

# Visa Information System (VIS)

## FAQs

### 1) What is the VIS?

**The Visa Information System (VIS) is a system for the exchange of data on short-stay visas between Schengen States.**

The VIS consists of a **central database**, a national interface in each Schengen State, and a communication infrastructure between the central database and the national interface. **The VIS is connected to the national visa systems of all Schengen States** via the national interfaces to enable competent authorities of the Schengen States to process data on visa applications and on visa issued, refused, annulled, revoked or extended.

The VIS is composed of two systems, first the VIS database with alphanumerical searching capabilities and an Automated Fingerprint Identification System (AFIS) that compares received fingerprints against database and returns hit/no hit response, along with matches.

The principal central VIS is located in Strasbourg (France) and a back-up central VIS, capable of ensuring all functionalities of the principal central VIS is located in Sankt Johann in Pongau (Austria).

The VIS processes continuously the information collected by Schengen States' consulates. For example, the information entered locally by the visa authorities can be available within a few minutes in the VIS. The VIS supports swift services for verification of visa holders at the border crossing points. For example, a verification takes only a few seconds.

The VIS operates 24/7, 365 days a year.

The Commission was in charge of the development of the central database, the national interfaces and the communication infrastructure between the central VIS and the national interfaces. Their development was funded under EU budget. Each Schengen State is responsible for the development, management, and operation of its national system.

The Agency for the management of large-scale IT systems is since 1 December 2012 the Management Authority of the VIS.

### 2) What is the VIS legal framework?

The following instruments constitute the VIS legal framework:

- Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS), OJUE L 213, 15.6.2004, p. 5.
- **Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the VIS and the exchange of data**

**between Member States on short-stay visas (VIS Regulation)**, OJUE L 218, 13.8.2008, p. 60.

- Council Decision 2008/633/JHA of 23 June 2008 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 offence, OJUE L 218, 13.8.2008, p. 129.
- Regulation (EC) No 81/2009 of the European Parliament and of the Council of 14 January 2009 amending Regulation (EC) No 562/2006 as regards the use of the Visa Information System (VIS) under the Schengen Borders Code, OJUE L 35, 4.2.2009, p. 56.
- Regulation (EC) No 810/2009 of the European Parliament and the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code), OJUE L 243, 5.9.2009, p. 1.
- Commission Decision 2010/49/EC of 30 November 2009 determining the first regions for the start of operations of the Visa Information System (VIS), OJUE L 23, 27.1.2010, p. 62.
- Commission implementing Decision 2011/636/EU of 21 September 2011 determining the date from which the Visa Information System (VIS) is to start operations in a first region, OJUE L 249, 27.9.2011, p. 18.
- Commission Regulation (EU) No 977/2011 of 3 October 2011 amending Regulation (EC) No 810/2009 of the European Parliament and of the Council establishing a Community Code on Visas.
- Commission implementing Decision 2012/274/EU of 24 April 2012 determining the second set of regions for the start of operations of the Visa Information System (VIS), OJUE L 134, 25.5.2012.
- Commission implementing Decision 2012/233/EU of 27 April 2012 determining the date from which the Visa Information System (VIS) is to start operations in a second region, OJUE L 117, 1.5.2012, p. 9.
- Commission implementing Decision 2012/512/EU of 21 September 2012 determining the date from which the Visa Information System (VIS) is to start operations in a third region, OJUE L 256, 22.9.2012, p. 21.
- Commission implementing Decision 2013/122/EU of 7 March 2013 determining the date from which the Visa Information System (VIS) is to start operations in a fourth and a fifth region, OJUE L 65, 8.3.13, p. 35.
- Commission implementing Decision 2013/266/EU of 5 June 2013 determining the date from which the Visa Information System (VIS) is to start operations in a sixth and a seventh region, OJUE L 154, 6.6.2013, p. 8.
- Commission implementing Decision 2013/441/EU of 20 August 2013 determining the date from which the Visa information System (VIS) is to start operations in an eighth region, OJUE L 223, 21.8.2013, p. 15.
- Commission implementing Decision C(2013) 5914 final of 30 September 2013 determining the third and last set of regions for the start of operations of the Visa Information System (VIS).

