Basic information

2004/0287(COD) COD - Ordinary legislative procedure (ex-codecision procedure) Regulation	Procedure completed
Visa Information System (VIS) and exchange of data between Member States on short-stay visas (VIS Regulation) Amended by 2011/0051(COD) Amended by 2016/0106(COD) Amended by 2017/0351(COD) Amended by 2018/0152A(COD) Amended by 2019/0002(COD) Amended by 2020/0278(COD) Amended by 2022/0132A(COD) Amended by 2022/0132B(COD) **Subject** 7.10.04 External borders crossing and controls, visas	

Key players

European Parliament

Committee responsible	Rapporteur	Appointed
LIBE Civil Liberties, Justice and Home Affairs	LUDFORD Baroness Sarah (ALDE)	05/10/2004

Council of the European Union

Council configuration	Meetings	Date
Justice and Home Affairs (JHA)	2807	2007-06-12
Justice and Home Affairs (JHA)	2642	2005-02-24
Justice and Home Affairs (JHA)	2794	2007-04-19
Justice and Home Affairs (JHA)	2696	2005-12-01
Competitiveness (Internal Market, Industry, Research and Space)	2645	2005-03-07
Agriculture and Fisheries	2881	2008-06-23

European Commission

Commission DG	Commissioner
Justice and Consumers	BARROT Jacques

Key events

Date	Event	Reference	Summary
28/12/2004	Legislative proposal published	COM(2004)0835	Summary

26/01/2005	Committee referral announced in Parliament, 1st reading		
24/02/2005	Debate in Council		
07/03/2005	Resolution/conclusions adopted by Council		Summary
01/12/2005	Resolution/conclusions adopted by Council		Summary
19/04/2007	Debate in Council		Summary
14/05/2007	Vote in committee, 1st reading		Summary
22/05/2007	Committee report tabled for plenary, 1st reading	A6-0194/2007	
06/06/2007	Debate in Parliament		
07/06/2007	Decision by Parliament, 1st reading	T6-0227/2007	Summary
07/06/2007	Results of vote in Parliament		
23/06/2008	Act adopted by Council after Parliament's 1st reading		
09/07/2008	Final act signed		
09/07/2008	End of procedure in Parliament		
13/08/2008	Final act published in Official Journal		

Technical information

Procedure reference	2004/0287(COD)
Procedure type	COD - Ordinary legislative procedure (ex-codecision procedure)
Procedure subtype	Legislation
Legislative instrument	Regulation
Amendments and repeals	Amended by 2011/0051(COD) Amended by 2016/0106(COD) Amended by 2017/0351(COD) Amended by 2018/0152A(COD) Amended by 2019/0002(COD) Amended by 2020/0278(COD) Amended by 2022/0132A(COD) Amended by 2022/0132B(COD)
Legal basis	EC Treaty (after Amsterdam) EC 066 EC Treaty (after Amsterdam) EC 062-p2
Stage reached in procedure	Procedure completed
Committee dossier	LIBE/6/25780

Documentation gateway

European Parliament

Document type	Committee	Reference	Date	Summary
Amendments tabled in committee		PE370.101	09/05/2007	
Committee report tabled for plenary, 1st reading/single reading		A6-0194/2007	22/05/2007	
Text adopted by Parliament, 1st reading/single reading		T6-0227/2007	07/06/2007	Summary

Council of the EU

Document type	Reference	Date	Summary
Draft final act	03630/2007/LEX	09/07/2008	

European Commission

Document type	Reference	Date	Summary
Legislative proposal	COM(2004)0835	28/12/2004	Summary
Document attached to the procedure	SEC(2004)1628	28/12/2004	Summary
Follow-up document	COM(2016)0655	14/10/2016	Summary
Follow-up document	SWD(2016)0327	14/10/2016	
Follow-up document	SWD(2016)0328	14/10/2016	

Other institutions and bodies

Institution/body	Document type	Reference	Date	Summary
OS	Document attached to the procedure	N6-0015/2005 OJ C 181 23.07.2005, p. 0013-0029	23/03/2005	Summary

Additional information

Source	Document	Date
European Commission	EUR-Lex	

Final act

Corrigendum to final act 32008R0767R(05)
OJ L 284 12.11.2018, p. 0039

Regulation 2008/0767
OJ L 218 13.08.2008, p. 0060 Summary

Delegated acts

Reference	Subject
2023/2633(DEA)	Examination of delegated act

Visa Information System (VIS) and exchange of data between Member States on short-stay visas (VIS Regulation)

2004/0287(COD) - 14/10/2016 - Follow-up document

The Commission adopted a report on the implementation of Regulation (EC) No 767/2008 of the European Parliament and of the Council establishing the Visa Information System (VIS), the use of fingerprints at external borders and the use of biometrics in the visa application procedure/REFIT Evaluation

The current legal framework: the legal framework adopted to establish the VIS includes the following acts:

- Council Decision 2004/512/EC established the VIS itself;
- Regulation (EC) No 767/2008 laying down the VIS's purpose, functionalities and responsibilities and the conditions and procedures for the exchange of visa data between Member States;
- Regulation (EC) No 810/2009 (the Visa Code) setting out the rules on the registration of biometric identifiers in the VIS.

