



Council of the
European Union

Brussels, 5 November 2018
(OR. en)

13725/18

Interinstitutional File:
2018/0152(COD)

LIMITE

VISA 290
FRONT 373
MIGR 170
DAPIX 331
SIRIS 148
COMIX 598
CODEC 1842

NOTE

From: Presidency

To: Visa Working Party/Mixed Committee (EU-Iceland/Norway and Switzerland/Liechtenstein)

No. prev. doc.: 11778/18, 12980/18, 12986/18

Subject: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA
- Latest Presidency compromise proposals after the third examination

In view to the discussions in the Visa Working Party of 12-13 November 2018, delegations will find in the Annex the latest Presidency compromise suggestions after the discussions that took place in the Visa Working Party of 22-23 October 2018.

Only the articles concerned by the Commission proposal have been included. Previously suggested changes compared to the Commission proposal (no shading) are marked in underlined and ~~striketrough~~ (not bold) while the latest changes compared to the previous versions (docs. 11778/18, 12986/18) are marked in **bold/underlined** for additions and in **~~bold/striketrough~~** for deletions.

Only when the new concept in Chapter IIIa receives sufficient support from the delegations, the cross-references made to the articles of this Chapter in a series of provisions (e.g. in Articles 6a, 6b, 22g, 22h, 22i, 22j, 22o, 22p, 23, 24, 25, 29a, 31, 37) will be changed. Delegations are requested to refrain from making technical comments in this regard during the meeting.

During the meeting the Presidency wishes to focus only on those articles that underwent important changes (Articles 4, 5, 6a, 6b, 8, 9 to 9 ca, 16, 21 to 22j, 22n, 22o, 31, 37, 38, 45a, 45e and 50 of the VIS regulation and Articles 10, 13 and 21 of the Visa Code) as well as on the recitals. The Presidency considers that the rest of the articles - with their latest (often editorial) changes - already meet the expectations of the vast majority of the Member States, therefore it is not intended to re-launch the discussion on them.

The objective of the Presidency remains to obtain the negotiating mandate from Coreper on 5 December 2018. Should it be necessary, any outstanding issues after 12-13 November will be dealt with on 28 November by the Visa Working Party. For the smooth finalisation of the text, delegations are invited to lift their reservations.

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA

[recitals - see doc. 13799/18]

Article 1

Regulation (EC) No 767/2008 is amended as follows:

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.

This Regulation also lays down procedures for the exchange of information between Member States on long-stay visas and residence permits, including on certain decisions on long-stay visas and residence permits.

By storing identity, travel document and biometric data in the common identity repository (CIR) established by Article 17 of Regulation 2018/XX of the European Parliament and of the Council* [Regulation 2018/XX on interoperability], the VIS contributes to facilitating and assisting in the correct identification of persons registered in the VIS.

Article 2

Purpose of VIS

1. The VIS shall have the purpose of improving the implementation of the common visa policy, consular cooperation and consultation between ~~competent~~ central visa authorities by facilitating the exchange of data between Member States on applications and on the decisions relating thereto, in order to:

- (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 for a visa;
- (c) ~~to~~ facilitate the fight against fraud;
- (d) ~~to facilitate~~ improve the effectiveness and efficiency of checks at external border crossing points and within the territory of the Member States;
- (e) ~~to~~ assist in the identification, in particular in order to facilitate the ~~and~~ return 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~~ assist in the identification of persons in specific circumstances ~~who have gone missing~~;
- (g) ~~to~~ facilitate the application of Regulation (EU) No 604/2013 of the European Parliament and of the Council* and of Directive 2013/32/EU of the European Parliament and of the Council**;
- (h) ~~to~~ contribute to the prevention, detection and investigation of terrorist offences or of other serious criminal offences;
- (i) ~~to~~ contribute to the prevention of threats to the internal security of any of the Member States;
- (j) ~~to~~ ensure the correct identification of persons;
- (k) support the objectives of the Schengen Information System (SIS) related to the alerts in respect of ~~third country nationals subject to a refusal of entry and stay, subject to a return decision, persons wanted for arrest, or for surrender or extradition purposes, on missing or vulnerable persons, or persons sought to assist with a judicial procedure and or persons for discreet checks, inquiry checks or specific checks.~~

2. As regards long stay visas and residence permits, the VIS shall have the purpose of facilitating the exchange of data between Member States on the decisions related thereto, in order to:

- (a) support a high level of security by contributing to the assessment of whether the applicant is considered to pose a threat to public policy, internal security or public health prior to their arrival at the external borders crossing points;
- (b) ~~improve enhance~~ the effectiveness and efficiency of border checks and of checks within the territory;
 - (ba) to assist in the identification, in particular in order to facilitate the return 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;
- (c) contribute to the prevention, detection and investigation of terrorist offences or of other serious criminal offences;

- (d) ensure the correct identification of persons;
- (e) facilitate the application of Regulation (EU) No 604/2013 and of Directive 2013/32/EU;
- (f) support the objectives of the Schengen Information System (SIS) related to the alerts in respect of ~~third country nationals subject to a refusal of entry and stay, subject to a return decision, persons wanted for arrest, or for surrender or extradition purposes, on missing or~~ vulnerable persons, ~~on~~ persons sought to assist with a judicial procedure and ~~on~~ persons for discreet checks, inquiry checks or specific checks.

Article 3^t

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 This deletion is suggested by the Commission in its proposal.

Article 4

Definitions

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

1. 'visa' means:

(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) ^(2);

(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;

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 ^(3);

4. 'application form' means the uniform application form for visas in Annex 1 ~~of Regulation (EC) No 810/2009~~ 16 to the Common Consular Instructions²;

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 ^(4), 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);

² Revert the original Commission proposal (i.e. no change).