### 3) What is the VIS deployment plan?

**The VIS did not start operations on the same date in all Schengen States' consulates worldwide.** The VIS is being progressively deployed, **region by region**, in the order defined by the Commission on the basis of three criteria defined by the VIS Regulation: the risk of irregular immigration, the threats to the internal security of the Schengen States, and the feasibility for collecting biometrics from all locations in the region.

**The Commission adopted in November 2009 a Decision determining the first three regions for the VIS consular roll-out.** The VIS first started operations in all Schengen States' visa issuing consulates in **North Africa**, on 11 October 2011, in **the Near East**, on 10 May 2012, and then in **the Gulf region**, on 2 October 2012.

**The Commission adopted on 24 April 2012 a Decision determining the second set of regions for the start of operations: West and Central Africa** (start of operations in March 2013); **East and Southern Africa** (June 2013); **South America** (September 2013); **Central Asia, South East Asia and the occupied Palestinian territory (November 2013).**

The Commission has adopted on 30 September 2013 a Decision setting the sequence of the VIS roll-out in the remaining regions of the world: Central America, North America, the Caribbean, Australasia, Western Balkans and Turkey, the Eastern neighbouring countries, Russia, China/Japan and neighbouring countries, India/Pakistan and neighbouring countries, the European 'microstates', the UK/Ireland, the other EU Member States.

**Schengen States have the possibility to start using the VIS, with or without collecting visa applicants' fingerprints, in any location ahead of the general planning, provided that they notify first the Commission.**

### 4) Which data are registered in the VIS?

In each region where the VIS will be progressively deployed, Schengen States' visa authorities will register in the VIS **data relating to short-stay visa applications** (i.e. applications for stays in the Schengen area up to three months). **Data on national long-stay visas will not be registered in VIS.**

On receipt of an application, the visa authorities of the competent Schengen State will create an application file in the VIS and will register **the alphanumeric data contained in the Schengen visa application form<sup>1</sup>, the digital photograph, and the 10 fingerprints taken flat of the applicant.**

If the applicant is travelling in a group the application files of the travellers will be linked in the VIS. If a previous application has been registered for the same applicant, both applications will also be linked in the VIS.

**For each region, the Commission determines the date from which the use of the VIS and the collection of fingerprints is mandatory** for all Schengen visa-

---

<sup>1</sup> including the applicant's name, his/her nationality, his/her place of residence, his/her occupation, the travel document's number, the type of visa requested, the main destination and the duration of the intended stay, the intended border of first entry, the details of the inviting person.

issuing consulates in the region concerned. **Before that date, a Schengen State may decide to start operations ahead of the general roll-out planning with or without collecting the fingerprints** of visa applicants. If a Schengen State decides not to collect the fingerprints, the other data will be registered in the VIS.

When a **decision has been taken on the application** (issuance/ refusal of the visa) or subsequently (annulment, revocation, extension), **the information is registered in the VIS** by the visa authorities of the competent Schengen States. When the visa is issued and if all the applicant's data - including his/her fingerprints - was registered in the VIS, a code 'VIS' is inserted in the visa sticker. If the fingerprints were not collected because this was not yet mandatory in the region concerned, the code 'VIS 0' is inserted in the visa sticker.

#### **5) What are the consequences of VIS in practice for visa applicants?**

**First-time visa applicants will always have to appear in person when lodging the application in order to provide their photograph and fingerprints.**

**The photograph can be digitally taken at the time of the application or scanned from an existing one.**

**For subsequent applications within 5 years the fingerprints can be copied from the previous application file in the VIS.**

Nevertheless it has to be underlined that in case of reasonable doubt regarding the identity of the applicant, the consulate shall collect again fingerprints within the 5 year period specified above.

Furthermore, the applicant may request that they be collected if, at the time when the application is lodged, it cannot be immediately confirmed that the fingerprints were collected within this 5 years period.