The VIS is instrumental in order to:

1. improve the implementation of the common visa policy, consular cooperation and consultation between central authorities to prevent threats to internal security and 'visa shopping';
2. facilitate the fight against fraud and checks at external border crossing points and within the Member States' territory;
3. assist in the identification and return of illegal immigrants;
4. facilitate the application of the Dublin Regulation.

The VIS specifically contributes to safeguarding the Member States' internal security and combating terrorism and illegal immigration by improving and facilitating the procedures for issuing visas.

Visa statistics: at the moment, around 16 million Schengen visas are issued every year by the 26 Member States and Schengen associated countries. By the end of March 2016 data on close to **23 million visa applications** and 18.8 million fingerprints had been entered in the VIS.

Assessment and monitoring: the VIS legal framework provided for an evaluation of the relevant acts. On this basis, and considering as well the overall principles and criteria for carrying an evaluation of EU policy instruments in the context of the Regulatory and Fitness (REFIT) programme, the Commission launched in 2015 the first evaluation of the system since its entry into operation (2011).

This evaluation was performed internally by the Commission. A number of different data collection tools were used to gather information, which included the opinions of third-country nationals and governments of countries under visa obligation worldwide.

Main conclusions and recommendations: overall, the findings of the evaluation point to the fact that the introduction of the VIS has led to:

- a **simplification and facilitation** of the visa application process by ensuring that data gathered by all Member States are stored and exchanged via a common system ;
- a **reduction in the administrative burden** of national administrations ; and
- **clear, smooth and effective procedures** when dealing with processing visa applications, performing checks at external borders or in the territory, identifying third country nationals for migration or return purposes or examining asylum applications.

A majority of Member States concurred that the introduction of the VIS facilitated the checks at external border crossing points and within the Member States' territory. Furthermore, many Member States felt that the introduction of the VIS had supported the application of the Dublin Regulation by helping to determine which Member State was responsible for examining an asylum application in cases where a visa had been issued by a Member State to the asylum applicant.

For almost half of the responding Member States the introduction of the VIS had a positive impact on the prevention of threats to the Member States' internal security.

Problems revealed by the evaluation: the evaluation has, however, shown that there is are some deficiencies in the system, the main ones being as follows:

- **data quality**: quality problems have been found for both alphanumeric and biometric data: these problems (recurrent since the launch of VIS) are at the top of the list of priority areas identified by the evaluation;
- **monitoring and statistics**: finding informative and reliable statistics was one of the major hurdles encountered while gathering information for the evaluation. However, this is essential for the system to function properly;
- **use of the VIS when collecting the data:** while the evaluation found that the VIS significantly facilitated the fight against visa fraud, the system was not conceived to prevent fraud **during a visa application**. Given that the obligation to check travellers' fingerprints makes it harder for fraudsters to cross the border using fraudulent visa stickers, a possible knock-on effect could be a shift from the use of fraudulent visa stickers towards the use of **visas obtained under false pretences** in consulates (at the time of applying for a visa). To prevent this, consulates should verify the applicant's identity before taking the fingerprints;

- **use of the data for law enforcement purposes:** access to VIS for law enforcement purposes remains fragmentary in most Member States. In particular, the possibility for fingerprint searches is not yet used;
- **data protection in the VIS**: ensuring that data subjects can access, rectify and erase data held about them increases the transparency of data processing for them. A notable phenomenon identified by the evaluation was the absence, or very low number, of requests by data subjects to exercise their rights to access, correct or delete their personal data stored in the VIS. The finding could be explained by Member States' good performance on the protection of personal data.

To ensure that these problems might be rectified, the Commission proposes a series of short and long-term measures.

For example, **as regards the quality of fingerprints**, the system needs to be technically adjusted so that it can better distinguish between cases where fingerprints are not required for legal reasons and cases where there is a factual reason why they cannot be provided. Alternative standards could also be put in place, such as **taking photographs directly when applying for a visa.** As a short term solution, the Commission proposes that **eu-LISA** should be entrusted with a role, including the task of producing data quality reports.

With respect to **access to the VIS for law enforcement purposes**, the Commission suggests that law enforcement authorities could be given the possibility to search the VIS using latent fingerprints and photographs.

It goes on to propose a series of other solutions to the problems discussed. However, certain problems cannot be resolved without a **revision of the legal basis of the VIS**. These include:

- transferring the responsibility for producing statistics to eu-LISA;
- interconnectivity with other systems;
- improved data quality rules and the production of data quality reports;
- scrapping obsolete provisions of the current law (e.g. on the roll-out, the setup and transition to VIS Mail or various transition periods).

Where a legislative revision is envisaged, the Commission will conduct an impact assessment.

Visa Information System (VIS) and exchange of data between Member States on short-stay visas (VIS Regulation)

2004/0287(COD) - 19/04/2007

The Mixed Committee took note of the main results of the Trialogue 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 Trialogue 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.