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

(12) 'VIS data' means all data stored in the VIS Central System and in the CIR in accordance with Articles 9 to 14, 22c to 22f;

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

(14) 'fingerprint data' means the VIS data relating fingerprints ~~that is stored in a VIS file~~;

(15) 'facial image' means digital image of the face taken live, or a scan of the photograph as referred to in Article 10(3)c of Regulation (EC) No 810/2009 when live facial image is not required or exceptionally the facial image extracted from the chip of the machine readable travel document in accordance with Article 13 of Regulation (EC) No 810/2009;

(15a) 'hitmatch' means the existence of a correspondence as a result of an automated comparison between personal established by comparing two or more occurrences of data recorded or being recorded in an information system or a database;³

(16) 'Europol data' means personal data processed by Europol for the purpose referred to in Article 18(2)(a) of Regulation (EU) 2016/794 of the European Parliament and of the Council*;

(17) 'residence permit' means all residence permits issued by the Member States in accordance with the uniform format laid down by Council Regulation (EC) No 1030/2002** and all other documents referred to in Article 2(16)(b) of Regulation (EU) 2016/399;

(18) 'long-stay visa' means an visa authorisation⁴ issued by a Member State as provided for in Article 18 of the Schengen Convention;

(19) 'national supervisory authority' ~~as regards law enforcement purposes~~ means the supervisory authority~~s~~ established in accordance with Article 51(1) of Regulation (EU) 2016/679*** and the supervisory authority established in accordance with Article 41 of Directive (EU) 2016/680 of the European Parliament and of the Council****;

(20) 'law enforcement' means the prevention, detection or investigation of terrorist offences or other serious criminal offences;

(21) 'terrorist offences' means the offences under national law which corresponds or are is equivalent to one of the offences ~~those~~ referred to in Directive (EU) 2017/541 of the European Parliament and of the Council****;

(22) 'serious criminal offences' means the offences which corresponds or ~~are is~~ equivalent to one of the offences ~~those~~ referred to in Article 2(2) of Council Framework Decision 2002/584/JHA*****, if they are punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years.

³ Aligned to the definition in the Interoperability Proposal (see point (21) in Article 4 in doc. 11312/18). As a consequence the references made to hit/hits have been changed to match/matches in the entire text.

⁴ Revert the original Commission proposal due to the definition of "visa" in point 1.

Article 5

Categories of data

1. Only the following categories of data shall be recorded in the VIS:

(a) alphanumeric data on the ~~short-stay~~ visa applicant and on visas requested, issued, refused, annulled, revoked or extended referred to in Article 9(1) to (4) and Articles 10 to 14, alphanumeric data on long stay visa and residence permits issued, withdrawn, refused, annulled, revoked, **renewed** or extended referred to in Articles 22c, 22d, 22e and 22f, as well as information regarding the **matches hits** referred to in Articles 9a and 22b, and the results of verifications referred to in Article 9c(6);

(b) facial images referred to in Article 9(5), ~~and Article 22c(2)(f) and Article 22d(f)~~ **or photographs where facial images are not required**;

(c) fingerprint data referred to in Article 9(6), ~~and Article 22c(2)(g) and Article 22d(g)~~;

(ca) scans of the biographic data page of the travel document referred to in Article 9(7) and Article 22c(2) ~~h~~ cd and 22d ca;

(d) links to other applications referred to in Article 8(3) and (4) and Article 22a(3).

2. The messages transmitted by 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.

3. The CIR shall contain the data referred to in Article 9(4)(a) to (cc), Article 9(5) and 9(6), Article 22c(2)(a), ~~to (cc), (f) and (g), and Article 22d(a) to (ce), (f) and (g)~~. The remaining VIS data shall be stored in the VIS Central System.

Article 5a

List of recognised travel documents

1. The list of travel documents which entitle the holder to cross the external borders and which may be endorsed with a visa, as established by Decision No 1105/2011/EU of the European Parliament and of the Council*, shall be integrated in the VIS.

2. The VIS shall provide the functionality for the centralised management of the list of recognised travel documents and of the notification of the recognition or non-recognition of the listed travel documents pursuant to Article 4 of Decision No 1105/2011/EU.

3. The detailed rules on managing the functionality referred to in paragraph 2 shall be laid down in implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 49(2).

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 and to the authorities competent to decide on an application for a long-stay visa or residence permit in accordance with Chapter IIIa of this Regulation Article 22c to f.

2. Access to the VIS for consulting the data shall be reserved exclusively for the duly authorised staff of the national authorities of each Member State and of the EU bodies which are competent for the purposes laid down in Article 6a and b, Articles 15 to 22, Articles 22e to 22f and Articles 22g to 22j, as well as for the purposes laid down in Articles 20 and 21 of [*Regulation 2018/XX on interoperability*].

That access shall be 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.

4. In addition to the notifications mentioned in paragraph 3, each Member State shall also communicate to the Management Authority without delay a list of the competent national authorities having access to the VIS for the purposes of this Regulation. That list shall specify for which purpose each authority is to have access to the data stored in the VIS.

The VIS shall provide the functionality for the centralised management of this list.

5. The detailed rules on managing the functionality for the centralised management of the list in paragraph 3 shall be laid down in implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 49(2).

Article 6a⁵

Access to data for identification

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.

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) **and/or Article 9(5)**; or Article 22c(2)(a) and/or (b), (c), (cc) **and/or Article 22c(f)**; or Article 22d(a), (b) and/or (c) **and/or Article 22d(f)**; this search may be carried out in combination with the data referred to in Article 9(4)(b). **However, the facial image shall not be the only search criterion.**

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 individual file as well as** the linked application file(s), pursuant to Article 8(3) and (4) **and linked individual file(s) pursuant to Article 22a(3)**, 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) or the data referred to in Article 22c or Article 22d;

(c) facial images ~~photographs~~;

(d) the data entered in respect of any visa issued, refused, annulled, revoked or whose validity is extended, or of applications where examination has been discontinued, referred to in Articles 10 to 14 or data entered in respect of any long stay visa or residence permit issued, extended, renewed, refused, withdrawn, revoked or annulled referred to in Articles 22c to f.

