REGULATION (EC) No 767/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 9 July 2008

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 62(2)(b)(ii) and Article 66 thereof,

Having regard to the proposal from the Commission,

Acting in accordance with the procedure laid down in Article 251 of the Treaty ([1]),

Whereas:

(1) Building upon the conclusions of the Council of 20 September 2001, and the conclusions of the European Council in Laeken in December 2001, in Seville in June 2002, in Thessaloniki in June 2003 and in Brussels in March 2004, 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.

(2) Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS) ([2]) established the VIS as a system for the exchange of visa data between Member States.

(3) 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 to facilitate the examination of visa applications and related decisions, taking into account the orientations for the development of the VIS adopted by the Council on 19 February 2004 and to give the Commission the mandate to set up the VIS.

(4) For a transitional period, the Commission should be responsible for the operational management of the central VIS, of the national interfaces and of certain aspects of the communication infrastructure between the central VIS and the national interfaces. In the long term, and following an impact assessment containing a substantive analysis of alternatives from a financial, operational and organisational perspective, and legislative proposals from the Commission, a permanent Management Authority with responsibility for these tasks should be established. The transitional period should last for no more than five years from the date of entry into force of this Regulation.

(5) The VIS should have the purpose of improving 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 of 18 February 2003 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 ([3]), and contribute to the prevention of threats to the internal security of any of the Member States.

(6) This Regulation is based on the *acquis* of the common visa policy. The data to be processed by the VIS should be determined on the basis of the data provided by the common form for visa applications as introduced by Council Decision 2002/354/EC of 25 April 2002 on the adaptation of Part III of, and the creation of an Annex 16 to, the Common Consular Instructions ([4]), and the information on the visa sticker provided for in Council Regulation (EC) No 1683/95 of 29 May 1995 laying down a uniform format for visas ([5]).

(7) The VIS should be connected to the national systems of the Member States to enable the competent authorities of the Member States to process data on visa applications and on visas issued, refused, annulled, revoked or extended.

([1]) Opinion of the European Parliament of 7 June 2007 (OJ C 125 E, 22.5.2008, p. 118) and Council Decision of 23 June 2008.

([2]) OJ L 213, 15.6.2004, p. 5.

([3]) OJ L 50, 25.2.2003, p. 1.

([4]) OJ L 123, 9.5.2002, p. 50.

([5]) OJ L 164, 14.7.1995, p. 1. Regulation as last amended by Regulation (EC) No 1791/2006 (OJ L 363, 20.12.2006, p. 1).

(8) The conditions and procedures for entering, amending, deleting and consulting the data in the VIS should take into account the procedures laid down in the Common Consular Instructions on visas for the diplomatic missions and consular posts ([1]) (the Common Consular Instructions).

(9) The technical functionalities of the network for consulting the central visa authorities as laid down in Article 17(2) of the Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders ([2]) (the Schengen Convention) should be integrated into the VIS.

(10) To ensure reliable verification and identification of visa applicants, it is necessary to process biometric data in the VIS.

(11) It is necessary to define the competent authorities of the Member States, the duly authorised staff of which are to have access to enter, amend, delete or consult data for the specific purposes of the VIS in accordance with this Regulation to the extent necessary for the performance of their tasks.

(12) Any processing of VIS data should be proportionate to the objectives pursued and necessary for the performance of the tasks of the competent authorities. When using the VIS, the competent authorities should ensure that the human dignity and integrity of the persons whose data are requested are respected and should not discriminate against persons on grounds of sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation.

(13) This Regulation should 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.

(14) The personal data stored in the VIS should be kept for no longer than is necessary for the purposes of the VIS. It is appropriate to keep the data for a maximum period of five years, in order to enable data on previous applications to be taken into account for the assessment of visa applications, including the applicants' good faith, and for the documentation of illegal immigrants who may, at some stage, have applied for a visa. A shorter period would not be sufficient for those purposes. The data should be deleted after a period of five years, unless there are grounds to delete them earlier.

(15) Precise rules should be laid down as regards the responsibilities for the establishment and operation of the VIS, and the responsibilities of the Member States for the national systems and the access to data by the national authorities.

(16) Rules on the liability of the Member States in respect of damage arising from any breach of this Regulation should be laid down. The liability of the Commission in respect of such damage is governed by the second paragraph of Article 288 of the Treaty.

(17) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ([3]) applies to the processing of personal data by the Member States in application of this Regulation. However, certain points should be clarified in respect of the responsibility for the processing of data, of safeguarding the rights of the data subjects and of the supervision on data protection.

(18) Regulation (EC) No 45/2001 of the European Parliament and the Council of 18 December 2000 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 ([4]) applies to the activities of the Community institutions or bodies when carrying out their tasks as responsible for the operational management of the VIS. However, certain points should be clarified in respect of the responsibility for the processing of data and of the supervision of data protection.

(19) The National Supervisory Authorities established in accordance with Article 28 of Directive 95/46/EC should monitor the lawfulness of the processing of personal data by the Member States, while the European Data Protection Supervisor as established by Regulation (EC) No 45/2001 should monitor the activities of the Community institutions and bodies in relation to the processing of personal data, taking into account the limited tasks of the Community institutions and bodies with regard to the data themselves.

([1]) OJ C 326, 22.12.2005, p. 1. Instructions as last amended by Council Decision 2006/684/EC (OJ L 280, 12.10.2006, p. 29).

([2]) OJ L 239, 22.9.2000, p. 19. Convention as last amended by Regulation (EC) No 1987/2006 of the European Parliament and of the Council (OJ L 381, 28.12.2006, p. 4).

([3]) OJ L 281, 23.11.1995, p. 31. Directive as amended by Regulation (EC) No 1882/2003 (OJ L 284, 31.10.2003, p. 1).

([4]) OJ L 8, 12.1.2001, p. 1.

(20) The European Data Protection Supervisor and the National Supervisory Authorities should cooperate actively with each other.

(21) The effective monitoring of the application of this Regulation requires evaluation at regular intervals.

(22) The Member States should lay down rules on penalties applicable to infringements of the provisions of this Regulation and ensure that they are implemented.

(23) The measures necessary for the implementation of this Regulation should be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission ([1]).

(24) This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union.

(25) Since the objectives of this Regulation, namely the establishment of a common Visa Information System and the creation of common obligations, conditions and procedures for the exchange of visa data between Member States, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and impact of the action, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.

(26) In accordance with Articles 1 and 2 of the Protocol on the position of Denmark, annexed to the Treaty on European Union and the Treaty establishing the European Community, 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* under the provisions of Title IV of Part Three of the Treaty establishing the European Community, Denmark should, in accordance with Article 5 of that Protocol, decide within a period of six months after the adoption of this Regulation whether it will implement it in its national law.

