This text is meant purely as a documentation tool and has no legal effect. The Union's institutions do not assume any liability for its contents. The authentic versions of the relevant acts, including their preambles, are those published in the Official Journal of the European Union and available in EUR-Lex. Those official texts are directly accessible through the links embedded in this document

►B 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)

(OJ L 218, 13.8.2008, p. 60)

Amended by:

		Official Journal		
		No	page	date
►M1	Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009	L 243	1	15.9.2009
►M2	Regulation (EU) No 610/2013 of the European Parliament and of the Council of 26 June 2013	L 182	1	29.6.2013
►M3	Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017	L 327	20	9.12.2017
►M4	Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019	L 135	27	22.5.2019

Corrected by:

►C1 Corrigendum, OJ L 284, 12.11.2018, p. 38 (810/2009)
►C2 Corrigendum, OJ L 284, 12.11.2018, p. 39 (767/2008)
►C3 Corrigendum, OJ L 117, 3.5.2019, p. 14 (2017/2226)

▼B

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)

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.

▼M4

By storing identity data, travel document data and biometric data in the common identity repository (CIR) established by Article 17(1) of Regulation (EU) 2019/817 of the European Parliament and of the Council ([1]), the VIS contributes to facilitating and assisting in the correct identification of persons registered in the VIS under the conditions and for the purposes of Article 20 of that Regulation.

▼B

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;

([1]) Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27).

▼B

(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 [1]. 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. 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.

[1] See page 129 of this Official Journal.

▼B

Article 4

Definitions

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

1. ‘visa’ means:

▼M1

(a) ‘uniform visa’ as defined in Article 2(3) of Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community code on Visas (Visa Code) ([1]);

———————

(c) ‘airport transit visa’ as defined in Article 2(5) of Regulation (EC) No 810/2009;

(d) ‘visa with limited territorial validity’ as defined in Article 2(4) of Regulation (EC) No 810/2009;

———————

▼B

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 ([2]);

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 ([3]), 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;

([1]) OJ L 243, 15.9.2009, p. 1.
([2]) OJ L 64, 7.3.2003, p. 1.
([3]) 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

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;

▼M4

12. ‘VIS data’ means all data stored in the VIS Central System and in the CIR in accordance with Articles 9 to 14;

13. ‘identity data’ means the data referred to in Article 9(4)(a) and (aa);

14. ‘fingerprint data’ means the data relating to the five fingerprints of the index, middle finger, ring finger, little finger and the thumb from the right hand and, where present, from the left hand.

▼B

Article 5

Categories of data

▼C2

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 points (1) to (4) of Article 9 and Articles 10 to 14;

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

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

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

▼M4

1a. The CIR shall contain the data referred to in Article 9(4)(a) to (c), (5) and (6). The remaining VIS data shall be stored in the VIS Central System.

▼B

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.

▼M4

2. Access to the VIS for the purposes of consulting the data shall be reserved exclusively for the duly authorised staff of the national authorities of each Member State which are competent for the purposes laid down in Articles 15 to 22, and for the duly authorised staff of the national authorities of each Member State and of the Union agencies which are competent for the purposes laid down in Articles 20 and 21 of Regulation (EU) 2019/817. Such access shall be limited according to the extent that the data are required for the performance of their tasks for those purposes, and proportionate to the objectives pursued.

▼B

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. ►M1 When the application is admissible according to Article 19 of Regulation (EC) No 810/2009 ◄, 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.

▼B

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

▼M1

Data to be entered on application

▼B

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:

▼M4

(a) surname (family name); first name or names (given names); date of birth; sex;

(aa) surname at birth (former surname(s)); place and country of birth; current nationality and nationality at birth;

(b) the type and number of the travel document or documents and the three-letter code of the issuing country of the travel document or documents;

(c) the date of expiry of the validity of the travel document or documents;

(ca) the authority which issued the travel document and its date of issue;

▼B

(d) place and date of the application;

▼M1

———————

▼B

(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;

▼M1

(g) Member State(s) of destination and duration of the intended stay or transit;

(h) main purpose(s) of the journey;

(i) intended date of arrival in the Schengen area and intended date of departure from the Schengen area;

(j) Member State of first entry;

(k) the applicant's home address;

▼B

(l) current occupation and employer; for students: name of ►M1 educational establishment ◄;

(m) in the case of minors, surname and first name(s) of the applicant's ►M1 parental authority or legal guardian ◄;

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;

▼M3

(da) if applicable, the information indicating that the visa has been issued with limited territorial validity pursuant to Article 25(1)(b) of Regulation (EC) No 810/2009;

▼B

(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;

▼B

(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]);

▼M1

(k) if applicable, the information indicating that the visa sticker has been filled in manually;

▼M3

(l) if applicable, the status of the person indicating that the third-country national is a member of the family of a Union citizen to whom Directive 2004/38/EC of the European Parliament and of the Council ([2]) applies or of a third-country national enjoying the right of free movement equivalent to that of Union citizens under an agreement between the Union and its Member States, on the one hand, and a third country, on the other.

