Personal Data Protection in the Visa Information System

Visa Information System (VIS) is a system for the exchange of data among the Member States on applications for short-stay visas and on the decisions taken in relation thereto, including the decisions whether to annul, revoke or extend the visa, to facilitate the examination of such applications and the related decisions.

What is the objective of the VIS?

Facilitating visa checks and issuance of visas: The VIS allows border guards to verify whether an individual who provides the visa is its legal holder and identify persons in the Schengen territory who do not have any documents or have suspicious ones. Use of biometric data for the verification of the identity of the visa holder allows more expedient, precise and safer checking of personal data. This system also facilitates the visa issuance process, particularly for frequent travellers.

Anti-abuse: Though most of the visa holders comply with the rules, abuses may also occur. The VIS will help to prevent fraudulent behaviour, for instance, will not allow submitting applications for issuance of the visa for other EU States when the first application has been refused.

Protection for travellers: Biometric technology facilitates the detection of travellers using another person's travel documents and protects travellers from identity theft.

Facilitating asylum applications: The VIS allows easier detection which EU State is responsible for the examination of the asylum application and easier examination of such applications.

Strengthening of security: The VIS helps to prevent, detect and investigate terrorist offences and other serious offences.

How does it operate in practice?

The visa applicant's 10 fingerprints and digital photograph are collected. These biometric data, along with the data provided in the visa application form, are recorded in a secure central database. The information is stored in the central database in Strasbourg (with a backup site in Austria).

Fingerprints are neither required from children under the age of 12 nor from people who cannot physically provide finger scans. Frequent travellers to the Schengen Area do not have to give new finger scans every time they apply for a new visa.

Third country nationals have to address the representation of the state where they intend to travel and there biometric data are collected. The received information is entered into the system and is valid for five years. This period of storage starts from the date of expiry of the issued visa, the date of the negative decision or the date when the decision to change the issued visa was taken.

The visa holder's finger scans may be compared against those in the database at the Schengen Area's external borders. A mismatch does not mean that entry for the third country national will be automatically refused – it will just lead to further checks on the traveller's identity using additional data.

There are two types of inquiries concerning the establishment of personal identity: verification and identification. During verification at the border crossing point the finger scans are compared to the biometric entries attached to the visa. During identification the finger scans are compared to the content of all database.

Which countries use the VIS and operate it?

As the Schengen instrument the VIS is applicable to all Schengen States. Denmark also has taken the decision for the implementation of this instrument.

Who can use the VIS?

Competent visa institutions may consult the VIS in order to consider applications and take related decisions. Institutions

responsible for the checks at external borders and in national territories are entitled to search the VIS in order to verify personal identity, visa authenticity or whether the person complies with the requirements related to the entry, stay or whether the person lives in national territories. Asylum institutions may only search the VIS in order to determine the EU State, responsible for the examination of the asylum application. In certain cases national authorities or Europol may request access to data entered into the VIS in order to prevent terrorist and criminal offences and perform their investigation.

How is personal data protection ensured?

Access to the VIS data is granted only to the authorised personnel in performing their tasks. They have to ensure that the use of the VIS data is limited to what is necessary, appropriate and proportional in relation to the tasks to be performed. Every individual shall have the right to request access to his/her data in the VIS and make sure they are entered correctly and lawfully. If that is not the case, persons shall have the right to request that data related to them are corrected or deleted.

How to address concerning access, correction, modification or unlawful use of personal data?

If you believe that your personal data were used unlawfully, they need to be corrected or deleted, you may contact the data controller concerning the access to these data. In Lithuania the Ministry of Interior of the Republic of Lithuania (www.vrm.lt.) is the data controller.

National supervisory authority

The purpose of the national supervisory authority is to monitor independently the legality of personal data processing in the VIS in a respective Member State, including control of their transmission to and from the VIS. The State Data Protection Inspectorate is appointed as the competent authority in Lithuania.

For more information please contact the State Data Protection Inspectorate at

A. Juozapavičiaus St. 6, LT-09310 Vilnius, Lithuania
Tel. + 370 5 271 2804. Fax. + 370 5 261 9494