(27) As regards Iceland and Norway, this Regulation constitutes a development of provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis* ([2]), which falls within the area referred to in Article 1, point B of Council Decision 1999/437/EC ([3]) of 17 May 1999 on certain arrangements for the application of that Agreement.

(28) An arrangement should be made to allow representatives of Iceland and Norway to be associated with the work of committees assisting the Commission in the exercise of its implementing powers. Such an arrangement has been contemplated in the Agreement in the form of Exchange of Letters between the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning committees which assist the European Commission in the exercise of its executive powers ([4]), annexed to the Agreement referred to in Recital 27.

(29) This Regulation constitutes a development of provisions of the Schengen *acquis* in which the United Kingdom does not take part, in accordance with Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis* ([5]), and subsequent Council Decision 2004/926/EC of 22 December 2004 on the putting into effect of parts of the Schengen *acquis* by the United Kingdom of Great Britain and Northern Ireland ([6]). The United Kingdom is therefore not taking part in its adoption and is not bound by it or subject to its application.

(30) This Regulation constitutes a development of provisions of the Schengen *acquis* in which Ireland does not take part, in accordance with Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen *acquis* ([7]). Ireland is therefore not taking part in its adoption and is not bound by it or subject to its application.

(31) As regards Switzerland, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement signed by the European Union, the European Community and the Swiss Confederation on the association of the Swiss Confederation with the implementation, application and development

([1]) OJ L 184, 17.7.1999, p. 23. Decision as amended by Decision 2006/512/EC (OJ L 200, 22.7.2006, p. 11).

([2]) OJ L 176, 10.7.1999, p. 36.
([3]) OJ L 176, 10.7.1999, p. 31.
([4]) OJ L 176, 10.7.1999, p. 53.
([5]) OJ L 131, 1.6.2000, p. 43.
([6]) OJ L 395, 31.12.2004, p. 70.
([7]) OJ L 64, 7.3.2002, p. 20.

of the Schengen *acquis* which falls within the area referred to in Article 1, point B of Decision 1999/437/EC read in conjunction with Article 4(1) of Council Decision 2004/860/EC [1].

(32) An arrangement should be made to allow representatives of Switzerland to be associated with the work of committees assisting the Commission in the exercise of its implementing powers. Such an arrangement has been contemplated in the Exchange of Letters between the Community and Switzerland, annexed to the Agreement referred to in Recital 31.

(33) This Regulation constitutes an act building on the Schengen *acquis* or otherwise related to it within the meaning of Article 3(2) of the 2003 Act of Accession and Article 4(2) of the 2005 Act of Accession,

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and scope

This Regulation defines the purpose of, the functionalities of and the responsibilities for the Visa Information System (VIS), as established by Article 1 of 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.

Article 2

Purpose

The VIS shall have the purpose of improving 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:

(a) to facilitate the visa application procedure;

(b) to prevent the bypassing of the criteria for the determination of the Member State responsible for examining the application;

(c) to facilitate the fight against fraud;

(d) to facilitate checks at external border crossing points and within the territory of the Member States;

(e) to 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;

(f) to facilitate the application of Regulation (EC) No 343/2003;

(g) to contribute to the prevention of threats to the internal security of any of the Member States.

Article 3

Availability of data for the prevention, detection and investigation of terrorist offences and other serious criminal offences

1. 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 referred to in Articles 9 to 14 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.

2. The consultation referred to in paragraph 1 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 of 23 June 2008 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 [2]. 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. In an exceptional case of urgency, the central access point(s) may receive written, electronic or oral requests and only verify *ex-post* whether all the conditions for access 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.

3. Data obtained from the VIS pursuant to the Decision referred to in paragraph 2 shall not be transferred or made available to a third country or to an international organisation.

[1] Decision 2004/860/EC of 25 October 2004 on the signing, on behalf of the European Community, and on the provisional application of certain provisions of the Agreement between the European Union, the European Community and the Swiss Confederation, concerning the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L 370, 17.12.2004, p. 78).

[2] See page 129 of this Official Journal.

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 that Decision. In accordance with national law, Member States shall ensure that records on such transfers are kept and make them available to national data protection authorities on request. The transfer of data by the Member State which entered the data in the VIS shall be subject to the national law of that Member State.

4. This Regulation is without prejudice to any obligations under applicable national law for the communication of information on any criminal activity detected by the authorities referred to in Article 6 in the course of their duties to the responsible authorities for the purposes of preventing, investigating and prosecuting the related criminal offences.

Article 4

Definitions

For the purposes of this Regulation, the following definitions shall apply:

1. 'visa' means:

   (a) 'short-stay visa' as defined in Article 11(1)(a) of the Schengen Convention;

   (b) 'transit visa' as defined in Article 11(1)(b) of the Schengen Convention;

   (c) 'airport transit visa' as defined in part I, point 2.1.1, of the Common Consular Instructions;

   (d) 'visa with limited territorial validity' as defined in Articles 11(2), 14 and 16 of the Schengen Convention;

   (e) 'national long-stay visa valid concurrently as a short-stay visa' as defined in Article 18 of the Schengen Convention;

2. 'visa sticker' means the uniform format for visas as defined by Regulation (EC) No 1683/95;

3. 'visa authorities' means the authorities which in each Member State are responsible for examining and for taking decisions on visa applications or for decisions whether to annul, revoke or extend visas, including the central visa authorities and the authorities responsible for issuing visas at the border in accordance with Council Regulation (EC) No 415/2003 of 27 February 2003 on the issue of visas at the border, including the issue of such visas to seamen in transit ([1]);

4. 'application form' means the uniform application form for visas in Annex 16 to the Common Consular Instructions;

5. 'applicant' means any person subject to the visa requirement pursuant to Council Regulation (EC) No 539/2001 of 15 March 2001 listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement ([2]), who has lodged an application for a visa;

6. 'group members' means applicants who are obliged for legal reasons to enter and leave the territory of the Member States together;

7. 'travel document' means a passport or other equivalent document entitling the holder to cross the external borders and to which a visa may be affixed;

8. 'Member State responsible' means the Member State which has entered the data in the VIS;

9. 'verification' means the process of comparison of sets of data to establish the validity of a claimed identity (one-to-one check);

10. 'identification' means the process of determining a person's identity through a database search against multiple sets of data (one-to-many check);

11. 'alphanumeric data' means data represented by letters, digits, special characters, spaces and punctuation marks.

Article 5

Categories of data

1. Only the 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 referred to in Articles 9(1) to (4) and Articles 10 to 14;

([1]) OJ L 64, 7.3.2003, p. 1.