Visa Information System (VIS) and exchange of data between Member States on short-stay visas (VIS Regulation)

2004/0287(COD) - 07/06/2007 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted a resolution drafted by Baroness Sarah **LUDFORD** (ALDE, UK) amending the proposed regulation on the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas. Parliament's text was the result of an agreement with Council aimed at ensuring that the legislative process is completed at the first reading stage. The key amendments were as follows:

- the aims of the VIS should include facilitating the visa application procedure and contributing to the prevention of threats to the internal security of any of the Member States;

- Parliament amended Article 3 relating to the availability of data for the prevention, detection and investigation of terrorist offences and other serious criminal offences. Designated authorities of the Member States and Europol may access data contained in the VIS in specific cases and following a substantiated written or electronic request, if this can contribute to the prevention, detection or investigation of terrorist offences and other serious criminal offences. This access will be indirect, 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, these checks can be made afterwards;

- a number of definitions were amended and Parliament inserted a definition for "alphanumeric data" ;

- each competent authority authorised to access the VIS shall ensure that the use of the VIS is necessary, appropriate and proportionate to the performance of tasks of the competent authorities. Each competent authority shall ensure that in using the VIS, it does not discriminate against applicants and visa holders on grounds of sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation and that it fully respects the human dignity and the integrity of the applicant or of the visa h holder.

- where particular data is not required to be provided for legal reasons or factually cannot be provided, the specific data field(s) shall be marked as "not applicable". In the case of fingerprints, the system shall permit a distinction to be made between the cases where fingerprints are not required to be provided for legal reasons and the cases where they cannot be provided factually; after a period of four years this functionality shall expire unless it is confirmed by a Commission decision on the basis of the evaluation ;

- Parliament expanded the list of data to be provided upon lodging the application ;

- after a transitional period, a management authority funded from the general budget of the European Union, shall be responsible for the operational management of the Central VIS and the National Interfaces. The Management Authority shall ensure, in cooperation with the Member States, that at all times the best available technology, subject to a cost-benefit analysis, is used for the Central VIS and the National Interfaces ;

- during a transitional period before the Management Authority takes up its responsibilities, the Commission shall be responsible for the operational management of the VIS. The Commission may delegate that task and tasks relating to implementation of the budget to national public-sector bodies, in two different countries. The latter must meet specified selection critieria ;

- the principal Central VIS, which carries out technical supervision and administration, shall be located in Strasbourg (France) and a backup Central VIS, capable of ensuring all functionalities of the principal Central VIS in case of failure of this system, shall be located in Sankt Johann im Pongau (Austria) ;

- 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. ;

- data processed in the VIS shall not be transferred or made available to a third country or to an international organisation. However, a derogation may be made in individual cases for the purpose of proving the identity of third-country nationals, including for the purpose of return, only where certain conditions are satisfied ;

- each application file shall be stored in the VIS for a maximum of five years

- each Member State must adopt a security plan ;

- access to VIS data by other authorities will be permitted for certain specific purposes such as verification at external borders, verification of the identity of the visa holder or the authenticity of the visa, examination of an asylum application, etc.;

- a new article provided for active cooperation between the National Supervisory Organisations and the European Data Protection Supervisor, which shall draw up a joint report of activities every two years.

Visa Information System (VIS) and exchange of data between Member States on short-stay visas (VIS Regulation)

2004/0287(COD) - 01/12/2005

The Council adopted conclusions on the VIS : exchange of data on Schengen short-stay visas including the national long-stay visas which are concurrently valid as short-stay visas.

In particular, the Council considers that without prejudice to the adoption of the proposal for the Visa Information System, Member States who will be implementing the VIS Regulation should plan for the collection of biometric data for the VIS, at consular posts, on a coordinated and coherent regional basis, that reflects the problems of illegal migration and threats to the internal security of the Member States and the feasibility of collecting biometric data from all locations. Those Member States should endeavour to be in a position to collect all the biometric data required for the VIS within 24 months of the commencement of the roll out.

Those Member States should endeavour to be in a position to commence the collection of biometric data for the VIS in early 2007, which should begin with consular posts in North Africa and the Near East regions.

In order to facilitate the development of a collaborative approach and the completion of the roll out within the time table, every effort should be made to resolve outstanding issues, in particular, the methods of collection of biometric data. Those Member States should also plan to process biometric data at border crossing points in a coordinated and coherent manner that complements the collection of the data at consular posts.

Visa Information System (VIS) and exchange of data between Member States on short-stay visas (VIS Regulation)

2004/0287(COD) - 09/07/2008 - Final act

PURPOSE: to establish the legal framework for the Visa Information System and the procedures and conditions for the exchange of visa data between Member States on short-stay visa applications.

LEGISLATIVE ACT: 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).

BACKGROUND: the establishment of the Visa Information System (VIS) represents one of the key initiatives within the policies of the European Union aimed at establishing an area of freedom, security and justice. In 2004, the Council adopted Council Decision 2004/512/EC establishing the Visa Information System (VIS) (CNS/2004/0029) established the VIS as a system for the exchange of visa data between Member States. This Decision gave to the Commission the mandate to prepare the technical development of VIS and to provide the required legislative basis to allow for the inclusion in the Community budget of the necessary appropriations for the technical development of VIS and the execution of that part of the budget.

It is now necessary to define the purpose, the functionalities and responsibilities for the VIS, and to establish the conditions and procedures for the exchange of visa data between Member States. This is the purpose of the present Regulation. It shall be complemented by a separate legal instrument adopted under Title VI of the Treaty on European Union concerning access for the consultation of the VIS by authorities responsible for internal security (CNS/2005/0232).

