Visa Information System (VIS): visa processing

2018/0152A(COD) - 13/03/2019 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 522 votes to 122, with 31 abstentions, a legislative resolution on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA.

The European Parliament's position adopted at first reading under the ordinary legislative procedure amended the Commission's proposal as follows.

Extended scope of the Visa Information System (VIS)

The Visa Information System (VIS) is a European database used by authorities to monitor third-country nationals requiring a visa to travel to the Schengen area.

The reform of the VIS should enable the system to better respond to security developments and migration challenges, and to optimise the management of the EU's external borders by extending its scope to **long-stay visas and residence permits** in order to address gaps in security information.

Purpose of the VIS

As regards short-stay visas, the VIS shall facilitate the exchange of data between Member States on visa applications and decisions, with a view to facilitating and accelerating the visa application procedure.

With regard to long-stay visas and residence permits, the VIS shall: (i) support a high level of security in all Member States by contributing to the assessment of whether the applicant or holder of a document is considered to pose a threat to public policy, internal security; (ii) facilitate checks at external border crossing points and enhance the effectiveness of checks within the territory of the Member States.

For all visas, the VIS shall assist in the identification of missing persons, in particular children, and contribute the prevention of threats to the internal security of any of the Member States, namely through the prevention, detection and investigation of terrorist offences or of other serious criminal offences in appropriate and strictly defined circumstances.

System architecture

Members proposed that Council Decision 2004/512/EC establishing the Visa Information System (VIS) be repealed and fully integrated into the VIS Regulation. They also recommend that certain elements of the Commission's implementing decisions be included in this Regulation.

The VIS would be based on a centralised architecture. The centralised services shall be duplicated to two different locations namely Strasbourg, France, hosting the principal VIS Central System, central unit (CU) and St Johann im Pongau, Austria, hosting the backup VIS Central System, backup central unit (BCU).

The central VIS system, the uniform national interfaces, the web service, the carrier gateway and the VIS communication infrastructure shall share and re-use as much as technically possible the hardware and

software components of respectively the entry/exist central (EES Central System), the EES national uniform interfaces, the ETIAS carrier gateway, the EES web service and the EES communication infrastructure.

Data processing

Processing of personal data within the VIS by each competent authority shall not result in discrimination against applicants, visa holders or applicants and holders of long-stay visas, and residence permits.

It shall fully respect human dignity and integrity and fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the European Union, including the right to respect for one's private life and to the protection of personal data. Particular attention shall be paid to children, the elderly and persons with a disability and persons in need of international protection.

Fingerprint data of children

No fingerprints of children under the age of 6 shall be entered into VIS.

Parliament proposed that the collection of fingerprints from children should be subject to stricter safeguards and a limitation on the purposes for which such data may be used to situations where it is in the best interests of the child, in particular by limiting the storage period of stored data.

The biometric data of minors from the age of six shall be taken by officials trained specifically to take a minor's biometric data in a child-friendly and child-sensitive manner and in full respect of the best interests of the child.

Access to the system by centralised European agencies

The proposed reform shall ensure better access for Europol and law enforcement authorities to VIS data in order to identify crime victims and advance their investigations into serious crime or terrorism.

In the case of the European Border and Coast Guard Agency, Members believe it is essential that this agency has access to the system. However, they proposed restricting access for return teams while reinforcing access to statistics for the purpose of risk analysis.

Links with other systems and interoperability

Parliament intends to ensure the utmost coherence with other systems, in particular ETIAS, including its safeguards. Checks against other databases should also be carried out for holders of long-stay visas and residence permits.

However, in order to provide appropriate guarantees, Members specified which controls should be carried out. They also specified the specific measures following each hit, both to protect third-country nationals and to ensure the confidentiality of information.

Any hit resulting from the queries which cannot automatically be confirmed by VIS shall be manually verified by the national single point of contact. Depending on the type of data triggering the hit, the hit should be assessed either by consulates or by a national single point of contact, with the latter being responsible for hits generated in particular bylaw enforcement databases or systems.

Each Member State shall designate a national authority, operational 24 hours a day, 7 days a week, which shall ensure the relevant manual verifications and assessment of hits for the purposes of this Regulation.

Data transfer

Personal data obtained by a Member State pursuant to this Regulation shall not be transferred or made available to any third country, international organisation or private entity established in or outside the Union. As an exception to that rule, however, it shall be possible to transfer such personal data to a third country or to an international organisation where such a transfer is subject to strict conditions and necessary in individual cases in order to assist with the identification of a third-country national in relation to his or her return.

Entry into force

Parliament proposed enhancing reporting mechanisms and setting a deadline of a maximum of two years to have this reformed VIS up and running.