([2]) OJ L 81, 21.3.2001, p. 1. Regulation as last amended by Regulation (EC) No 1932/2006 (OJ L 405, 30.12.2006, p. 23).

(b) photographs referred to in Article 9(5);

(c) fingerprint data referred to in Article 9(6);

(d) links to other applications referred to in Article 8(3) and (4).

2. The messages transmitted by the infrastructure of the VIS, referred to in Article 16, Article 24(2) and Article 25(2), shall not be recorded in the VIS, without prejudice to the recording of data processing operations pursuant to Article 34.

Article 6

Access for entering, amending, deleting and consulting data

1. Access to the VIS for entering, amending or deleting the data referred to in Article 5(1) in accordance with this Regulation shall be reserved exclusively to the duly authorised staff of the visa authorities.

2. 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 Articles 15 to 22, limited to the extent that the data are required for the performance of their tasks in accordance with those purposes, and proportionate to the objectives pursued.

3. 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, including those referred to in Article 41(4), and any amendments thereto. That list shall specify for what purpose each authority may process data in the VIS.

Within 3 months after the VIS has become operational in accordance with Article 48(1), the Commission shall publish a consolidated list in the *Official Journal of the European Union*. Where there are amendments thereto, the Commission shall publish once a year an updated consolidated list.

Article 7

General principles

1. 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.

2. 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 holder.

CHAPTER II

ENTRY AND USE OF DATA BY VISA AUTHORITIES

Article 8

Procedures for entering data upon the application

1. On receipt of an application, the visa authority shall create without delay the application file, by entering the data referred to in Article 9 in the VIS, as far as these data are required to be provided by the applicant.

2. When creating the application file, the visa authority shall check in the VIS, in accordance with Article 15, whether a previous application of the individual applicant has been registered in the VIS by any of the Member States.

3. If a previous application has been registered, the visa authority shall link each new application file to the previous application file on that applicant.

4. If the applicant is travelling in a group or with his spouse and/or children, the visa authority shall create an application file for each applicant and link the application files of the persons travelling together.

5. Where particular data are 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 for the purposes of Article 17 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 referred to in Article 50(4).

Article 9

Data upon lodging the application

The visa authority shall enter the following data in the application file:

1. the application number;

2. status information, indicating that a visa has been requested;

3. the authority with which the application has been lodged, including its location, and whether the application has been lodged with that authority representing another Member State;

4. the following data to be taken from the application form:

   (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) place and date of the application;

   (e) type of visa requested;

   (f) details of the person issuing an invitation and/or liable to pay the applicant's subsistence costs during the stay, being:

      (i) in the case of a natural person, the surname and first name and address of the person;

      (ii) in the case of a company or other organisation, the name and address of the company/other organisation, surname and first name of the contact person in that company/organisation;

   (g) main destination and duration of the intended stay;

   (h) purpose of travel;

   (i) intended date of arrival and departure;

   (j) intended border of first entry or transit route;

   (k) residence;

   (l) current occupation and employer; for students: name of school;

   (m) in the case of minors, surname and first name(s) of the applicant's father and mother;

5. a photograph of the applicant, in accordance with Regulation (EC) No 1683/95;

6. fingerprints of the applicant, in accordance with the relevant provisions of the Common Consular Instructions.

Article 10

Data to be added for a visa issued

1. Where a decision has been taken to issue a visa, the visa authority that issued the visa shall add the following data to the application file:

   (a) status information indicating that the visa has been issued;

   (b) the authority that issued the visa, including its location, and whether that authority issued it on behalf of another Member State;

   (c) place and date of the decision to issue the visa;

   (d) the type of visa;

   (e) the number of the visa sticker;

   (f) the territory in which the visa holder is entitled to travel, in accordance with the relevant provisions of the Common Consular Instructions;

   (g) the commencement and expiry dates of the validity period of the visa;

   (h) the number of entries authorised by the visa in the territory for which the visa is valid;

   (i) the duration of the stay as authorised by the visa;

   (j) if applicable, the information indicating that the visa has been issued on a separate sheet in accordance with Council Regulation (EC) No 333/2002 of 18 February 2002 on a uniform format for forms for affixing the visa issued by Member States to persons holding travel documents not recognised by the Member State drawing up the form [1].

2. If an application is withdrawn or not pursued further by the applicant before a decision has been taken whether to issue a visa, the visa authority with which the application was lodged shall indicate that the application has been closed for these reasons and the date when the application was closed.

[1] OJ L 53, 23.2.2002, p. 4.

Article 11

Data to be added where the examination of the application is discontinued

In circumstances where the visa authority representing another Member State is forced to discontinue the examination of the application, it shall add the following data to the application file:

1. status information indicating that the examination of the application has been discontinued;

2. the authority that discontinued the examination of the application, including its location;

3. place and date of the decision to discontinue the examination;

4. the Member State competent to examine the application.

Article 12

Data to be added for a visa refusal

1. Where a decision has been taken to refuse a visa, the visa authority which refused the visa shall add the following data to the application file:

(a) status information indicating that the visa has been refused;

(b) the authority that refused the visa, including its location;

(c) place and date of the decision to refuse the visa.

2. The application file shall also indicate the ground(s) for refusal of the visa, which shall be one or more of the following. The applicant:

(a) has no valid travel document(s);

(b) has a false/counterfeit/forged travel document;

(c) does not justify the purpose and conditions of stay, in particular is considered to represent a specific risk of illegal immigration pursuant to Part V of the Common Consular Instructions;

(d) has already stayed for three months during a six-month period on the territory of the Member States;

(e) does not have sufficient means of subsistence in relation to the period and form of stay, or the means to return to the country of origin or transit;

(f) is a person for whom an alert has been issued for the purposes of refusing entry in the Schengen Information System (SIS) and/or in the national register;

(g) is considered to constitute a threat to public policy, internal security or the international relations of any of the Member States, or to public health, as defined in Article 2 point 19 of Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code) ([1]).

Article 13

Data to be added for a visa annulled or revoked or with a shortened validity period

1. Where a decision has been taken to annul or to revoke a visa, or to shorten the validity period of a visa, the visa authority that has taken the decision shall add the following data to the application file:

(a) status information indicating that the visa has been annulled or revoked or the validity period has been shortened;

(b) authority that annulled or revoked the visa or shortened the validity period of the visa, including its location;

(c) place and date of the decision;

(d) the new expiry date of the validity of the visa, if appropriate;

(e) the number of the visa sticker, if the reduced period takes the form of a new visa sticker.