▼B

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.

Article 11

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

▼M1

Where the visa authority representing another Member State discontinues the examination of the application, it shall add the following data to the application file:

▼B

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:

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

([2]) Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (OJ L 158, 30.4.2004, p. 77).

▼M1

(a) status information indicating that the visa has been refused and whether that authority refused it on behalf of another Member State;

▼B

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

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

▼M1

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

(a) the applicant:

(i) presents a travel document which is false, counterfeit or forged;

(ii) does not provide justification for the purpose and conditions of the intended stay;

(iii) does not provide proof of sufficient means of subsistence, both for the duration of the intended stay and for the return to his country of origin or residence, or for the transit to a third country into which he is certain to be admitted, or is not in a position to acquire such means lawfully;

▼M2

(iv) has already stayed for 90 days during the current 180-day period on the territory of the Member States on the basis of a uniform visa or a visa with limited territorial validity;

▼M1

(v) is a person for whom an alert has been issued in the SIS for the purpose of refusing entry;

(vi) is considered to be a threat to public policy, internal security or public health as defined in Article 2(19) of the Schengen Borders Code or to the international relations of any of the Member States, in particular where an alert has been issued in Member States' national databases for the purpose of refusing entry on the same grounds;

(vii) does not provide proof of holding adequate and valid travel medical insurance, where applicable;

(b) the information submitted regarding the justification for the purpose and conditions of the intended stay was not reliable;

(c) the applicant's intention to leave the territory of the Member States before the expiry of the visa could not be ascertained;

(d) sufficient proof that the applicant has not been in a position to apply for a visa in advance justifying application for a visa at the border was not provided.

Article 13

Data to be added for a visa annulled or revoked

1. Where a decision has been taken to annul or to revoke 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;

(b) authority that annulled or revoked the visa, including its location;

(c) place and date of the decision.

▼M1

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

(a) one or more of the ground(s) listed in Article 12(2);

(b) the request of the visa holder to revoke the visa.

▼M3

3. Where a decision has been taken to annul or to revoke a visa, the visa authority that has taken the decision shall immediately retrieve and export from the VIS into the Entry/Exit System established by Regulation (EU) 2017/2226 of the European Parliament and of the Council ([1]) (EES) the data listed under Article 19(1) of that Regulation.

▼B

Article 14

Data to be added for a visa extended

▼M1

1. Where a decision has been taken to extend the period of validity and/or the duration of stay of an issued visa, the visa authority which extended the visa shall add the following data to the application file:

▼B

(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;

▼M1

(d) the number of the visa sticker of the extended visa;

▼B

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

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

▼M1

(g) the territory in which the visa holder is entitled to travel, if the territorial validity of the extended visa differs from that of the original visa;

▼B

(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;

▼M1

———————

▼B

(d) serious personal reasons.

([1]) Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (OJ L 327, 9.12.2017, p. 20).

▼M3

3. The visa authority that has taken a decision to extend the period of validity, the duration of stay of an issued visa, or both, shall immediately retrieve and export from the VIS into the EES the data listed under Article 19(1) of Regulation (EU) 2017/2226.

▼B

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, ►M1 or extend 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;

▼M3

(b) surname (family name), first name or names (given names); date of birth; nationality or nationalities; sex;

(c) the type and number of the travel document; three letter code of the issuing country of the travel document; and the date of expiry of the validity of the travel document;

▼C2

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

▼B

(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.

▼M3

4. For the purposes of consulting the EES in order to examine and decide on visa applications in accordance with Article 24 of Regulation (EU) 2017/2226, the competent visa authority shall be given access to search the EES directly from the VIS with one or several of the data referred to in that Article.

5. Where the search with the data referred to in paragraph 2 of this Article indicates that data on the third-country national are not recorded in the VIS or where there are doubts as to the identity of the third-country national, the competent visa authority shall have access to data for identification in accordance with Article 20.

▼B

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;

▼M1

4. Member State of first entry;

▼B

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

▼M1

6. the type of visa issued;

▼B

7. the type of the travel document;

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

▼B

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;

▼M1

11. main purpose(s) of the journey;

▼C2

12. the cases in which the data referred to in point (6) of Article 9 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 point (6) of Article 9 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 point (6) of Article 9 was refused a visa, in accordance with the second sentence of Article 8(5).