3. Where the person holds a visa or long stay visa or residence permit, the competent authorities shall access the VIS first in accordance with Articles 18 or 19 or Articles 22g or h.

⁵ Existing Article 20 of the Regulation. The Presidency suggests moving it under the General Provisions Chapter.

Article 6b⁶

Use of VIS data for the purpose of entering SIS alerts on certain categories of missing persons **and the subsequent access to those data**

1. **Fingerprint D**ata stored in the VIS may be used for the purpose of entering an alert on persons referred to in missing persons, abducted or identified as victims of trafficking in human beings in accordance with [Article 32(2) of Regulation (EU) ... of the European Parliament and of the Council* [Regulation (EU) on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters]. In those cases, the transmission exchange of **fingerprint** data shall take place via secured means to the SIRENE Bbureau of the Member State responsible ~~owning the data.~~

~~2. Where there is a hit against a SIS alert as referred to in paragraph 1, child protection authorities and, including national judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to charge and their coordinating authorities, as referred to in [Article 443] of Regulation (EU) ... [COM(2016) 883 final – SIS LE], may request, in the performance of their tasks, access to the data entered in VIS. The conditions provided for in Union and national legislation shall apply.~~

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.

3. The best interests of the child shall be a primary consideration for Member States with respect to all procedures provided for in this Regulation. The child's well-being, safety and security, in particular where there is a risk of the child being a victim of ~~human~~ trafficking in human beings, and the views of the child shall be taken into consideration and given due weight in accordance with his or her age and maturity.

⁶ Article 20a of the Commission proposal. The Presidency suggests moving it under the General Provisions Chapter with the changes indicated in the text.

CHAPTER II

ENTRY AND USE OF DATA ON ~~SHORT STAY VISAS~~ BY VISA AUTHORITIES

Article 8

Procedures for entering data upon the application

1. When the application is admissible pursuant to Article 19 of Regulation (EC) No 810/2009, the visa authority shall create the application file within ~~23~~ **4** working days, by entering the data referred to in Article 9 in the VIS, as far as those data are required to be provided by the applicant.

1a. Upon creation of the application file, the VIS shall automatically launch the query pursuant to Article 9a and return results.

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'. The absence of fingerprints should be indicated by "VIS0"; furthermore, the system shall permit a distinction to be made between the cases pursuant to Article 13(7)(a) to (d) of Regulation (EC) No 810/2009.

Article 9

Data to be entered on 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 form⁷:

(a) surname (family name); first name(s) ~~or names~~ (given names); date of birth; current nationality or nationalities; sex;

(aa) surname at birth (former ~~surname~~ family name(s)); place and country of birth; 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~~;

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

(d) place and date of the application;

(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) 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;

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

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

5. the facial image ~~or the photograph~~ of the applicant, **in accordance with Article 10 and Article 13(1) of Regulation (EC) No 810/2009**;

⁷ List below to be aligned with the new visa application form once the text of the Visa Code amendment is finalised.

~~6. fingerprints of the applicant, in accordance with Article 13 the relevant provisions of the Common Consular Instructions Regulation (EC) No 810/2009⁸;~~

7. a scan of the biographic data page of the travel document;

7a. if applicable, the fact that the applicant applies as a family member of a Union citizen to whom Directive 2004/38/EC* applies or of a national of a third country 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.

~~8. The facial image of third country nationals referred to in point 5 of the first paragraph shall have sufficient image resolution and quality to be used in automated biometric matching.⁹~~

~~By way of derogation from the second paragraph, in exceptional cases where the quality and resolution specifications set for the enrolment of the live facial image in the VIS cannot be met, the facial image may be extracted electronically from the chip of the electronic Machine Readable Travel Document (eMRTD). In such cases, the facial image shall only be inserted into the individual file after electronic verification that the facial image recorded in the chip of the eMRTD corresponds to the live facial image of the third country national concerned.¹⁰~~

***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**

Article 9a

Queries to other systems

1. The application files shall be automatically processed by the VIS to identify **matches hits**. The VIS shall examine each application file individually.
2. When an application is created ~~or~~ **and when a visa is issued**, the VIS shall check whether the travel document related to that application is recognised in accordance to Decision No 1105/2011/EU, by performing an automatic search against the list of recognised travel documents referred to in Article 5a, and shall return a result.

⁸ Revert the original Commission proposal (i.e. no change).

⁹ Moved to Article 13 of the Visa Code.

¹⁰ Moved to Article 13 of the Visa Code.

3. For the purpose of the verifications provided for in Article 21(1) and Article 21(3)(a), (c) and (d) of Regulation (EC) No 810/2009, the VIS shall launch a query ~~by using the European Search Portal defined in Article 6(1) [of the Interoperability Regulation]~~ to compare the relevant data referred to in points (4), (5) and (6) of Article 9 of this Regulation to the data present in a record, file or alert registered in the VIS, the Schengen Information System (SIS), the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS), including the watchlist referred to in Article ~~29-34~~ of Regulation (EU) 2018/XX for the purposes of establishing a European Travel Information and Authorisation System], the Eurodac, [the ECRIS-TCN system as far as convictions related to terrorist offences and other forms of serious criminal offences are concerned], the Europol data, the Interpol Stolen and Lost Travel Document database (SLTD) and the Interpol Travel Documents Associated with Notices database (Interpol TDAWN).

This query may be launched using, as ~~where~~ appropriate, the European Search Portal defined in Article 6(1) or in accordance with Chapter II [of the Interoperability Regulation].

4. The VIS shall add a reference to any match hit obtained pursuant to paragraph 3, with the exception of matches resulting from the comparison referred to in paragraph 5, to the application file. Additionally, the VIS shall identify, where relevant, the Member State(s) that entered or supplied the data having triggered the ~~hit~~match(es) or Europol, and shall record this in the application file.
5. For the purposes of Article 2(1)(k), the queries carried out under paragraph 3 of this Article shall compare the relevant data referred to in Article 15(2) to the data present in the SIS in order to determine whether the applicant is subject to one of the following alerts:
- (a)~~an alert in respect of persons wanted for arrest for surrender purposes or extradition purposes;~~
 - (b)an alert in respect of missing or vulnerable persons;
 - (c)an alert in respect of persons sought to assist with a judicial procedure;
 - (d)an alert on persons ~~and objects~~ for discreet checks, inquiry checks or specific checks.