2. The application file shall also indicate the ground(s) for annulment, revocation or shortening the validity period of the visa, which shall be:

(a) in the case of annulment or revocation, one or more of the grounds listed in Article 12(2);

([1]) OJ L 105, 13.4.2006, p. 1. Regulation as amended by Regulation (EC) No 296/2008 (OJ L 97, 9.4.2008, p. 60).

(b) in the case of a decision to shorten the validity period of the visa, one or more of the following grounds:

(i) for the purposes of the expulsion of the visa holder;

(ii) absence of adequate means of subsistence for the initially intended duration of the stay.

Article 14

Data to be added for a visa extended

1. Where a decision has been taken to extend a visa, the visa authority which extended the visa shall add the following data to the application file:

(a) status information indicating that the visa has been extended;

(b) the authority that extended the visa, including its location;

(c) place and date of the decision;

(d) the number of the visa sticker, if the extension of the visa takes the form of a new visa;

(e) the commencement and expiry dates of the extended period;

(f) period of the extension of the authorised duration of the stay;

(g) the territory in which the visa holder is entitled to travel, in accordance with the relevant provisions of the Common Consular Instructions;

(h) the type of the visa extended.

2. The application file shall also indicate the grounds for extending the visa, which shall be one or more of the following:

(a) force majeure;

(b) humanitarian reasons;

(c) serious occupational reasons;

(d) serious personal reasons.

Article 15

Use of the VIS for examining applications

1. The competent visa authority shall consult the VIS for the purposes of the examination of applications and the decisions relating to those applications, including the decision whether to annul, revoke, extend or shorten the validity of the visa in accordance with the relevant provisions.

2. For the purposes referred to in paragraph 1, the competent visa authority shall be given access to search with one or several of the following data:

(a) the application number;

(b) the data referred to in Article 9(4)(a);

(c) the data on the travel document, referred to in Article 9(4)(c);

(d) the surname, first name and address of the natural person or the name and address of the company/other organisation, referred to in Article 9(4)(f);

(e) fingerprints;

(f) the number of the visa sticker and date of issue of any previous visa.

3. If the search with one or several of the data listed in paragraph 2 indicates that data on the applicant are recorded in the VIS, the competent visa authority shall be given access to the application file(s) and the linked application file(s) pursuant to Article 8(3) and (4), solely for the purposes referred to in paragraph 1.

Article 16

Use of the VIS for consultation and requests for documents

1. For the purposes of consultation between central visa authorities on applications according to Article 17(2) of the Schengen Convention, the consultation request and the responses thereto shall be transmitted in accordance with paragraph 2 of this Article.

2. The Member State which is responsible for examining the application shall transmit the consultation request with the application number to the VIS, indicating the Member State or the Member States to be consulted.

The VIS shall transmit the request to the Member State or the Member States indicated.

The Member State or the Member States consulted shall transmit their response to the VIS, which shall transmit that response to the Member State which initiated the request.

3. The procedure set out in paragraph 2 may also apply to the transmission of information on the issue of visas with limited territorial validity and other messages related to consular

cooperation as well as to the transmission of requests to the competent visa authority to forward copies of travel documents and other documents supporting the application and to the transmission of electronic copies of those documents. The competent visa authorities shall respond to the request without delay.

4. The personal data transmitted pursuant to this Article shall be used solely for the consultation of central visa authorities and consular cooperation.

Article 17

Use of data for reporting and statistics

The competent visa authorities shall have access to consult the following data, solely for the purposes of reporting and statistics without allowing the identification of individual applicants:

1. status information;

2. the competent visa authority, including its location;

3. current nationality of the applicant;

4. border of first entry;

5. date and place of the application or the decision concerning the visa;

6. the type of visa requested or issued;

7. the type of the travel document;

8. the grounds indicated for any decision concerning the visa or visa application;

9. the competent visa authority, including its location, which refused the visa application and the date of the refusal;

10. the cases in which the same applicant applied for a visa from more than one visa authority, indicating these visa authorities, their location and the dates of refusals;

11. purpose of travel;

12. the cases in which the data referred to in Article 9(6) could factually not be provided, in accordance with the second sentence of Article 8(5);

13. the cases in which the data referred to in Article 9(6) was not required to be provided for legal reasons, in accordance with the second sentence of Article 8(5);

14. the cases in which a person who could factually not provide the data referred to in Article 9(6) was refused a visa, in accordance with the second sentence of Article 8(5).

CHAPTER III

ACCESS TO DATA BY OTHER AUTHORITIES

Article 18

Access to data for verification at external border crossing points

1. For the sole purpose of verifying the identity of the visa holder and/or the authenticity of the visa and/or whether the conditions for entry to the territory of the Member States in accordance with Article 5 of the Schengen Borders Code are fulfilled, the competent authorities for carrying out checks at external border crossing points in accordance with the Schengen Borders Code shall, subject to paragraphs 2 and 3, have access to search using the number of the visa sticker in combination with verification of fingerprints of the visa holder.

2. For a maximum period of three years after the VIS has started operations, the search may be carried out using only the number of the visa sticker. As from one year after the start of operations, the period of three years may be reduced in the case of air borders in accordance with the procedure referred to in Article 49(3).

3. For visa holders whose fingerprints cannot be used, the search shall be carried out only with the number of the visa sticker.

4. If the search with the data listed in paragraph 1 indicates that data on the visa holder are recorded in the VIS, the competent border control authority shall be given access to consult the following data of the application file as well as of linked application file(s) pursuant to Article 8(4), solely for the purposes referred to in paragraph 1:

(a) the status information and the data taken from the application form, referred to in Article 9(2) and (4);

(b) photographs;

(c) the data entered in respect of the visa(s) issued, annulled, revoked or whose validity is extended or shortened, referred to in Articles 10, 13 and 14.

5. In circumstances where verification of the visa holder or of the visa fails or where there are doubts as to the identity of the visa holder, the authenticity of the visa and/or the travel document, the duly authorised staff of those competent authorities shall have access to data in accordance with Article 20(1) and (2).

Article 19

Access to data for verification within the territory of the Member States

1. For the sole purpose of verifying the identity of the visa holder and/or the authenticity of the visa and/or whether the conditions for entry to, stay or residence on the territory of the Member States are fulfilled, the authorities competent for carrying out checks within the territory of the Member States as to whether the conditions for entry to, stay or residence on the territory of the Member States are fulfilled, shall have access to search with the number of the visa sticker in combination with verification of fingerprints of the visa holder, or the number of the visa sticker.

For visa holders whose fingerprints cannot be used, the search shall be carried out only with the number of the visa sticker.