▼B

CHAPTER III

ACCESS TO DATA BY OTHER AUTHORITIES

▼M3

Article 17a

Interoperability with the EES

1. From the start of operations of the EES, as provided for in Article 66(1) of Regulation (EU) 2017/2226, interoperability between the EES and the VIS shall be established to ensure greater efficiency and rapidity of border checks. To that end, eu-LISA shall establish a Secure Communication Channel between the central system of the EES and the central VIS. Direct consultation between the EES and the VIS shall only be possible if both this Regulation and Regulation 2017/2226 so provide. Retrieval of visa-related data from the VIS, their exportation into the EES and the updating of data from the VIS in the EES shall be an automated process once the operation in question is launched by the authority concerned.

2. Interoperability shall enable the visa authorities using the VIS to consult the EES from the VIS:

(a) when examining and deciding on visa applications as referred to in Article 24 of Regulation (EU) 2017/2226 and Article 15(4) of this Regulation;

(b) in order to retrieve and export the visa-related data directly from the VIS into the EES in the event that a visa is annulled, revoked or extended in accordance with Article 19 of Regulation (EU) 2017/2226 and Articles 13 and 14 of this Regulation.

3. Interoperability shall enable the border authorities using the EES to consult the VIS from the EES in order to:

▼M3

(a) retrieve the visa-related data directly from the VIS and import them into the EES so that an entry/exit record or refusal of entry record of a visa holder may be created or updated in the EES in accordance with Articles 14, 16 and 18 of Regulation (EU) 2017/2226 and Article 18a of this Regulation;

(b) retrieve the visa-related data directly from the VIS and import them into the EES in the event that a visa is annulled, revoked or extended in accordance with Article 19 of Regulation (EU) 2017/2226 and Articles 13 and 14 of this Regulation;

(c) verify the authenticity and validity of the visa, whether the conditions for entry to the territory of the Member States in accordance with Article 6 of Regulation (EU) 2016/399 of the European Parliament and of the Council [1] are fulfilled, or both, as referred to in Article 18(2) of this Regulation;

(d) check whether visa-exempt third-country nationals for whom an individual file is not recorded in the EES were previously registered in the VIS in accordance with Article 23 of Regulation (EU) 2017/2226 and Article 19a of this Regulation;

(e) verify, where the identity of a visa holder is verified using fingerprints, the identity of a visa holder with fingerprints against the VIS in accordance with Articles 23(2) and 23(4) of Regulation (EU) 2017/2226 and Article 18(6) of this Regulation.

4. For the operation of the EES web service referred to in Article 13 of Regulation (EU) 2017/2226, the VIS shall update on a daily basis the separate read-only database referred to in Article 13(5) of that Regulation via a one-way extraction of the minimum necessary subset of VIS data.

5. In accordance with Article 36 of Regulation (EU) 2017/2226, the Commission shall adopt the measures necessary for the establishment and the high level design of the interoperability. In order to establish interoperability with the EES, the Management Authority shall develop the required evolutions and adaptations of the central VIS, the national interface in each Member State, and the communication infrastructure between the central VIS and the national interfaces. The Member States shall adapt and develop the national infrastructures.

Article 18

Access to data for verification at borders at which the EES is operated

1. For the sole purpose of verifying the identity of the visa holders, the authenticity, temporal and territorial validity and status of the visa or whether the conditions for entry to the territory of the Member States in accordance with Article 6 of Regulation (EU) 2016/399 are fulfilled, or both, the competent authorities for carrying out checks at borders at which the EES is operated shall have access to the VIS to search using the following data:

[1] Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ L 77, 23.3.2016, p. 1).

▼**M3**

(a) surname (family name), first name or names (given names); date of birth; nationality or nationalities; sex; type and number of the travel document or documents; three letter code of the issuing country of the travel document or documents; and the date of expiry of the validity of the travel document or documents; or

(b) the number of the visa sticker.

2. Solely for the purposes referred to in paragraph 1 of this Article, where a search is launched in the EES pursuant to Article 23(2) of Regulation (EU) 2017/2226, the competent border authority shall launch a search in the VIS directly from the EES using the data referred to in point (a) of paragraph 1 of this Article.

3. By way of derogation from paragraph 2 of this Article, where a search is launched in the EES pursuant to Article 23(2) or (4) of Regulation (EU) 2017/2226, the competent border authority may search the VIS without making use of the interoperability with the EES, where specific circumstances so require, in particular, where it is more appropriate, due to the specific situation of a third-country national, to search using the data referred to in point (b) of paragraph 1 of this Article, or where it is technically impossible, on a temporary basis, to consult the EES data or in the event of a failure of the EES.