Article 9b

Specific provisions applicable to the queries to other systems for family members of EU citizens or of other third country nationals enjoying the right of free movement under Union law

1. As regards third country nationals who are members of the family of a Union citizen to whom Directive 2004/38/EC applies or of a national of a third country 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, the automated checks in Article 9a(3) shall be carried out solely for the purpose of checking that there are no factual indications or reasonable grounds based on factual indications to conclude that the presence of the person on the territory of the Member States poses a risk to security or high epidemic risk in accordance with Directive 2004/38/EC.

2. The VIS shall not verify whether:

- a) **the applicant is currently reported as overstayer or whether he or she has been reported as overstayer in the past through consultation of the EES;**
- b) **the applicant corresponds to a person whose data is recorded in the Eurodac.**

3. Where the automated processing of the application as referred to in Article 9a(3) has reported a match corresponding to a refusal of entry and stay alert as referred to in Article 24 of Regulation (EC) 1987/2006, the visa authority shall verify the ground for the decision following which this alert was entered in the SIS. If this ground is related to an illegal immigration risk, the alert shall not be taken into consideration for the assessment of the application. The visa authority shall proceed according to Article 25(2) of the SIS II Regulation.

Article 9c

Manual vVerification of the matches by the central visa authorities

- 1. Any **matchhit** ~~resulting from the queries~~ pursuant to Article 9a(3) shall be manually verified by the ~~central~~ **designated competent visa** authority of the Member State processing the application.
 - 2. Where manually verifying the **hitmatches**, the ~~central~~ **competent** visa authority shall have access to the application file and any linked application files, as well as to all the **hitmatches** triggered during the automated processing pursuant to Article 9a(3).
 - 3. The ~~central~~ **competent visa** authority shall verify whether the identity of the applicant recorded in the application file corresponds to the data present in the VIS, or one of the consulted databases **and record, if applicable, the answer of Europol, if provided in accordance with Article 9ca, in the application file.**
 - 4. Where the personal data do not correspond, and no other **matchhit** has been reported during the automated processing pursuant to Article 9a(3), the ~~central~~ **competent visa** authority shall erase the false **hit match** from the application file.
- 4a. Following the verification by the competent visa authority as referred to in paragraph 3, where the personal data correspond to the data present in the SIS, the VIS shall also send an automated notification to the SIRENE Bureau of the Member State that entered the alert having triggered a match against SIS.**
- 4b. The notification provided to the SIRENE Bureau of the Member State that entered the alert shall contain the relevant data referred to in Article 9 of this Regulation.**

5. ~~Where the data correspond to or where doubts remain concerning the identity of the applicant, the central visa authority processing the application shall inform the central visa authority of the other Member State(s), which were identified as having entered or supplied the data that triggered the hit pursuant to Article 9a(3). Where one or more Member States were identified as having entered or supplied the data that triggered such hit, the central visa authority shall consult the central visa authorities of the other Member State(s) using the procedure set out in Article 16(2).~~
6. ~~The result of the verifications carried out by the central visa authorities of the other Member States shall be added to the application file.~~
7. By derogation from paragraph 1, where the comparison referred to in Article 9a(5) reports one or more **hitmatches**, the VIS shall send an automated notification to the **SIRENE Bureau** central visa authority of the Member State that **launched the query entered the alert. The SIRENE Bureau concerned shall further verify the correspondance of the applicant's personal data with the personal data contained in the alert having triggered the match and to** take any appropriate follow-up action **in accordance with the relevant legislation.**
8. ~~Where Europol is identified as having supplied the data having triggered a hit in accordance with Article 9a(3), the central competent authority of the responsible Member State shall consult the Europol national unit for follow up in accordance with Regulation (EU) 2016/794 and in particular its Chapter IV.~~

Article 9ca

Consultation of Europol

1. Where Europol is identified as having supplied the data having triggered a **hit match in the Europol data** in accordance with Article 9ba(3), **an automated notification shall be sent to Europol in order to verify the match by comparing it with its own data. For this purpose, the VIS shall also transmit to Europol the relevant data of the application file which triggered that match. Once the match is confirmed, Europol should send a positive or negative answer to the competent visa authority of the responsible Member State which shall record it in the application file in accordance with Article 9c(3).**
2. ~~Where consulted in accordance with paragraph 1, Europol shall provide a reasoned opinion on the application. Europol's opinion shall be made available to the central authority of the responsible Member State which shall record it in the application file. Such consultation shall take place in accordance with Regulation (EU) 2016/794 and in particular its Chapter IV.~~
3. ~~The central authority of the responsible Member State shall consult Europol. Where consulted in accordance with paragraph 1, Europol shall provide a reasoned opinion on the application. Europol's opinion shall be made available to the central authority of the responsible Member State which shall record it in the application file. Europol shall reply within 60 hours of the date of the notification of the consultation. The failure by Europol to reply within the deadline shall be considered as a positive opinion on the application.~~

4. ~~The central authority of the responsible Member State may consult Europol following the reply of an applicant to a request for additional information. In such a case, the central authority shall transmit to Europol the relevant additional information or documentation provided by the applicant in relation to the request the visa for which Europol is consulted.~~
5. Where Europol provides a negative opinion on the application and the responsible Member State decides to issue a visa, the visa authority shall ~~justify its decision and shall~~ record the ~~reasons it~~ in the application file.

Article 9d

Responsibilities of Europol

Europol shall adapt its information system to ensure that automatic processing of the queries referred to in Article 9a(3) and Article 22b(2) is possible.

[...]

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.

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.

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⁽⁷⁾ (EES) the data listed under Article 19(1) of that Regulation.