CONTENT: the VIS shall improve the implementation of the common visa policy, consular cooperation and consultation between central visa authorities by facilitating the exchange of data between Member States on applications and on the decisions relating thereto, in order to facilitate the visa application procedure, to prevent 'visa shopping', to facilitate the fight against fraud and to facilitate checks at external border crossing points and within the territory of the Member States.

The VIS should also assist in the identification of any person who may not, or may no longer, fulfil the conditions for entry to, stay or residence on the territory of the Member States, and facilitate the application of Council Regulation (EC) No 343/2003 (Dublin II) establishing the criteria and mechanism for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national and contribute to the prevention of threats to the internal security of any of the Member States.

Subject matter and scope: this Regulation defines the purpose of, the functionalities of and the responsibilities for the Visa Information System (VIS), as established Decision 2004/512/EC. It sets up the conditions and procedures for the exchange of data between Member States on applications for short-stay visas and on the decisions taken in relation thereto, including the decision whether to annul, revoke or extend the visa, to facilitate the examination of such applications and the related decisions.

Categories of data:the Regulation governing the VIS allows the competent authorities (in particular visa, border and immigration agencies) to store in a central European database alphanumeric and biometric data on visa applicants and visas which have been issued, denied or revoked, and retrieve the data concerned. This enables them to prevent what is referred to as visa shopping, and to identify applications by the same person under different names.

Onlythe following categories of data shall be recorded in the VIS:

a) alphanumeric data on the applicant and on visas requested, issued, refused, annulled, revoked or extended;

b) photographs;

c) fingerprint data;

d) links to other applications as set out in this Regulation.

Access for entering, amending, deleting and consulting data: access to the VIS for entering, amending or deleting the data shall be reserved exclusively to the duly authorised staff of the visa authorities. Access to the VIS for consulting the data shall be reserved exclusively to the duly authorised staff of the authorities of each Member State which are competent for the purposes laid down in the Regulation, limited to the extent that the data are required for the performance of their tasks.

Each Member State shall designate the competent authorities, the duly authorised staff of which shall have access to enter, amend, delete or consult data in the VIS. Each Member State shall without delay communicate to the Commission a list of these authorities. That list shall specify for what purpose each authority may process data in the VIS.

Availability of data for the prevention, detection and investigation of terrorist offences and other serious criminal offences: the designated authorities of the Member States may in a specific case and following a reasoned written or electronic request access the data kept in the VIS if there are reasonable grounds to consider that consultation of VIS data will substantially contribute to the prevention, detection or investigation of terrorist offences and of other serious criminal offences. Europol may access the VIS within the limits of its mandate and when necessary for the performance of its tasks.

The consultation shall be carried out through central access point(s) which shall be responsible for ensuring strict compliance with the conditions for access and the procedures established in Council Decision 2008/633/JHA concerning access for consultation of the Visa Information System (VIS) by the 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.

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.

General principles applicable to the VIS: each competent authority authorised to access the VIS in accordance with this Regulation shall ensure that the use of the VIS is necessary, appropriate and proportionate to the performance of the tasks of the competent authorities. They shall ensure that in

using the VIS, it does not discriminate against applicants and visa holders on grounds of sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation and that it fully respects the human dignity and the integrity of the applicant or of the visa holder.

The Regulation also defines the rules applicable to:

1) **The entry and use of data by visa authorities**: provisions are set out as regards procedures to be respected by the competent authorities as regards entering data upon the application; data upon lodging the application; data to be added for a visa issued; data to be added where the examination of the application is discontinued; data to be added for a visa refusal; data to be added for a visa annulled or revoked or with a shortened validity period; data to be added for a visa extended, etc.

2) **The access to data by other authorities**: the Regulation lays down the procedures to be respected as regards the access to for verification at external border crossing points; within the Member States; access to data for determining the responsibility for asylum applications and examining the application for asylum; etc.

3) **Retention and amendment of the data**: each application file shall be stored in the VIS for a **maximum of five years**. Upon expiry of this, the VIS shall automatically delete the application file and the links to this file.

4) **Operation and responsibilities**: after a transitional period, which should not exceed 5 years from the date of entry into force, the Commission shall be responsible for the operational management of the central VIS and the national interfaces and shall ensure, in cooperation with the Member States, that at all times the best available technology, subject to a cost-benefit analysis, is used for the central VIS and the national interfaces. The Commission may delegate that task and tasks relating to implementation of the budget, to national public-sector bodies in two different Member States. Prior to any delegation and at regular intervals thereafter, the Commission shall inform the European Parliament and the Council of the terms of the delegation, its precise scope, and the bodies to which tasks are delegated. The principal central VIS, which performs technical supervision and administration functions, shall be located in Strasbourg (France) and a back-up central VIS, capable of ensuring all functionalities of the principal central VIS in the event of failure of the system, shall be located in Sankt Johann im Pongau (Austria). The VIS shall be connected to the national system of each Member State via the national interface in the Member State concerned. Each Member State shall designate a national authority, which shall provide the access of the competent authorities to the VIS, and connect that national authority to the national interface. They shall observe automated procedures for processing the data and shall be responsible for the development of the national system and/or its adaptation to the VIS; the organisation, management, operation and maintenance of its national system; the management and arrangements for access of the duly authorised staff of the competent national authorities to the VIS in accordance with this Regulation and to establish and regularly update a list of such staff and their profiles; bearing the costs incurred by the national system and the costs of their connection to the national interface, including the investment and operational costs of the communication infrastructure between the national interface and the national system. Appropriate training shall be given to staff about data security and data protection rules and shall be informed of any relevant criminal offences and penalties. Each Member State shall ensure that the data are processed lawfully, and in particular that only duly authorised staff have access to data processed in the VIS for the performance of their tasks. Data processed in the VIS pursuant to this Regulation shall not be transferred or made available to a third country or to an international organisation (except in the case of urgent situations an under certain conditions).

