in the VIS according to Regulation (EC) No 767/2008 shall be subject to the national law of that Member State.

5. 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.

6. The bodies referred to in paragraph 5 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 5 to obtain the necessary information to enable them to carry out their tasks in accordance with this Article.

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 9***Data security**

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

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 stores data (checks at entrance to the installation);

**▼B**

- (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 the VIS create profiles describing the functions and responsibilities of persons who are authorised to access and search the data and make these profiles available to the national supervisory authorities referred to in Article 8(5) 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 10***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 Member 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 failed to take reasonable measures to prevent the damage from occurring or to minimise its impact.



**▼B**

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 11***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(5).

*Article 12***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 13***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 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 Regulation (EC) No 767/2008.

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 14***Right of access, correction and deletion**

1. The right of persons to have access to data relating to them obtained from the VIS pursuant to this Decision shall be exercised in accordance with the law of the Member State in which they invoke that right.

2. If national law so provides, the national supervisory authority shall decide whether information is to be communicated and by what procedures.

3. A Member State other than that which has entered the data into the VIS according to Regulation (EC) No 767/2008 may communicate information concerning such data only if it first gives the Member State entering the data an opportunity to state its position.

**▼B**

4. Information shall not be communicated to the data subject if this is indispensable for the performance of a lawful task in connection with the data or for the protection of the rights and freedoms of third parties.

5. Any person has the right to have factually inaccurate data relating to him corrected or unlawfully stored data relating to him deleted. 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 immediately inform the visa authority of the Member State which has entered the data in the VIS, which shall check the data concerned and, if necessary, correct or delete it immediately, pursuant to Article 24 of Regulation (EC) No 767/2008.

6. The individual concerned shall be informed as soon as possible and in any event not later than 60 days from the date on which he applies for access or sooner if national law so provides.

7. The individual concerned shall be informed about the follow-up given to the exercise of his rights of correction and deletion as soon as possible and in any event not later than three months from the date on which he applies for correction or deletion or sooner if national law so provides.

8. In each Member State any person shall have the right to bring an action or a complaint before the competent authorities or courts of that Member State which refused the right of access to or the right of correction or deletion of data relating to him, provided for in this Article.

*Article 15***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 16***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 of the system, data integrity and security.

Those records shall show:

- (a) the exact purpose of the access for consultation referred to in Article 5(1)(a), including the form of terrorist offence or other serious criminal offence concerned, and for Europol, the exact purpose of the access for consultation referred to in Article 7(1);
- (b) the respective national file reference;

**▼B**

- (c) the date and exact time of access;
- (d) where applicable that use has been made of the procedure referred to in Article 4(2);
- (e) the data used for consultation;
- (f) the type of data consulted;
- (g) according to national rules or the rules of the Europol Convention the identifying mark of the official who carried out the search and of the official who ordered the search or supply.

2. 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 records containing data of a non-personal nature may be used for the monitoring and evaluation referred to in Article 17.

3. These records shall be protected by appropriate measures against unauthorised access and abuse and deleted after a period of one year after the retention period referred to in Article 23(1) of Regulation (EC) No 767/2008 has expired, unless they are required for monitoring procedures referred to in paragraph 2 of this Article which have already begun.

*Article 17***Monitoring and evaluation**

1. The Management Authority referred to in Regulation (EC) No 767/2008 shall ensure that systems are in place to monitor the functioning of the VIS pursuant to this Decision against objectives, in terms of output, cost-effectiveness, security and quality of service.

2. 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.

3. 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. 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 4(2).

4. 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.

**▼B**

5. The Member States and Europol shall provide to the Management Authority and the Commission the information necessary to draft the reports referred to in paragraph 3 and 4. This information shall not jeopardise working methods nor include information that reveals sources, staff members or investigations of the designated authorities.

6. The Management Authority shall provide the Commission with the information necessary to produce the overall evaluations referred to in paragraph 4.

7. During the 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 3.

*Article 18***Entry into force and date of application**

1. This Decision shall enter into force on the 20th day following its publication in the *Official Journal of the European Union*.

2. This Decision shall take effect from a date to be determined by the Council once the Commission has informed the Council that Regulation (EC) No 767/2008 has entered into force and is fully applicable.

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