4. When the application file is updated pursuant to paragraphs 1 and 2, the VIS shall send a notification to the Member State that issued the visa, informing of the decision to annul or revoke that visa. Such notification shall be generated automatically by the central system and transmitted via the mechanism provided in Article 16.

[...]

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, 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;

(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;

(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;

(ea) facial image;

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

2a. The facial image referred to in point (ea) of paragraph 2 shall not be the only search criterion.

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.

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 ~~6a20~~.

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. When an application file is created in the VIS regarding a national of a specific third country or belonging to a specific category of such nationals for which prior consultation is requested pursuant to Article 22 of Regulation (EC) No 810/2009, the VIS shall automatically transmit the request for consultation 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 created the application.

Solely for the purpose of carrying out the consultation procedure, the list of Member States requiring that their central authorities be consulted by other Member States' central authorities during the examination of visa applications for uniform visas lodged by nationals of specific third countries or specific categories of such nationals, according to Article 22 of Regulation (EC) No 810/2009, and of the third country nationals concerned, shall be integrated into the VIS. The VIS shall provide the functionality for the centralised management of this list.

3. The procedure set out in paragraph 2 shall mutatis mutandis also apply to:

- (a) the transmission of information pursuant to Article 24(2) on data amendments as well as Article 25(4) of this Regulation and Article 31 of Regulation (EC) No 810/2009, respectively on the issuing of visas with limited territorial validity, ~~Article 24(2) on data amendments and Article 31 of Regulation (EC) No 810/2009~~ on ex post notifications;
- (b) all other messages related to consular cooperation that entail transmission of personal data recorded in the VIS or related to it, to the transmission of requests to the competent visa authority to forward copies of travel documents pursuant to point 7 of Article 9 and other documents supporting the application and to the transmission of electronic copies of those documents, as well as to requests pursuant to Article 9c and Article 38(3). The competent visa authorities shall respond to any such requests within ~~two~~ **three five** working days.

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

Article 17¹¹

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. Member State of first entry;~~
- ~~5. date and place of the application or the decision concerning the visa;~~
- ~~6. the type of visa 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. main purpose(s) of the journey;~~
- ~~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).~~

¹¹ This deletion is suggested by the Commission in its proposal.

CHAPTER III

ACCESS TO ~~SHORT STAY~~-VISA DATA BY OTHER AUTHORITIES

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:

(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, referred to in Article 9(2) and (4);

(b) facial images ~~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:

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

(b) facial images ~~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 mentioned under paragraph 1 shall be carried out with the alphanumeric data foreseen under paragraph 1 in combination with the facial image.

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 ~~6a~~²⁰(1) and (2).

[...]

Article 20¹²

Access to data for identification

~~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.~~

~~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 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.~~

¹² Moved to Chapter I (new Article 6a).

Article 20a¹³

Use of VIS data for the purpose of entering SIS alerts on missing persons and the subsequent access to those data

~~1. Fingerprint data stored in the VIS may be used for the purpose of entering an alert on missing persons in accordance with Article 32(2) of Regulation (EU) ... of the European Parliament and of the Council* [Regulation (EU) on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters]. In those cases, the exchange of fingerprint data shall take place via secured means to the SIRENE bureau of the Member State owning the data.~~

~~2. Where there is a hit against a SIS alert as referred to in paragraph 1, child protection authorities and national judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to charge and their coordinating authorities, as referred to in Article 43 of Regulation (EU) ... [COM(2016) 883 final – SIS LE], may request, in the performance of their tasks, access to the data entered in VIS. The conditions provided for in Union and national legislation shall apply.~~

~~_____~~
~~* Regulation (EU) .. of the European Parliament and of the Council of ... (OJ L .., p. ...).~~

~~{...}~~

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 604343/2010¹⁴, 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) and/or Article 9(5); this search may be carried out in combination with the data referred to in Article 9(4)(b). However, the facial image shall not be the only search criterion.

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;

¹³ Moved to Chapter I (new Article 6b).

¹⁴ Revert the original Commission proposal (i.e. no change).

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

(c) *the type of visa*;

(d) *the period of validity of the visa*;

(e) *the duration of the intended stay*;

(f) *facial images* ~~photographs~~;

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

(g) the data referred to in Article 9(4)(a) and (~~aab~~) 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 ~~604343/2010~~¹⁵.*

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~~ ³⁴ of Regulation (EUC) No ~~604343/2010~~¹⁶ 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) **and/or Article 9(5)**; this search may be carried out in combination with the data referred to in Article 9(4)(b). **However, the facial image shall not be the only search criterion.**

2. If the search with the data listed in paragraph 1 indicates that data on the applicant for international protection is recorded in the VIS, the competent asylum authority shall have access to consult the following data of the applicant and of any linked application files of the applicant pursuant to Article 8(3), for the sole purpose referred to in paragraph 1:

(a) the application number;

(b) the data taken from the application form(s), referred to in points (4), (5) and (7) of Article 9;

(c) *facial images* ~~photographs~~;

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

(e) the data referred to in points (4) and (5) of Article 9 of the linked application files pursuant to Article 8(4).

¹⁵ Revert the original Commission proposal (i.e. no change).

¹⁶ Revert the original Commission proposal (i.e. no change).

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 34~~21~~(6) of Regulation (EUC) No 604~~343~~/2010~~3~~¹⁷.