5) **Rights and supervision on data protection**: a number of measures aim to protect individuals with regards to the processing of data. Member States shall cooperate actively to enforce the rights laid down in this Regulation. Any person may request that data relating to him which are inaccurate be corrected and that data recorded unlawfully be deleted. The correction and deletion shall be carried out without delay by the Member State responsible, in accordance with its laws, regulations and procedures. In each Member State, the national supervisory authority shall, upon request, assist and advise the person concerned in exercising his right to correct or delete data relating to him in accordance with Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The National Supervisory Authority of the Member State responsible which transmitted the data and the National Supervisory Authorities of the Member States with which the request was lodged shall cooperate to this end.

Remedies: it is provided that 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.

Regulation (EC) No 45/2001 of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data applies to the activities of the Community institutions or bodies when carrying out their tasks as responsible for the operational management of the VIS.

Territorial application: the Regulation sets out conditions for the participation to the VIS by certain Member States which do not normally participate in the common visa policy (United Kingdom and Ireland which will not be associated with the implementation of the VIS) or for countries associated with the implementation of Schengen (Iceland, Norway and Switzerland). Denmark does not take part in the adoption of this Regulation and is therefore not bound by it or subject to its application. Given that this Regulation builds upon the Schengen acquis, Denmark should decide within a period of six months after the adoption of this Regulation whether it will implement it in its national law.

Start of operations: the Commission shall determine the date from which the VIS is to start operations, when specific measures have been adopted; the Commission has declared the successful completion of a comprehensive test of the VIS, which shall be conducted by the Commission together with Member States; following validation of technical arrangements, the Member States have notified the Commission that they have made the necessary technical and legal arrangements.

Monitoring and evaluation: the Management Authority shall ensure that procedures are in place to monitor the functioning of the VIS against objectives relating to output, cost-effectiveness, security and quality of service. Reports shall be submitted every 2 years after the VIS is brought into operation on the technical functioning of the VIS, including the security thereof. 3 years after the VIS is brought into operation and every 4 years thereafter, the Commission shall produce an overall evaluation of the VIS.

ENTRY INTO FORCE: 2 September 2008. The Regulation shall apply from the date determined by the Commission from which the VIS is to start operations.

Visa Information System (VIS) and exchange of data between Member States on short-stay visas (VIS Regulation)

2004/0287(COD) - 23/03/2005 - Document attached to the procedure

OPINION OF THE EUROPEAN DATA PROTECTION SUPERVISOR

Given the sensitive nature of storing personal information on the Visa Information System, the European Data Protection Officer has been asked to give his opinion on the proposed legislative act. On balance, the EDPS approves of the VIS and recognises the need for creating a harmonised system of storing visa information, managed centrally by the EU. The report prepared by the EDPS states that, from a data protection point of view, the provisions have been drafted with due care and seem to be consistent and adequate as a whole. In spite of supporting the overall objective of the proposed legislative act, the EDPS has nevertheless identified a number of key concerns, regarding certain aspects of the proposed provisions, which are outlined below.

When examining the proposal, the EDPS took respect for an “individual’s private life” as the main point of reference for future discussions. Bearing this key principle in mind, the EDPS made the following observations:

- The VIS should be limited to the collection and exchange of data necessary for the development of a common visa policy. The information collected should be proportionate to this goal.

- The purpose of the VIS should be limited. This should be reflected in its content and who is authorised to use the system. Law enforcement agencies should not be given ‘routine’ access to the VIS given that it would not be in accordance with the stated purpose of the VIS (i.e. a common visa policy). The law enforcement authorities should be granted access on an *ad hoc* basis, under specific circumstances only and subject to the appropriate safeguards.

- The EDPS recognises the value and potential importance of using biometrics for storing information on an individual. Nevertheless, the Report highlights a number of fault lines associated with biometrics that indicate they can have far reaching consequences for individuals and society as a whole. Biometrics, for example, irrevocably alter the relationship between body and identity, in that they make the characteristics of the human body ‘machine-readable’ and subject to further use. Revocation of biometric data is almost impossible – a finger or face is difficult to change. Although this offers a number of possibilities for Member States’ authorities it also needs to be examined from the point of view of ‘identity theft’. The storage of fingerprints and photographs in a database linked to a stolen ID could lead to permanent problems for the real owner of his/her identity. Moreover, by its very nature, biometric data is not secret and can leave traces (fingerprints, DNA), which allows for the collection of this data – without the owner ever being made aware of this. For its part, the EDPS is concerned that the present proposal is being considered in the absence of a more widespread debate on biometrics. As a result one of the main recommendations of the EDPS is the introduction of more **stringent safeguards** for the use of biometric data in the proposed Regulation. These safeguards should be linked to the principle of limiting the information stored, restricting access to its content and boosting VIS security measures.