4. If the search with the data listed in paragraph 1 indicates that data are stored in the VIS on one or more issued or extended visas which are within their validity period and are under their territorial validity for the border crossing, the competent authority for carrying out checks at borders at which the EES is operated shall be given access to consult the following data contained in the application file concerned as well as in an application file or files linked pursuant to Article 8(4), solely for the purposes referred to in paragraph 1 of this Article:

(a) the status information and the data taken from the application form, ►**C3** referred to in points (2) and (4) of Article 9; ◄

(b) photographs;

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

In addition, for those visa holders for whom certain data are not required to be provided for legal reasons or factually cannot be provided, the competent authority for carrying out checks at borders at which the EES is operated shall receive a notification related to the specific data field or fields concerned which shall be marked as ‘not applicable’.

5. If the search with the data listed in paragraph 1 of this Article indicates that data on the person are recorded in the VIS but no valid visa is recorded, the competent authority for carrying out checks at borders at which the EES is operated shall be given access to consult the following data contained in the application file or files as well as in an application file or files linked pursuant to Article 8(4), solely for the purposes referred to in paragraph 1 of this Article:

▼M3

(a) the status information and the data taken from the application form, ►C3 referred to in points (2) and (4) of Article 9; ◄

(b) photographs;

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

6. In addition to the consultation carried out under paragraph 1 of this Article, the competent authority for carrying out checks at borders at which the EES is operated shall verify the identity of a person against the VIS if the search with the data listed in paragraph 1 of this Article indicates that data on the person are recorded in the VIS and one of the following conditions is met:

(a) the identity of the person cannot be verified against the EES in accordance with Article 23(2) of Regulation (EU) 2017/2226, because:

(i) the visa holder is not yet registered into the EES;

(ii) the identity is verified, at the border crossing point concerned, using fingerprints in accordance with Article 23(2) of Regulation (EU) 2017/2226;

(iii) there are doubts as to the identity of the visa holder;

(iv) of any other reason;

(b) the identity of the person can be verified against the EES but Article 23(5) of Regulation (EU) 2017/2226 applies.

The competent authorities for carrying out checks at borders at which the EES is operated shall verify the fingerprints of the visa holder against the fingerprints recorded in the VIS. For visa holders whose fingerprints cannot be used, the search referred to in paragraph 1 shall be carried out only with the alphanumeric data provided for in paragraph 1.

7. For the purpose of verifying the fingerprints against the VIS as provided for in paragraph 6, the competent authority may launch a search from the EES to the VIS.

8. Where verification of the visa holder or of the visa fails or where there are doubts as to the identity of the visa holder or the authenticity of the visa or travel document, the duly authorised staff of the competent authorities for carrying out checks at borders at which the EES is operated shall have access to data in accordance with Article 20(1) and (2).

▼M3

Article 18a

Retrieval of VIS data for creating or updating an entry/exit record or a refusal of entry record of a visa holder in the EES

Solely for the purpose of creating or updating an entry/exit record or a refusal of entry record of a visa holder in the EES in accordance with Article 14(2) and Articles 16 and 18 of Regulation (EU) 2017/2226, the competent authority for carrying out checks at borders at which the EES is operated shall be given access to retrieve from the VIS and import into the EES the data stored in the VIS and listed in points (c) to (f) of Article 16(2) of that Regulation.

▼B

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:

▼C2

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

▼B

(b) photographs;

(c) the data entered in respect of the visa(s) issued, annulled, revoked or whose validity is extended ►M1 ——————— ◄, 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).

▼M3

Article 19a

Use of the VIS before creating in the EES the individual files of visa-exempt third-country nationals

1. For the purpose of checking whether a person has been previously registered in the VIS, the competent authorities for carrying out checks at external border crossing points in accordance with Regulation (EU) 2016/399 shall consult the VIS before creating in the EES the individual file of *visa-exempt* third-country nationals as laid down in Article 17 of Regulation 2017/2226.

2. For the purpose of paragraph 1 of this Article, where Article 23(4) of Regulation 2017/2226 applies and the search referred to in Article 27 of that Regulation indicates that data on a third-country national are not recorded in the EES, the competent authority for carrying out checks at borders at which the EES is operated shall have access to search in the VIS using the following data: surname (family name); first name or names (given names); date of birth; nationality or nationalities; sex; type and number of the travel document; three letter code of the issuing country of the travel document; and the date of expiry of the validity of the travel document.