CHAPTER IIIa

ENTRY AND USE OF DATA ON LONG STAY VISAS AND RESIDENCE PERMITS

Article 22a

Procedures for entering data upon ~~decision on an~~ application for a long stay visa or residence permit

1. Upon ~~decision on an~~ application for a long stay visa or residence permit, the **competent** authority ~~that issued that decision~~ shall create without delay the individual **application** file, by entering the **following application** data ~~referred to in Article 22c or Article 22d~~ in the VIS, ~~insofar as available~~ **as far as those data are required to be provided by the applicant:**
 - a. **application number;**
 - b. **status information, indicating that a long stay visa or residence permit has been requested;**
 - c. **the authority with which the application has been lodged, including its location;**
 - d. **surname (family name); first name(s); date of birth; current nationality or nationalities; sex; date, place of birth;**
 - e. **type and number of the travel document and the three letter code of the issuing country of the travel document;**
 - f. **the date of expiry of the validity of the travel document;**
 - g. **authority which issued the travel document and its date of issue;**
 - h. **a scan of the biographic data page of the travel document;**
 - i. **in the case of minors, surname and first name(s) of the holder's parental authority or legal guardian;**
 - j. **a facial image of the holder, where possible taken live or a photograph;**
 - k. **fingerprints of the holder.**
2. Upon creation of the individual **application** file, the VIS shall automatically launch the query pursuant to Article 22b.

¹⁷ Revert the original Commission proposal (i.e. no change).

3. If the holder has applied as part of a group or with a family member, the authority shall create an individual file for each person in the group and link the files of the persons having applied together and who were issued a long stay visa or residence permit.
4. Where particular data are not required to be provided in accordance with Union or national legislation or factually cannot be provided, the specific data field(s) shall be marked as ‘not applicable’. In the case of fingerprints, the system shall permit a distinction to be made between the cases where fingerprints are not required to be provided in accordance with Union or national legislation and the cases where they cannot be provided factually.

Article 22b

Queries to other systems

1. Solely for the purpose of assessing whether the person could pose a threat to the public policy, or internal security or public health of the Member States, pursuant to Article 6(1)(e) of Regulation (EU) 2016/399, the files shall be automatically processed by the VIS to identify **hitmatch(es)**. The VIS shall examine each file individually.
2. Every time an individual **application** file is created ~~upon issuance or refusal pursuant to Article 22c or 22d of a long stay visa or residence permit in accordance with Article 22a,~~ the VIS shall ~~shall~~ launch a query by using the European Search Portal defined in Article 6(1) of [the Interoperability Regulation] to compare the relevant **application** data ~~referred to in Article 22c(2)(a), (b), (c), (f) and (g) of this Regulation~~ with the relevant data~~s~~ in the VIS, the Schengen Information System (SIS), the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS) including the watchlist referred to in Article 29 of Regulation (EU) 2018/XX for the purposes of establishing a European Travel Information and Authorisation System, **the Eurodac**, [the ECRIS-TCN system as far as convictions related to terrorist offences and other forms of serious criminal offences are concerned], the Europol data, the Interpol Stolen and Lost Travel Document database (SLTD), and the Interpol Travel Documents Associated with Notices database (Interpol TDAWN).
3. The VIS shall add a reference to any **match hit** obtained pursuant to paragraphs (2) ~~and (5)~~ to the individual file. Additionally, the VIS shall identify, where relevant, the Member State(s) that entered or supplied the data having triggered the **hitmatch(es)** or Europol, and shall record this in the individual file.
4. ~~For the purposes of Article 2(2)(f) in respect of an issued or extended long stay visa the queries carried out under 22b paragraph 2 of this Article shall compare the relevant data referred to in Article 22c(2), to the data present in the SIS in order to determine whether the holder is subject to one of the following alerts:~~
 - ~~(a) an alert in respect of persons wanted for arrest for surrender purposes or extradition purposes;~~
 - ~~(b) an alert in respect of missing persons;~~

- ~~(c) — an alert in respect of persons sought to assist with a judicial procedure;~~
- ~~(d) — an alert on persons and objects for discreet checks or specific checks.~~

~~Where the comparison referred to in this paragraph reports one or several hit(s), the VIS shall send an automated notification to the central authority of the Member State that launched the query request and the Member State concerned shall take any appropriate follow-up action.~~

- ~~5. — As regards the consultation of EES, ETIAS and VIS data pursuant to paragraph 2, the hits shall be limited to indicating refusals of a travel authorisation, refusals of entry or of the decision to refuse, annul or revoke a visa or residence permit which are based on security grounds.~~
- ~~6. — Where the long stay visa or residence permit is issued or extended by a consulate consular authority of a Member State, Article 9a shall apply.~~
- ~~7. — Where the long stay visa or residence permit is issued or extended or where a long stay visa is extended by an authority in the territory of a Member State, the following shall apply:
 - ~~(a) — that authority shall verify whether the data recorded in the individual file corresponds to the data present in the VIS, or one of the consulted EU information systems/databases, the Europol data, or the Interpol databases pursuant to paragraph 2;~~
 - ~~(b) — where the hit pursuant to paragraph 2 is related to Europol data, the Europol national unit shall be informed for follow up;~~
 - ~~(c) — where the data do not correspond, and no other hit has been reported during the automated processing pursuant to paragraphs 2 and 3, the authority shall delete the false hit from the application file;~~
 - ~~(d) — where the data correspond to or where doubts remain concerning the identity of the applicant, the authority shall take action on the data that triggered the hit pursuant to paragraph 4 according to the procedures, conditions and criteria provided by EU and national legislation.~~~~

Article 22c

Individual file to be created for a long stay visa or residence permit issued

Where a decision has been taken to issue a long stay visa or residence permit, the competent authority that issued the long stay visa or residence permit shall add the following data to the individual application file ~~An individual file created pursuant to Article 22a(1) shall contain the following data, where the data is collected in accordance with the relevant Union and national legislation:~~

~~(1) the authority which issued the document, including its location;~~

~~(2) the following data of the holder:~~

~~(a) surname (family name); first name(s); date of birth; current nationality or nationalities; sex; date, place and country of birth;~~

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

~~(c) the date of expiry of the validity of the travel document;~~

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

~~(cd) a scan of the biographic data page of the travel document;~~

~~(d) in the case of minors, surname and first name(s) of the holder's parental authority or legal guardian;~~

~~(e) the surname, first name and address of the natural person or the name and address of the employer or any other organisation on which the application was based;~~

~~(f) a facial image of the holder, where possible taken live or a photograph;~~

~~(g) two fingerprints of the holder, in accordance with the relevant Union and national legislation;~~

~~(3) the following data concerning the long stay visa or residence permit issued:~~

(a) status information indicating that a long-stay visa or residence permit has been issued;

(aa) the authority that took the decision and its location;

(b) place and date of the decision ~~to issue the long stay visa or residence permit;~~

(c) the type of document issued (long-stay visa or residence permit);

(d) the number of the issued long-stay visa or residence permit;

(e) the commencement and expiry dates of the long-stay visa or residence permit.