- The EDPS also makes some interesting comments regarding the technical imperfection of biometrics. Whilst it acknowledges that biometrics offers a number of advantages, some of the advantages, such as data universality, permanence and usability, are never absolute. It is estimated that up to 5% of people would not be able to enrol on the system because they have no readable fingerprints – or no finger prints at all. The impact assessment report suggests that in 2007 there could be up to 20 million visa applicants. Were this to be the case, up to one million people will not be able to follow the normal enrolment process, with obvious consequences for visa applications and border checking. Further, given that biometrics can have an error rate of 0.5 to 1%, the EDPS points out that as a technology it can never offer an ‘exact identification’ of the data subject – as is suggested in the proposed Regulation. In light of this, the EDPS recommends that fallback procedures are developed and included in the proposal.

- On the matter of refusing a visa, the EDPS raises some concern over public health issues. The proposed provision, which would make public health a condition for entry, is considered by the EDPS as too vague.

- The EDPS calls for a precise and comprehensive definition of ‘group members’.

- Regarding the matter of retaining data, the EDPS concludes that the provisions outlined in the proposed Regulation are reasonable. It must, however, be made explicit in the proposal that personal data must be entirely re-assessed for each new visa application.

- The EDPS points out that once the verification of identity has succeeded at border points, the Regulation does not make it clear for why further data is still needed.

- The EDPS calls for the creation of a complete list of user identities, which are to be kept permanently up-to-date by the Member States.

- Concerning the rights of the Data subject, the EDPS requests that data subjects should be informed about the retention period applying to their data.

- The EDPS requests an annual meeting with the national supervisory bodies of the VIS at least once a year; that technological implementation of data protection technologies should be done by way of a Regulation in accordance with the co-decision procedure and lastly, that the EDPS should be allowed to give advice on the Regulation's committee.

To conclude, the EDPS calls on all of the institutions involved in formulating the proposed Regulation to give due consideration to some of the issues it raises in this opinion, prior to its final adoption.

Visa Information System (VIS) and exchange of data between Member States on short-stay visas (VIS Regulation)

2004/0287(COD) - 07/03/2005

The Council adopted the following conclusions on the access to the VIS by Member State authorities responsible for internal security:

- it considers that in order to achieve fully the aim of improving internal security and the fight against terrorism which the Council assigned to the VIS in its conclusions of 19 February 2004, access, for the purpose of consultation, should be guaranteed to Member State authorities responsible for internal security in the course of their duties in relation to the prevention, detection and investigation of criminal offences, including terrorist acts and threats;

- it reiterates that any access to the VIS must be subject to strict compliance with the rules governing the protection of personal data;

- it invites the Commission to present as soon as possible, and by the end of 2005 at the latest, its proposal on the protection of personal data within the framework of Title VI of the TEU;

- it requests the Commission to present, at the same time, a proposal based on Title VI of the TEU aimed at guaranteeing Member State authorities responsible for internal security access to the VIS for the purpose of consultation in the course of their duties in relation to the prevention, detection and investigation of criminal offences, including terrorist acts and threats, with a view to its adoption within the same timeframe as of the Regulation on the VIS;

- it requests that, in the meantime, examination of the proposal for a Regulation on the visa information system (VIS) and the exchange of data between Member States on short-stay visas should continue;

- it will make every effort, together with the European Parliament, and with full respect for each institution's prerogatives, to adopt the proposal for a Regulation on the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas within a timeframe enabling the VIS to be implemented in accordance with the timetable set by the Council in its conclusions of 19 February 2004.

Visa Information System (VIS) and exchange of data between Member States on short-stay visas (VIS Regulation)

2004/0287(COD) - 28/12/2004 - Legislative proposal

PURPOSE : to set up a common system and common procedures for the exchange of visa data between Member States.

PROPOSED ACT : Regulation of the European Parliament and of the Council.

CONTENT : the present proposal aims to give the Commission the mandate to set up, maintain and operate the VIS and defines the purpose, functionalities and responsibilities for the Visa Information System and the procedures and conditions for the exchange of visa data between Member States on short-stay visa applications to facilitate the examination of such applications and the related decisions. This second legal instrument has been elaborated on the basis of the political orientation given by the Council conclusions of 19 February 2004. The financial statement for this legal instrument relates, in particular, to the costs for processing biometrics, phase 2 of the VIS.

The VIS has two main goals: contributing to the internal security of the Member States and the fight against illegal immigration by supporting the common visa policy and the checks on the visa applicants, thereby facilitating bona fide travelling in the Schengen area without internal borders.

The data to be processed in the VIS shall include alphanumeric data and photographs, but also fingerprint data of the applicants, to ensure exact verification and identification. In particular, the clear definition of access rights and the purposes for which the data may be consulted and the responsibilities for the use of the data and supervision shall ensure a high level of data protection.

The VIS shall improve the administration of the common visa policy, the consular cooperation and the consultation between central consular authorities in order to prevent threats to internal security and 'visa shopping', to facilitate the fight against fraud and checks at external border checkpoints and within the territory of the Member States, to assist in the identification and return of illegal immigrants and to:

- facilitate the application of the "Dublin II Regulation" 343/2003/EC. The improvement of the assessment of visa applications including the consultation between central authorities, and the verification and identification of applicants at consulates and at checkpoints contributes to the internal security of the Member States and towards combating terrorism, which constitutes a horizontal objective and basic criterion for the common visa policy, as well as the fight against illegal immigration. Simultaneously, the VIS will benefit bona fide travellers by improving the procedures for issuing visas and for checks.