**Visa applicants' biometric data can be collected by Schengen States' consulates and external service providers but not commercial intermediaries (e.g. travel agencies).**

Since 31 October 2011, Schengen States' border guards check the VIS using, systematically, the visa sticker number and, possibly, the verification of fingerprints of the visa holder. After a transitional period of three years, the searches in the VIS will always be carried out using the visa sticker number in combination with the fingerprints, except in a limited set of circumstances (for instance due to the intensity of traffic).

**When arriving at the external border of the Schengen area, visa holders will have to provide their fingerprints for comparison with those registered in the VIS, if requested by Schengen States' border control authorities.**

Visa holders whose fingerprints were not collected at the time of application, either because they were exempted from this requirement or because the collection of fingerprints was not yet mandatory in the region concerned, will not be requested to provide fingerprints at the border.

## **6) Which applicants are exempted from the requirement to provide fingerprints?**

In accordance with Article 13(7) of the Visa Code, are exempted from the requirement to provide fingerprints the following categories of applicants:

- **children under the age of 12;**

- **persons for whom fingerprinting is physically impossible.** If the fingerprinting of fewer than 10 fingers is possible, the maximum number of fingerprints shall be taken. If the impossibility is temporary, the applicant shall be required to provide the fingerprints at the following application;

- **heads of State or government and members of a national government** with accompanying spouses, **and the members of their official delegation when they are invited** by Member States' governments or by international organisations **for an official purpose;**

- sovereigns and other senior members of a royal family, when they are invited by Member States' government or by international organisation for an official purpose.

**This list is mandatory and exhaustive. Holders of diplomatic passports are not exempted as such from the fingerprinting requirement.** They may be exempted if they are members of the official delegation of heads of State/ members of a national government invited for an official purpose.

## **7) Which authorities have access to the VIS?**

The **visa authorities** of the Schengen States have access to the VIS **both for entering and consulting the data.** The data on the application and on the decisions related thereto are entered in the VIS by the visa authorities of the Schengen State competent for examining the application or for taking the decision. **Data entered by one Schengen State may then be consulted by the visa authorities of all other Schengen States, for instance when examining another application from the same applicant.**

**Other authorities from the Schengen States have access to the VIS for consultation only.**

The **national border authorities** have access to the VIS for the purpose of **verifying the identity of the visa holder, the authenticity of the visa, and whether the conditions for entry to the territory of the Schengen States are fulfilled.** Checks in the VIS at the external borders of the Schengen area are compulsory since 31 October 2011. For a maximum period of three years after the VIS has started operations these checks may be performed using the visa sticker number only. After this transitional period checks in the VIS at the borders will have to comprise systematic fingerprint verifications, except in a limited set of circumstances.

**The national authorities responsible for carrying out checks within the territory of the Schengen States** have access to the VIS for the purpose of **verifying the identity of the visa holder, the authenticity of the visa, and whether the conditions for entry, stay or residence on the territory of the Schengen States are fulfilled.**

The **competent national asylum authorities** have access to the VIS for determining the Member State responsible for examining an asylum application in accordance with Regulation (EC) n° 343/2003 and for the examination of such an application.

In the future, **Europol will have access for consultation to the VIS for the purposes of the prevention, detection and investigations of terrorist offences and of other serious criminal offences.**

**The national law enforcement authorities may request access to VIS data for the same purposes**, since 1.9.2013, providing that certain legal conditions are fulfilled: access to VIS data must be necessary in a specific case and there must be reasonable grounds to consider that the consultation of the data will substantially contribute to the prevention, detection or investigation of terrorist and other serious crimes.

As a rule, **VIS data cannot be transferred or made available to a third country or an international organization.** By way of derogation, certain data registered in the VIS (name, nationality, travel document number, residence) may be communicated to a third country or an international organization when necessary in an individual case for proving the identity of a third country national, including for the purpose of return.

#### **8) What are the data protection rules with regard to VIS data?**

**Strict data protection rules are defined in the VIS Regulation** and subject to the control of national and European data protection authorities.

**Data is kept in the VIS for maximum 5 years** starting on the expiry date of the visa, if a visa has been issued; or on the new expiry date of the visa, if a visa has been extended; or on the date a negative decision is taken by the visa authorities.