Article 22d

Individual file to be created in certain cases of refusal of a long stay visa or residence permit

Where a decision has been taken to refuse a long stay visa or a residence permit because the applicant is considered to pose a threat to public policy, internal security or to public health or the applicant has presented documents which were fraudulently acquired, or falsified, or tampered with, the authority which refused it shall **add the following data to the individual application file create without delay an individual file with the following data,** where the data is collected in accordance with the relevant Union and national legislation:

- a. ~~surname, surname at birth (former surname(s)); first name(s); sex; date, place and country of birth;~~
- b. ~~current nationality/nationalities and nationality/nationalities at birth;~~
- e. ~~type and number of the travel document, the authority which issued it and the date of issue and of expiry;~~
- ea. a scan of the biographic data page of the travel document;**
- d. ~~in the case of minors, surname and first name(s) of the applicant's parental authority or legal guardian;~~
- e. ~~the surname, first name and address of the natural person on whom the application is based;~~
- f. ~~a facial image of the applicant, where possible taken live or a photograph;~~
- g. ~~two fingerprints of the applicant, in accordance with the relevant Union and national legislation;~~
- h. information indicating that the long-stay visa or residence permit has been refused because the applicant is considered to pose a threat to public policy, public security or to public health, or because the applicant presented documents which were fraudulently acquired, or falsified, or tampered with;
- i. the authority that refused the long-stay visa or residence permit, including its location;
- j. place and date of the decision to refuse the long stay-visa or residence permit.

Article 22e

Data to be added for a long stay visa or residence permit ~~withdrawn, revoked or annulled~~

1. Where a decision has been taken to ~~withdraw, revoke or annul~~ a ~~long-stay visa or~~ residence permit ~~or long-stay visa or to shorten the validity period of a long-stay visa~~, the authority that has taken the decision shall add the following data to the individual **application** file, where the data is collected in accordance with the relevant Union and national legislation:

- (a) ~~status information indicating that the long-stay visa or residence permit has been withdrawn, revoked or annulled or~~, ~~in the case of a long stay visa, that the validity period has been shortened;~~
- (b) ~~the authority that took the decision and withdrew the long-stay visa or residence permit or shortened the validity period of the long-stay visa, including~~ its location;
- (c) place and date of the decision.;
- (d) ~~the new expiry date of the validity of the long-stay visa or residence permit, where appropriate;~~
- (e) ~~the number of the visa sticker or residence permit, if the reduced period takes the form of a new visa sticker.~~

2. The individual file shall also indicate the ground(s) for ~~withdrawal, revocation or annulment of the long-stay visa or residence permit or shortening of the validity period of the long-stay visa~~, in accordance with ~~point (h) of Article 22d.~~

Article 22f

Data to be added for a long stay visa ~~or residence permit~~ extended or a residence permit renewed

Where a decision has been taken to extend the validity of ~~a residence permit or~~ a long-stay visa, the authority which extended it shall add the following data to the individual **application** file, where the data is collected in accordance with the relevant Union and national legislation:

- (a) status information indicating that the validity of the long-stay visa ~~or residence permit~~ has been extended;
- (b) the authority that took the decision and ~~extended the long-stay visa or residence permit,~~ ~~including~~ its location;
- (c) place and date of the decision;
- (d) ~~in the case of a long-stay visa, the number of the visa sticker, if the extension of the long-stay visa takes the form of a new visa sticker;~~
- (e) the expiry date of the validity of the long stay visa ~~extended period.~~

Where a decision has been taken to renew a residence permit Article 22c applies.

Article 22g

Access to data for verification of long stay visas and residence permits at external border crossing points

1. For the sole purpose of verifying the identity of the document holder and/or the authenticity and the validity of the long-stay visa or residence permit and whether the person is not considered to be a threat to public policy, internal security or public health of any of the Member States in accordance with Article 6(1)(e) of Regulation (EU) 2016/399, the competent authorities for carrying out checks at external border crossing points in accordance with that Regulation shall have access to search using the number of the document in combination with one or several of the data in Article 22c(2)(a), (b), ~~and (c)~~, (f) and (g) of this Regulation.

2. If the search with the data listed in paragraph 1 indicates that data on the document holder are recorded in the VIS, the competent border control authority shall be given access to consult the following data of the individual file, solely for the purposes referred to in paragraph 1:

- (a) the status information of the long-stay visa or residence permit indicating if it has been issued, withdrawn or extended;
- (b) data referred to in Article 22c(3)(c), (d), and (e);
- (c) where applicable, data referred to in Article 22e(1)(d) and (e);
- (d) ~~where applicable, data facial images or photographs as~~ referred to in Article 22f(d) ~~and (e) c(2)(f)~~;
- (e) ~~photographs~~ fingerprints as referred to in Article 22c(2)(fg).
- (f) if applicable, the **hitmatch(es)** pursuant to Article 22b(3) and the results of the verifications linked to those **hitmatches** pursuant to Article 9c.

Article 22h

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

1. For the sole purpose of verifying the identity of the holder and the authenticity and the validity of the long-stay visa or residence permit or whether the person is not a threat to public policy, internal security or public health of any of the Member States, 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 and, as applicable, police authorities, shall have access to search using the number of the long-stay visa or residence permit in combination with one or several of the data in Article 22c(2)(a), (b), ~~and (c)~~, (f) and (g).