The scope of this Regulation is related to the exchange of data on Schengen short- stay visas as the primary purpose of the VIS, including the national long-stay visas which are concurrently valid as short-stay visas. The exchange of data on other national long-stay visa of the Schengen States, which is also included in the Council conclusions of 19 February 2004, requires a separate legal instrument: Other than for the short-term visas there exists no common aquis on procedures on the issue of long-term visas by Member States.

This draft Regulation shall constitute the core instrument for the legal framework for the VIS. However, to complement this legal framework, further legal instruments will be needed in particular for:

- amending the Common Consular Instructions (CCI), concerning standards and procedures for taking the biometric data, including the obligation and specifying the exceptions to the recording of biometrics;

- the development of a mechanism for the exchange of data with Ireland and the United Kingdom for the purposes to facilitate the application of the Dublin II Regulation 343/2003/EC and to assist in the identification and administrative procedures for returning of illegal immigrants, as far as Ireland and the UK participate in immigration and return policy;

- the exchange of data on long stay-visas which are not concurrently valid as short-stay visas by the VIS; this would need further political orientation in view of the absence of a common aquis for such visas.

Since the Regulation covers the exchange of data on short stay visas between Member States "which have abolished checks at their internal borders", it constitutes a development of the Schengen acquis on the common visa policy. The consequences for the participation in the VIS are as follows:

- Iceland and Norway: the procedures laid down in the Association Agreement concluded by the Council and the Republic of Iceland and the Kingdom of Norway concerning the latters' association with the implementation, application and development of the Schengen acquis are applicable, since the present proposal builds on the Schengen acquis as defined in Annex A of this Agreement.

- Denmark: Denmark will not participate in the adoption of the Regulation and is therefore not bound by it or subject to its application.

- United Kingdom and Ireland: the United Kingdom and Ireland are not taking part in the adoption of the Regulation and are not bound by it or subject to its application.

- New Member States: Since the initiative constitutes an act building upon the Schengen acquis or otherwise related to it within the meaning of Article 3 (2) of the Act of Accession, the Regulation shall only apply in a new Member State pursuant to a Council decision in conformity with this provision.

- Switzerland: This Regulation constitutes a development of the provisions of the Schengen aquis within the meaning of the Agreement signed by the European Community and Switzerland on the latter's association with the implementation, application and development of the Schengen acquis which fall within the area referred to in Article 4(1) of the Council decision on the signing, on behalf of the European Community, and on the provisional application of certain provisions of this Agreement.

FINANCIAL STATEMENT :

- Budget lines and headings : 18.08.03 Visa Information System.

- Total allocation for action (Part B): EUR 97 million for commitment until 2013.

- Period of application: Undetermined duration. Foreseen for 2007-2013: investment costs for biometric processing: EUR 64 million; exploitation costs for biometric processing: EUR 33 million. The amounts foreseen for the period 2007-2013 are subject to the adoption of the new financial perspectives.

- Overall financial impact of human resources and other administrative expenditure: EUR 216.000 per annum with 2 permanent posts.

Visa Information System (VIS) and exchange of data between Member States on short-stay visas (VIS Regulation)

2004/0287(COD) - 28/12/2004 - Document attached to the procedure

COMMISSION'S IMPACT ASSESSMENT

1. PROBLEM IDENTIFICATION:

At present there are 134 third countries whose citizens are required to have a visa issued by a Member State to enter the territory of Schengen States. Visas are issued by Member States separately, and the absence of a joint information processing centre has left the system open to abuse.

Other problems increase the need for a centralised visa information system:

- the existing arrangements for the exchange of visa data between Member States are slow, can be inaccurate and are not comprehensive;

- it is often difficult to check that a visa applicant is not using a false identity or stolen travel documents;

- an applicant who is refused a visa by one Schengen country can apply to others (visa shopping) and there is no formal information system for the authorities to check multiple applications;

- Member States dealing with asylum applications do not have efficient means to check whether the applicants have been issued with visas by other Member States; and

- inefficiencies in dealing with visa shopping and fraud make it more difficult to prevent and detect terrorists and members of organised crime groups.

For more information regarding the context of this paper, please refer to the summary of the Commission's initial proposal COM(2004)0835.

2. OBJECTIVE:

The establishment of the Visa Information System (VIS) represents one of the key initiatives within the EU policies aimed at supporting stability and security. Given the potential for a significant impact arising from action in this field, the Commission, in its Annual Policy Strategy for 2004, decided that an Extended Impact Assessment should be carried out. This paper focused on the estimation of the potential impacts of various options under consideration for the VIS. Economic/financial impacts were taken into account as well as social/political ones. Furthermore, proportionality aspects of the storage and the use of data as well as data protection issues have been considered.

This paper highlights the need for the VIS and its impacts in comparison to other policy options. It explains, in particular, why the storage and use of biometric data is essential to achieve the objectives of the VIS and identifies the appropriate safeguards for data protection and data security.