**Any person has the right to obtain communication of the data recorded in the VIS** related to him/her from the Schengen State which entered the data into the system. Any person may also request that **inaccurate data** related to him/her **be corrected** and that **data unlawfully recorded be deleted.**

**In each Schengen State, national supervisory authorities monitor independently the processing of the personal data registered in the VIS by the Schengen State in question.**

**The European Data Protection Supervisor** monitors the data processing activities by **the VIS Management authority**

## Questions

### **1) 'VIPs', high-ranking officials and diplomatic passport holders in our country do not represent a security or an immigration risk for the EU. Why should they be required to appear in person at the consulate for providing their fingerprints?**

- There are four categories of applicants which are exempted from the obligation to provide fingerprints:
  - children under the age of 12;
  - persons for whom fingerprinting is physically impossible;
  - heads of State or government and members of a national government with accompanying spouses, and the members of their official delegation when they are invited by Member States' governments or by international organisations for an official purpose;
  - sovereigns and other senior members of a royal family, when they are invited by Member States' government or by international organisation for an official purpose.
- This list of exemptions is mandatory and exhaustive.
- The use of biometrics is an essential feature of the VIS. It will guarantee accurate procedures and avoid false identifications.
- The list of exemptions from the fingerprint requirement had therefore to be limited and based on objective criteria, applicable to all third countries.
- Holders of diplomatic passports are as such not exempted from the fingerprinting requirement. However, this category of persons may be exempted from the visa requirement under visa waivers granted by individual EU Member States. Government representatives and officials travelling to attend regular political and technical dialogue meetings with the EU (e.g. senior

officials meetings, subcommittees) are not exempted either. However, high-ranking officials and holders of diplomatic passports will be exempted from the fingerprinting requirement when travelling as members of the official delegations of Heads of State or of members of the national government invited for an official purpose.

- It was not possible to provide for a general exemption for high-ranking officials or 'VIPs', as such a category very much depends on the local circumstances and cannot therefore be defined objectively.
- It was not possible either to provide for a general exemption for holders of diplomatic passports, as the standards for the issuance of these documents vary very much depending on the country concerned.
- In accordance with the provisions laid down in Regulation 539/2001, Schengen States may decide to exempt holders of diplomatic passports from certain countries from the visa requirement.
- The procedure for the collection of fingerprints is rapid, simple and discreet. In most consulates 'VIPs' may benefit from certain facilities when providing their biometric data (private rooms and reserved time slots).
- In addition, fingerprints will in principle be collected only at the first application within a 5 year period. For subsequent applications, the fingerprints will be copied from the previous application file unless there is a reasonable doubt regarding the identity of the applicant.
- The collection of fingerprints should not therefore create a major disturbance for any visa applicant.

**2) What will happen in case of technical problems with the database? Can visas still be issued? Could there be some**

## **problems for crossing the Schengen area external borders?**

- The experience with the use of the VIS in the first eight regions of deployment has shown that the system runs very smoothly.
- In the unlikely event of a technical failure of the central database, a back-up system capable of ensuring all functionalities of the VIS will take over after 30 min.
- If a Schengen State's consulate cannot connect or transmit data to the VIS due to a temporary technical problem at national level, the processing of visa applications could be momentarily disrupted. However, such problems should be solved very quickly and, at least, within the 15 calendar day limit for taking a decision on a Schengen visa application. There should be therefore no major disturbance for visa applicants.
- If Schengen States' border authorities cannot access the VIS due to a temporary technical problem, they will proceed to manual checks. Entry to the Schengen area will never be refused on the ground that the VIS is not working.

## **3) Which authorities will have access to the data stored in the VIS?**

- Schengen States' authorities responsible for the issuance of visas, border and immigration checks, and asylum procedures have a direct access to the data stored in the VIS.
- Since 1 September 2013, Schengen States' law enforcement authorities may request access to the data stored in the VIS under very strict legal conditions and only for the purpose of prevention, detection, or investigation of terrorist and other serious criminal offenses. Europol will also have access to the VIS for the same purposes.
- As a rule, VIS data cannot be transferred or made available to third countries or to international organizations.