3. Solely for the purposes referred to in paragraph 1 of this Article, further to a search launched in the EES pursuant to Article 23(4) of Regulation (EU) 2017/2226, the competent authority for carrying out checks at borders at which the EES is operated may launch a search in the VIS directly from the EES using the alphanumeric data provided for in paragraph 2 of this Article.

4. In addition, if the search with the data referred to in paragraph 2 indicates that data concerning the third-country national are recorded in the VIS, the competent authority for carrying out checks at borders at which the EES is operated shall verify the fingerprints of the third-country national against the fingerprints recorded in the VIS. That authority may launch the verification from the EES. For third-country nationals whose fingerprints cannot be used, the search shall be carried out only with the alphanumeric data provided for in paragraph 2.

5. If the search with the data listed in paragraph 2 of this Article and the verification carried out under paragraph 4 of this Article indicate that data on the person are recorded in the VIS, the competent authority for carrying out checks at borders at which the EES is operated shall be given access to consult the following data contained in the application file concerned as well as in an application file or files linked pursuant to Article 8(4), solely for the purpose referred to in paragraph 1 of this Article:

(a) the status information and the data taken from the application form, ►C3 referred to in points (2) and (4) of Article 9; ◄

(b) photographs;

▼M3

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

6. Where the verification provided under paragraph 4 or 5 of this Article fails or where there are doubts as to the identity of the person or the authenticity of the travel document, the duly authorised staff of the competent authorities for carrying out checks at borders at which the EES is operated shall have access to data in accordance with Article 20(1) and (2). The competent authority for carrying out checks at borders at which the EES is operated may launch from the EES the identification referred to in Article 20.

▼B

Article 20

Access to data for identification

▼M3

1. Solely for the purposes of the identification of any person who may have been registered previously in the VIS or who may not, or may no longer, fulfil the conditions for the entry to, or stay or residence on, the territory of the Member States, the authorities competent for carrying out checks at borders at which the EES is operated or within the territory of the Member States as to whether the conditions for entry to, or stay or residence on, the territory of the Member States are fulfilled, shall have access to search in the VIS with the fingerprints of that person.

▼C2

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 point (4)(a) and/or (c) of Article 9; this search may be carried out in combination with the data referred to in point (4)(b) of Article 9.

▼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 ►M1 ——————— ◄, 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.

▼C2

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

▼C2

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 point (4)(a) and/or (c) of Article 9; this search may be carried out in combination with the data referred to in point (4)(b) of Article 9.

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 point (4)(a) and (b) of Article 9;

(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 point (4)(a) and (b) of Article 9 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.

▼B

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.

▼C2

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 point (4)(a) and/or (c) of Article 9; this search may be carried out in combination with the data referred to in point (4)(b) of Article 9.

▼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:

▼B

(a) the application number;

▼C2

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

▼B

(c) photographs;

(d) the data entered in respect of any visa issued, annulled, revoked, or whose validity is extended ►M1 ——————— ◄, referred to in Articles 10, 13 and 14;

▼C2

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

▼B

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 ►M1 ——————— ◄ 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.

▼B

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.

▼M3

3a. From 30 June 2018, the Management Authority shall be responsible for the tasks referred to in paragraph 3.

▼B

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;

(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.

[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).

▼B

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).

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.

([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).

▼B

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.

▼C2

2. By way of derogation from paragraph 1, the data referred to in point (4)(a), (b), (c), (k) and (m) of Article 9 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:

▼B

(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);

▼B

(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.

▼B

Article 34

Keeping of records

▼M3

1. Each Member State and the Management Authority shall keep records of all data processing operations within the VIS. Those records shall indicate:

(a) the purpose of access referred to in Article 6(1) and in Articles 15 to 22;

(b) the date and time;

(c) the type of data transmitted as referred to in Articles 9 to 14;

(d) the type of data used for interrogation as referred to in Article 15(2), Article 17 and Articles 18(1) and (6), 19(1), 19a(2) and (4), 20(1), 21(1) and 22(1); and

(e) 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.

1a. For the operations listed in Article 17a, a record of each data processing operation carried out in the VIS and the EES shall be kept in accordance with this Article and Article 46 of Regulation (EU) 2017/2226.

▼B

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

▼C2

Article 37

Right of information

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

▼C2

(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 points (4), (5) and (6) of Article 9 are collected.

3. The information referred to in paragraph 1 shall be provided to the persons referred to in point (4)(f) of Article 9 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.

▼B

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.

▼B

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.

▼B

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.

▼B

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).

▼B

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;

▼B

(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.

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

▼B

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.

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.

▼B

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.

▼B

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.