3. POLICY OPTIONS AND IMPACTS:

3.1 - **Option 1***: no VIS :*this option would not create improvements in exchanges of visa application information between consular authorities of Member States. The absence of a visa information exchange system would not address some of the most pressing issues, such as visa shopping and visa fraud;

3.2 - **Option 2***: entry-exit system to obtain and check biometric and other data on visitors when they enter and leave the country:* the main aims of an entry-exit system would be to enable people arriving and departing to be examined, and for appropriate information - which is relevant to their immigration and residence status - to be gathered. This information is also stored in the central database. People who overstay their visas would also be identified in this part of the system. In principle, an entry-exit system would be a computerised system for collecting personal details of all visa holders entering and exiting Schengen territory.

An EU entry-exit system, incorporating biometrics for visa applicants, would provide a continuum of measures to control the movements of third country nationals, from a visa application stage through arrival at an external border to leaving the territory of the Schengen states. Such a system would enable much more efficient and effective border controls to be operated. There would also be improvement to immigration control arrangements, overall, due to the existence of more comprehensive records. However, it would be extremely costly to implement.

Moreover, opportunity costs for visa applicants can be expected, as applicants would have to travel to consular posts to provide biometric data. Furthermore, time will be lost at entry and exit points by providing and checking biometric data. The study comes to the conclusion that opportunity costs in this option are higher than the opportunity costs in a VIS with biometrics (Option 4).

In addition, the impact of entry-exit system on human rights would be extensive, and there would be a substantial need to meet personal data protection and data security requirements in particular in view of the use of biometrics, since there would be a risk of misuse.

Considerable reductions in visa fraud (and some reduction in other document fraud) can be anticipated, as well as in visa shopping.

There would be substantial advantages for bona-fide travellers requiring visas as past visa history could be established in the same way as a VIS with biometrics.This would be especially beneficial for regular travellers, who make repeated applications for Schengen visas. The entry-exit system would provide a big stimulus for IT industries.

3.3 - **Option 3***: to set up VIS without biometric data:* a Visa Information System without biometrics would be an electronic system containing information about the visa applicant taken from the visa application form and the decisions hereto, as well as the photograph of the applicant, introduced as a security feature in the uniform sticker for the Schengen visas. Access to enter and update visa data would be granted to persons authorised to be involved in the visa issuing process or in the process to annul, revoke and extend visas. These authorities would also have access for the purposes of consultation. Provided that visa data is required for the performance of their tasks, other authorities with responsibility for controlling border checkpoints as well as other competent authorities of each Member State would have access in accordance with the purposes of the VIS.

This system would ensure improvement of consular cooperation but would have little impact as a contribution towards internal security and fight against terrorism and on the fight against illegal immigration. Furthermore, bona fide travellers would benefit to a small extent from a VIS without biometrics as there would be just some improvements in the visa issuing process but no improvement in case of lost or stolen travel documents as they could not provetheir identity quickly.

3.4 - **Option 4***: to set up VIS with biometric data:* a Visa Information System with biometrics would contain all the information envisaged in a VIS without biometrics (and the same access and consultation procedures), but, crucially, it will also include biometric information of visa applicants, such as fingerprints. The choice of the biometric identifier should follow a coherent approach for documents and databases. Even if the biometric technology changes, fingerprint databases will still be used for a long time. Background checks to prevent threats to internal security can be done with fingerprints, contrary to, for example, iris technology. Further development at a later stage might enable the use of photographs for facial recognition.

The paper highlights that, in a large database, it is not possible to identify persons with alphanumeric data alone. Even for bona-fide travellers, the spelling of the same name can be different from one country to another, many instances of the same name exist and, in some countries, dates of births are not completely known. Identifying undocumented persons or persons is virtually impossible without biometrics.

Inclusion of biometric data in the VIS would not only significantly support the assessment of applicants in view of preventing 'visa shopping', fraud and threats to internal security, but would have positive consequences for bona-fide travellers. Matches against biometric data would help to verify their identity in case of a new application or at checks, but also in case of lost or stolen travel documents as bona-fide travellers could quickly prove their identity to get new travel documents and visas. Moreover, the inclusion of biometric data would also significantly support the identification of undocumented illegal immigrants and the return procedures, if these illegal immigrants have once applied for a visa.

It should, however, be noted that this option would entail very significant financial costs. Due to opportunity costs for visa applicants and the perceived invasion of privacy and human rights, some reductions in business travel and tourism might be anticipated.

CONCLUSION: The assessment highlights the need for the VIS and points out that, in spite of high costs and data protection issues, the storage and use of **biometric data is essential to achieve the objectives of the system. Therefore, Option 4 has been chosen as it closely meets the objectives and purposes outlined by the Council in February 2004.**

4. FOLLOW-UP: The effective monitoring of the VIS requires evaluation in regular intervals. For these purposes, it is necessary that systems are in place to monitor the functioning of the VIS against objectives, in terms of outputs, cost-effectiveness and quality of service. ***It is recommended that every 2 years a report on the technical functioning of the VIS should be submitted to the European Parliament and the Council.*** This report should include information on the performance of the VIS against quantitative indicators predefined by the Commission. ***Moreover, an overall evaluation of the VIS*** should be produced, including examining results achieved against objectives and assessing the continuing validity of the underlying rationale and any implications of future options.