2. If the search with the data listed in paragraph 1 indicates that data on the visa holder are recorded in the VIS, the competent authority shall be given access to consult the following data of the application file as well as of linked application file(s) pursuant to Article 8(4), solely for the purposes referred to in paragraph 1:

(a) the status information and the data taken from the application form, referred to in Article 9(2) and (4);

(b) photographs;

(c) the data entered in respect of the visa(s) issued, annulled, revoked or whose validity is extended or shortened, referred to in Articles 10, 13 and 14.

3. In circumstances where verification of the visa holder or of the visa fails or where there are doubts as to the identity of the visa holder, the authenticity of the visa and/or the travel document, the duly authorised staff of the competent authorities shall have access to data in accordance with Article 20(1) and (2).

Article 20

Access to data for identification

1. Solely for the purpose of the identification of any person who may not, or may no longer, fulfil the conditions for the entry to, stay or residence on the territory of the Member States, the authorities competent for carrying out checks at external border crossing points in accordance with the Schengen Borders Code or within the territory of the Member States as to whether the conditions for entry to, stay or residence on the territory of the Member States are fulfilled, shall have access to search with the fingerprints of that person.

Where the fingerprints of that person cannot be used or the search with the fingerprints fails, the search shall be carried out with the data referred to in Article 9(4)(a) and/or (c); this search may be carried out in combination with the data referred to in Article 9(4)(b).

2. If the search with the data listed in paragraph 1 indicates that data on the applicant are recorded in the VIS, the competent authority shall be given access to consult the following data of the application file and the linked application file(s), pursuant to Article 8(3) and (4), solely for the purposes referred to in paragraph 1:

(a) the application number, the status information and the authority to which the application was lodged;

(b) the data taken from the application form, referred to in Article 9(4);

(c) photographs;

(d) the data entered in respect of any visa issued, refused, annulled, revoked or whose validity is extended or shortened, or of applications where examination has been discontinued, referred to in Articles 10 to 14.

3. Where the person holds a visa, the competent authorities shall access the VIS first in accordance with Articles 18 or 19.

Article 21

Access to data for determining the responsibility for asylum applications

1. For the sole purpose of determining the Member State responsible for examining an asylum application according to Articles 9 and 21 of Regulation (EC) No 343/2003, the competent asylum authorities shall have access to search with the fingerprints of the asylum seeker.

Where the fingerprints of the asylum seeker cannot be used or the search with the fingerprints fails, the search shall be carried out with the data referred to in Article 9(4)(a) and/or (c); this search may be carried out in combination with the data referred to in Article 9(4)(b).

2. If the search with the data listed in paragraph 1 indicates that a visa issued with an expiry date of no more than six months before the date of the asylum application, and/or a visa extended to an expiry date of no more than six months before the date of the asylum application, is recorded in the VIS, the competent asylum authority shall be given access to consult the following data of the application file, and as regards the data listed in point (g) of the spouse and children, pursuant to Article 8(4), for the sole purpose referred to in paragraph 1:

(a) the application number and the authority that issued or extended the visa, and whether the authority issued it on behalf of another Member State;

(b) the data taken from the application form referred to in Article 9(4)(a) and (b);

(c) the type of visa;

(d) the period of validity of the visa;

(e) the duration of the intended stay;

(f) photographs;

(g) the data referred to in Article 9(4)(a) and (b) of the linked application file(s) on the spouse and children.

3. The consultation of the VIS pursuant to paragraphs 1 and 2 of this Article shall be carried out only by the designated national authorities referred to in Article 21(6) of Regulation (EC) No 343/2003.

Article 22

Access to data for examining the application for asylum

1. For the sole purpose of examining an application for asylum, the competent asylum authorities shall have access in accordance with Article 21 of Regulation (EC) No 343/2003 to search with the fingerprints of the asylum seeker.

Where the fingerprints of the asylum seeker cannot be used or the search with the fingerprints fails, the search shall be carried out with the data referred to in Article 9(4)(a) and/or (c); this search may be carried out in combination with the data referred to in Article 9(4)(b).

2. If the search with the data listed in paragraph 1 indicates that a visa issued is recorded in the VIS, the competent asylum authority shall have access to consult the following data of the application file and linked application file(s) of the applicant pursuant to Article 8(3), and, as regards the data listed in point (e) of the spouse and children, pursuant to Article 8(4), for the sole purpose referred to in paragraph 1:

(a) the application number;

(b) the data taken from the application form, referred to in Article 9(4)(a), (b) and (c);

(c) photographs;

(d) the data entered in respect of any visa issued, annulled, revoked, or whose validity is extended or shortened, referred to in Articles 10, 13 and 14;

(e) the data referred to in Article 9(4)(a) and (b) of the linked application file(s) on the spouse and children.

3. The consultation of the VIS pursuant to paragraphs 1 and 2 of this Article shall be carried out only by the designated national authorities referred to in Article 21(6) of Regulation (EC) No 343/2003.

CHAPTER IV

RETENTION AND AMENDMENT OF THE DATA

Article 23

Retention period for data storage

1. Each application file shall be stored in the VIS for a maximum of five years, without prejudice to the deletion referred to in Articles 24 and 25 and to the keeping of records referred to in Article 34.

That period shall start:

(a) on the expiry date of the visa, if a visa has been issued;

(b) on the new expiry date of the visa, if a visa has been extended;

(c) on the date of the creation of the application file in the VIS, if the application has been withdrawn, closed or discontinued;

(d) on the date of the decision of the visa authority if a visa has been refused, annulled, shortened or revoked.

2. Upon expiry of the period referred to in paragraph 1, the VIS shall automatically delete the application file and the link(s) to this file as referred to in Article 8(3) and (4).

Article 24

Amendment of data

1. Only the Member State responsible shall have the right to amend data which it has transmitted to the VIS, by correcting or deleting such data.

2. If a Member State has evidence to suggest that data processed in the VIS are inaccurate or that data were processed in the VIS contrary to this Regulation, it shall inform the Member State responsible immediately. Such message may be transmitted by the infrastructure of the VIS.

3. The Member State responsible shall check the data concerned and, if necessary, correct or delete them immediately.

Article 25

Advance data deletion

1. Where, before expiry of the period referred to in Article 23(1), an applicant has acquired the nationality of a Member State, the application files and the links referred to in Article 8(3) and (4) relating to him or her shall be deleted without delay from the VIS by the Member State which created the respective application file(s) and links.

2. Each Member State shall inform the Member State(s) responsible without delay if an applicant has acquired its nationality. Such message may be transmitted by the infrastructure of the VIS.

3. If the refusal of a visa has been annulled by a court or an appeal body, the Member State which refused the visa shall delete the data referred to in Article 12 without delay as soon as the decision to annul the refusal of the visa becomes final.

CHAPTER V

OPERATION AND RESPONSIBILITIES

Article 26

Operational management

1. After a transitional period, a management authority (the 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.

2. The Management Authority shall also be responsible for the following tasks relating to the communication infrastructure between the central VIS and the national interfaces:

(a) supervision;

(b) security;

(c) the coordination of relations between the Member States and the provider.

3. The Commission shall be responsible for all other tasks relating to the Communication Infrastructure between the central VIS and the national interfaces, in particular:

(a) tasks relating to implementation of the budget;

(b) acquisition and renewal;

(c) contractual matters.

4. 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, in accordance with Council Regulation (EC, Euratom) No 1605/2002 of 25 June 2002 on the Financial Regulation applicable to the general budget of the European Communities [1], to national public-sector bodies in two different Member States.

5. Each national public-sector body referred to in paragraph 4 shall meet the following selection criteria:

(a) it must demonstrate that it has extensive experience in operating a large-scale information system;

(b) it must have considerable expertise in the service and security requirements of a large-scale information system;

(c) it must have sufficient and experienced staff with the appropriate professional expertise and linguistic skills to work in an international cooperation environment such as that required by the VIS;

[1] OJ L 248, 16.9.2002, p. 1. Regulation as last amended by Regulation (EC) No 1525/2007 (OJ L 343, 27.12.2007, p. 9).

(d) it must have a secure and custom-built facility infrastructure able, in particular, to back up and guarantee the continuous functioning of large-scale IT systems; and

(e) its administrative environment must allow it to implement its tasks properly and avoid any conflict of interests.

6. Prior to any delegation as referred to in paragraph 4 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.

7. Where the Commission delegates its responsibility during the transitional period pursuant to paragraph 4, it shall ensure that the delegation fully respects the limits set by the institutional system laid out in the Treaty. It shall ensure, in particular, that the delegation does not adversely affect any effective control mechanism under Community law, whether by the Court of Justice, the Court of Auditors or the European Data Protection Supervisor.

8. Operational management of the VIS shall consist of all the tasks necessary to keep the VIS functioning 24 hours a day, seven days a week in accordance with this Regulation, in particular the maintenance work and technical developments necessary to ensure that the system functions at a satisfactory level of operational quality, in particular as regards the time required for interrogation of the central database by consular posts, which should be as short as possible.

9. Without prejudice to Article 17 of the Staff Regulations of officials of the European Communities, laid down in Regulation (EEC, Euratom, ECSC) No 259/68 ([1]), the Management Authority shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality to all its staff required to work with VIS data. This obligation shall also apply after such staff leave office or employment or after the termination of their activities.

Article 27

Location of the central Visa Information System

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).

([1]) OJ L 56, 4.3.1968, p. 1. Regulation as last amended by Regulation (EC, Euratom) No 337/2007 (OJ L 90, 30.3.2007, p. 1).

Article 28

Relation to the national systems

1. The VIS shall be connected to the national system of each Member State via the national interface in the Member State concerned.

2. Each Member State shall designate a national authority, which shall provide the access of the competent authorities referred to in Article 6(1) and (2) to the VIS, and connect that national authority to the national interface.

3. Each Member State shall observe automated procedures for processing the data.

4. Each Member State shall be responsible for:

(a) the development of the national system and/or its adaptation to the VIS according to Article 2(2) of Decision 2004/512/EC;

(b) the organisation, management, operation and maintenance of its national system;

(c) 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;

(d) 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.

5. 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 29

Responsibility for the use of data

1. 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 in accordance with this Regulation. The Member State responsible shall ensure in particular that:

(a) the data are collected lawfully;

(b) the data are transmitted lawfully to the VIS;

(c) the data are accurate and up-to-date when they are transmitted to the VIS.

2. The management authority shall ensure that the VIS is operated in accordance with this Regulation and its implementing rules referred to in Article 45(2). In particular, the management authority shall:

(a) take the necessary measures to ensure the security of the central VIS and the communication infrastructure between the central VIS and the national interfaces, without prejudice to the responsibilities of each Member State;

(b) ensure that only duly authorised staff have access to data processed in the VIS for the performance of the tasks of the management authority in accordance with this Regulation.

3. The management authority shall inform the European Parliament, the Council and the Commission of the measures which it takes pursuant to paragraph 2.

Article 30

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 purpose of the VIS and in accordance with the relevant legal provisions, including those concerning data protection, and for no longer than necessary in that individual case.

2. Paragraph 1 shall be without prejudice to the right of a Member State to keep in its national files data which that Member State entered in the VIS.

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 31

Communication of data to third countries or international organisations

1. 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.

2. By way of derogation from paragraph 1, the data referred to in Article 9(4)(a), (b), (c), (k) and (m) may be transferred or made available to a third country or to an international organisation listed in the Annex if necessary in individual cases for the purpose of proving the identity of third-country nationals, including for the purpose of return, only where the following conditions are satisfied:

(a) the Commission has adopted a decision on the adequate protection of personal data in that third country in accordance with Article 25(6) of Directive 95/46/EC, or a readmission agreement is in force between the Community and that third country, or the provisions of Article 26(1)(d) of Directive 95/46/EC apply;

(b) the third country or international organisation agrees to use the data only for the purpose for which they were provided;

(c) the data are transferred or made available in accordance with the relevant provisions of Community law, in particular readmission agreements, and the national law of the Member State which transferred or made the data available, including the legal provisions relevant to data security and data protection; and

(d) the Member State(s) which entered the data in the VIS has given its consent.

3. Such transfers of personal data to third countries or international organisations shall not prejudice the rights of refugees and persons requesting international protection, in particular as regards non-refoulement.

Article 32

Data security

1. The Member State responsible shall ensure the security of the data before and during transmission to the national interface. Each Member State shall ensure the security of the data which it receives from the VIS.

2. Each Member State shall, in relation to its national system, adopt the necessary measures, including a security plan, 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 carries out operations in accordance with the purposes of the VIS (checks at entrance to the installation);

(c) prevent the unauthorised reading, copying, modification or removal of data media (data media control);

(d) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);

(e) prevent the unauthorised processing of data in the VIS and any unauthorised modification or deletion of data processed in the VIS (control of data entry);

(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, enter, update, delete and search the data and make these profiles available to the National Supervisory Authorities referred to in Article 41 without delay at 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 have been processed in the VIS, when, by whom and for what purpose (control of data recording);

(j) prevent the unauthorised reading, copying, modification or deletion of personal data during the transmission of personal data to or from the VIS or during the transport of data media, 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 Regulation (self-auditing).

3. The Management Authority shall take the necessary measures in order to achieve the objectives set out in paragraph 2 as regards the operation of the VIS, including the adoption of a security plan.

Article 33

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 Regulation 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 Regulation causes damage to the VIS, that Member State shall be held liable for such damage, unless and insofar as the Management Authority or another Member State failed to take reasonable measures to prevent the damage from occurring or to minimise its impact.

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 34

Keeping of records

1. Each Member State and the Management Authority shall keep records of all data processing operations within the VIS. These records shall show the purpose of access referred to in Article 6(1) and in Articles 15 to 22, the date and time, the type of data transmitted as referred to in Articles 9 to 14, the type of data used for interrogation as referred to in Articles 15(2), 17, 18(1) to (3), 19(1), 20(1), 21(1) and 22(1) and the name of the authority entering or retrieving the data. In addition, each Member State shall keep records of the staff duly authorised to enter or retrieve the data.

2. Such records may be used only for the data-protection monitoring of the admissibility of data processing as well as to ensure data security. The records shall be protected by appropriate measures against unauthorised access and deleted after a period of one year after the retention period referred to in Article 23(1) has expired, if they are not required for monitoring procedures which have already begun.

Article 35

Self-monitoring

Member States shall ensure that each authority entitled to access VIS data takes the measures necessary to comply with this Regulation and cooperates, where necessary, with the National Supervisory Authority.

Article 36

Penalties

Member States shall take the necessary measures to ensure that any misuse of data entered in the VIS is punishable by penalties, including administrative and/or criminal penalties in accordance with national law, that are effective, proportionate and dissuasive.

CHAPTER VI

RIGHTS AND SUPERVISION ON DATA PROTECTION

Article 37

Right of information

1. Applicants and the persons referred to in Article 9(4)(f) shall be informed of the following by the Member State responsible:

(a) the identity of the controller referred to in Article 41(4), including his contact details;

(b) the purposes for which the data will be processed within the VIS;

(c) the categories of recipients of the data, including the authorities referred to in Article 3;

(d) the data retention period;

(e) that the collection of the data is mandatory for the examination of the application;

(f) the existence of the right of access to data relating to them, and the right to request that inaccurate data relating to them be corrected or that unlawfully processed data relating to them be deleted, including the right to receive information on the procedures for exercising those rights and the contact details of the National Supervisory Authorities referred to in Article 41(1), which shall hear claims concerning the protection of personal data.

2. The information referred to in paragraph 1 shall be provided in writing to the applicant when the data from the application form, the photograph and the fingerprint data as referred to in Article 9(4), (5) and (6) are collected.

3. The information referred to in paragraph 1 shall be provided to the persons referred to in Article 9(4)(f) on the forms to be signed by those persons providing proof of invitation, sponsorship and accommodation. In the absence of such a form signed by those persons, this information shall be provided in accordance with Article 11 of Directive 95/46/EC.

Article 38

Right of access, correction and deletion

1. Without prejudice to the obligation to provide other information in accordance with Article 12(a) of Directive 95/46/EC, any person shall have the right to obtain communication of the data relating to him recorded in the VIS and of the Member State which transmitted them to the VIS. Such access to data may be granted only by a Member State. Each Member State shall record any requests for such access.

2. 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.

3. If the request as provided for in paragraph 2 is made to a Member State other than the Member State responsible, the authorities of the Member State with which the request was lodged shall contact the authorities of the Member State responsible within a period of 14 days. The Member State responsible shall check the accuracy of the data and the lawfulness of their processing in the VIS within a period of one month.

4. If it emerges that data recorded in the VIS are inaccurate or have been recorded unlawfully, the Member State responsible shall correct or delete the data in accordance with Article 24(3). The Member State responsible shall confirm in writing to the person concerned without delay that it has taken action to correct or delete data relating to him.

5. If the Member State responsible does not agree that data recorded in the VIS are inaccurate or have been recorded unlawfully, it shall explain in writing to the person concerned without delay why it is not prepared to correct or delete data relating to him.

6. The Member State responsible shall also provide the person concerned with information explaining the steps which he can take if he does not accept the explanation provided. This shall include information on how to bring an action or a complaint before the competent authorities or courts of that Member State and on any assistance, including from the national supervisory authorities referred to in Article 41(1), that is available in accordance with the laws, regulations and procedures of that Member State.

Article 39

Cooperation to ensure the rights on data protection

1. The Member States shall cooperate actively to enforce the rights laid down in Article 38(2), (3) and (4).

2. 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 Article 28(4) of Directive 95/46/EC.

3. 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.

Article 40

Remedies

1. 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 Article 38(1) and (2).

2. The assistance of the National Supervisory Authorities referred to in Article 39(2) shall remain available throughout the proceedings.

Article 41

Supervision by the National Supervisory Authority

1. The authority or authorities designated in each Member State and endowed with the powers referred to in Article 28 of Directive 95/46/EC (the National Supervisory Authority) shall monitor independently the lawfulness of the processing of personal data referred to in Article 5(1) by the Member State in question, including their transmission to and from the VIS.

2. The National Supervisory Authority shall ensure that an audit of the data processing operations in the national system is carried out in accordance with relevant international auditing standards at least every four years.

3. Member States shall ensure that their National Supervisory Authority has sufficient resources to fulfil the tasks entrusted to it under this Regulation.

4. In relation to the processing of personal data in the VIS, each Member State shall designate the authority which is to be considered as controller in accordance with Article 2(d) of Directive 95/46/EC and which shall have central responsibility for the processing of data by that Member State. Each Member State shall communicate the details of that authority to the Commission.

5. Each Member State shall supply any information requested by the National Supervisory Authorities and shall, in particular, provide them with information on the activities carried out in accordance with Articles 28 and 29(1), grant them access to the lists referred to in Article 28(4)(c) and to its records as referred to in Article 34 and allow them access at all times to all their premises.

Article 42

Supervision by the European Data Protection Supervisor

1. The European Data Protection Supervisor shall check that the personal data processing activities of the Management Authority are carried out in accordance with this Regulation. The duties and powers referred to in Articles 46 and 47 of Regulation (EC) No 45/2001 shall apply accordingly.

2. The European Data Protection Supervisor shall ensure that an audit of the Management Authority's personal data processing activities is carried out in accordance with relevant international auditing standards at least every four years. A report of such audit shall be sent to the European Parliament, the Council, the Management Authority, the Commission and the National Supervisory Authorities. The Management Authority shall be given an opportunity to make comments before the report is adopted.

3. The Management Authority shall supply information requested by the European Data Protection Supervisor, give him access to all documents and to its records referred to in Article 34(1) and allow him access to all its premises, at any time.

Article 43

Cooperation between National Supervisory Authorities and the European Data Protection Supervisor

1. The National Supervisory Authorities and the European Data Protection Supervisor, each acting within the scope of their respective competences, shall cooperate actively within the framework of their responsibilities and shall ensure coordinated supervision of the VIS and the national systems.

2. They shall, each acting within the scope of their respective competences, exchange relevant information, assist each other in carrying out audits and inspections, examine difficulties of interpretation or application of this Regulation, study problems

with the exercise of independent supervision or with the exercise of the rights of data subjects, draw up harmonised proposals for joint solutions to any problems and promote awareness of data protection rights, as necessary.

3. The National Supervisory Authorities and the European Data Protection Supervisor shall meet for that purpose at least twice a year. The costs and servicing of these meetings shall be b for the account of the European Data Protection Supervisor. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary.

4. A joint report of activities shall be sent to the European Parliament, the Council, the Commission and the Management Authority every two years. This report shall include a chapter of each Member State prepared by the National Supervisory Authority of that Member State.

Article 44

Data protection during the transitional period

Where the Commission delegates its responsibilities during the transitional period to another body or bodies, pursuant to Article 26(4) of this Regulation, it shall ensure that the European Data Protection Supervisor has the right and is able to exercise his tasks fully, including the carrying out of on-the-spot checks, and to exercise any other powers conferred on him by Article 47 of Regulation (EC) No 45/2001.

CHAPTER VII

FINAL PROVISIONS

Article 45

Implementation by the Commission

1. The central VIS, the national interface in each Member State and the communication infrastructure between the central VIS and the national interfaces shall be implemented by the Commission as soon as possible after the entry into force of this Regulation, including the functionalities for processing the biometric data referred to in Article 5(1)(c).

2. The measures necessary for the technical implementation of the central VIS, the national interfaces and the communication infrastructure between the central VIS and the national interfaces shall be adopted in accordance with the procedure referred to in Article 49(2), in particular:

(a) for entering the data and linking applications in accordance with Article 8;

(b) for accessing the data in accordance with Article 15 and Articles 17 to 22;

(c) for amending, deleting and advance deleting of data in accordance with Articles 23 to 25;

(d) for keeping and accessing the records in accordance with Article 34;

(e) for the consultation mechanism and the procedures referred to in Article 16.

Article 46

Integration of the technical functionalities of the Schengen Consultation Network

The consultation mechanism referred to in Article 16 shall replace the Schengen Consultation Network from the date determined in accordance with the procedure referred to in Article 49(3) when all those Member States which use the Schengen Consultation Network at the date of entry into force of this Regulation have notified the legal and technical arrangements for the use of the VIS for the purpose of consultation between central visa authorities on visa applications according to Article 17(2) of the Schengen Convention.

Article 47

Start of transmission

Each Member State shall notify the Commission that it has made the necessary technical and legal arrangements to transmit the data referred to in Article 5(1) to the central VIS via the national interface.

Article 48

Start of operations

1. The Commission shall determine the date from which the VIS is to start operations, when:

(a) the measures referred to in Article 45(2) have been adopted;

(b) 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;

(c) following validation of technical arrangements, the Member States have notified the Commission that they have made the necessary technical and legal arrangements to collect and transmit the data referred to in Article 5(1) to the VIS for all applications in the first region determined according to paragraph 4, including arrangements for the collection and/or transmission of the data on behalf of another Member State.

2. The Commission shall inform the European Parliament of the results of the test carried out in accordance with paragraph 1(b).

3. In every other region, the Commission shall determine the date from which the transmission of the data in Article 5(1) becomes mandatory when Member States have notified the Commission that they have made the necessary technical and legal arrangements to collect and transmit the data referred to in Article 5(1) to the VIS for all applications in the region concerned, including arrangements for the collection and/or transmission of the data on behalf of another Member State. Before that date, each Member State may start operations in any of these regions, as soon as it has notified to the Commission that it has made the necessary technical and legal arrangements to collect and transmit at least the data referred to in Article 5(1)(a) and (b) to the VIS.

4. The regions referred to in paragraphs 1 and 3 shall be determined in accordance with the procedure referred to in Article 49(3). The criteria for the determination of these regions shall be the risk of illegal immigration, threats to the internal security of the Member States and the feasibility of collecting biometrics from all locations in this region.

5. The Commission shall publish the dates for the start of operations in each region in the *Official Journal of the European Union*.

6. No Member State shall consult the data transmitted by other Member States to the VIS before it or another Member State representing this Member State starts entering data in accordance with paragraphs 1 and 3.

Article 49

Committee

1. The Commission shall be assisted by the committee set up by Article 51(1) of Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [1].

2. Where reference is made to this paragraph, Articles 4 and 7 of Decision 1999/468/EC shall apply.

The period laid down in Article 4(3) of Decision 1999/468/EC shall be two months.

3. Where reference is made to this paragraph, Article 5 and 7 of Decision 1999/468/EC shall apply.

The period laid down in Article 5(6) of Decision 1999/468/EC shall be two months.

Article 50

Monitoring and evaluation

1. 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.

2. For the purposes 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 to the European Parliament, the Council and the Commission a report on the technical functioning of the VIS, including the security thereof.

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. This overall evaluation shall include an examination of results achieved against objectives and an assessment of the continuing validity of the underlying rationale, the application of this Regulation in respect of the VIS, the security of the VIS, the use made of the provisions referred to in Article 31 and any implications for future operations. The Commission shall transmit the evaluation to the European Parliament and the Council.

5. Before the end of the periods referred to in Article 18(2) the Commission shall report on the technical progress made regarding the use of fingerprints at external borders and its implications for the duration of searches using the number of the visa sticker in combination with verification of the fingerprints of the visa holder, including whether the expected duration of such a search entails excessive waiting time at border crossing points. The Commission shall transmit the evaluation to the European Parliament and the Council. On the basis of that evaluation, the European Parliament or the Council may invite the Commission to propose, if necessary, appropriate amendments to this Regulation.

6. Member States shall provide the Management Authority and the Commission with the information necessary to draft the reports referred to in paragraph 3, 4 and 5.

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

[1] OJ L 381, 28.12.2006, p. 4.

8. 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 51

Entry into force and application

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

2. It shall apply from the date referred to in Article 48(1).

3. Articles 26, 27, 32, 45, 48(1), (2) and (4) and Article 49 shall apply as from 2 September 2008.

4. During the transitional period referred to in Article 26(4), references in this Regulation to the Management Authority shall be construed as references to the Commission.

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaty establishing the European Community.

Done at Strasbourg, 9 July 2008.

For the European Parliament	*For the Council*
The President	*The President*
H.-G. PÖTTERING	J.-P. JOUYET

ANNEX

List of international organisations referred to in Article 31(2)

1. UN organisations (such as UNHCR);
2. International Organization for Migration (IOM);
3. The International Committee of the Red Cross.