2. If the search with the data listed in paragraph 1 indicates that data on the holder are recorded in the VIS, the competent authority shall be given access to consult the following data of the individual file ~~as well as, if applicable, of linked file(s) pursuant to Article 22a(4)~~, solely for the purposes referred to in paragraph 1:

- (a) the status information of the long-stay visa or residence permit indicating if it has been issued, withdrawn or extended;
- (b) data referred to in Article 22c(3)(c), (d), and (e);
- (c) where applicable, data referred to in Article 22e(1)(d) and (e);
- (d) where applicable, data referred to in Article 22f(d) and (e);
- (e) facial images or photographs as referred to in Article 22c(2)(f);
- (f) fingerprints as referred to in Article 22c(2)(g).

Article 22i

Access to data for determining the responsibility for applications for international protection

1. For the sole purpose of determining the Member State responsible for examining an application for international protection in accordance with Article 12 of Regulation (EU) No 604/2013, the competent asylum authorities shall have access to search with the fingerprints of the document holder for international protection.

Where the fingerprints of the document holder for international protection cannot be used or the search with the fingerprints fails, the search shall be carried out using the number of the long stay visa or residence permit in combination with one or several of the data in Article 22c(2)(a), (b) and (c) and (f). The facial image shall not be the only search criterion.

2. If the search with the data listed in paragraph 1 indicates that a long-stay visa or residence permit 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 linked application file(s) of the spouse and children, pursuant to Article 22a(34), for the sole purpose referred to in paragraph 1:

- (a) the authority that issued, refused, annulled, revoked or extended the long-stay visa or residence permit;
- (b) the data referred to in Article 22c(2)(a) and (b);
- (c) the type of document;
- (d) the period of validity of the long-stay visa or residence permit;
- (f) facial images or photographs as referred to in Article 22c(2)(f);
- (fa) fingerprints as referred to in Article 22c(2)(g);
- (g) the data referred to in Article 22c(2)(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 27 of Regulation (EU) No 603/2013 of the European Parliament and of the Council.

Article 22j

Access to data for examining the application for international protection

1. For the sole purpose of examining an application for international protection, the competent asylum authorities shall have access in accordance with Article 27 of Regulation (EU) No 603/2013 to search with the fingerprints of the document holder for international protection.

Where the fingerprints of the document holder for international protection cannot be used or the search with the fingerprints fails, the search shall be carried out using the number of the long stay visa or residence document in combination with one or several of the data in Article 22c(2)(a), (b) ~~and~~ (c) **and (f)**, or a combination of one or several data in Article 22d(a), (b), (c) and (f). The facial image shall not be the only search criterion.

2. If the search with the data listed in paragraph 1 indicates that data on the document holder for international protection is recorded in the VIS, the competent asylum authority shall have access to consult, for the sole purpose referred to in paragraph 1, the data entered in respect of any long-stay visa or residence permit issued, refused, withdrawn or whose validity is extended, referred to in Articles 22c, 22d, 22e and 22f of the document holder and of the linked application file(s) of the document holder pursuant to Article 22a(3).

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 27 of Regulation (EU) No 603/2013.

CHAPTER IIIb

Procedure and conditions for access to the VIS ~~for law enforcement purposes to prevent, detect or~~ investigate terrorist offences or other serious criminal offences

Article 22k

Member States' designated authorities

1. Member States shall designate the authorities which are entitled to consult the data stored in the VIS in order to prevent, detect ~~and~~ or investigate terrorist offences or other serious criminal offences.

2. Each Member State shall keep a list of the designated authorities. Each Member State shall notify the Management Authority ~~eu-LISA~~ and the Commission of its designated authorities and may at any time amend or replace its notification.

3. Each Member State shall designate a central access point which shall have access to the VIS. The central access point shall verify that the conditions to request access to the VIS laid down in Article 22n are fulfilled.

The designated authorities and the central access point may be part of the same organisation if permitted under national law, but the central access point shall act ~~fully~~ independently of the designated authorities when performing its tasks under this Regulation. The central access point ~~shall be separate independent from the designated authorities and~~ shall not receive instructions from ~~them~~ the designated authorities as regards the outcome of the verification which it shall perform independently.

Member States may designate more than one central access point to reflect their organisational and administrative structure in the fulfilment of their constitutional or legal requirements.

4. Each Member State shall notify the Management Authority ~~eu-LISA~~ and the Commission of its central access point and may at any time amend or replace its notification.

5. At national level, each Member State shall keep a list of the operating units within the designated authorities that are authorised to request access to data stored in the VIS through the central access point(s).

6. Only duly empowered staff of the central access point(s) shall be authorised to access the VIS in accordance with Articles 22m and 22n.

Article 22l

Europol

1. Europol shall designate one of its operating units as 'Europol designated authority' and shall authorise it to request access to the VIS through the VIS designated central access point referred to in paragraph 2 in order to support and strengthen action by Member States in preventing, detecting and investigating terrorist offences or other serious criminal offences.

2. Europol shall designate a specialised unit with duly empowered Europol officials as the central access point. The central access point shall verify that the conditions to request access to the VIS laid down in Article 22p are fulfilled.

The central access point shall act independently when performing its tasks under this Regulation and shall not receive instructions from the Europol designated authority referred to in paragraph 1 as regards the outcome of the verification.

Article 22m

Procedure for access to the VIS for law enforcement purposes

1. The operating units referred to in Article 22k(5) shall submit a reasoned electronic or written request to the central access points referred to in Article 22k(3) for access to data stored in the VIS. Upon receipt of a request for access, the central access point(s) shall verify whether the conditions for access referred to in Article 22n are fulfilled. If the conditions for access are fulfilled, the central access point(s) shall process the requests. The VIS data accessed shall be transmitted to the operating units referred to in Article 22k(5) in such a way as to not compromise the security of the data.
2. In a case of exceptional urgency, where there is a need to prevent an imminent danger to the life of a person associated with a terrorist offence or another serious criminal offence, the central access point(s) shall process the request immediately and shall only verify ex post whether all the conditions of Article 22n are fulfilled, including whether a case of urgency actually existed. The ex post verification shall take place without undue delay and in any event no later than 7 working days after the processing of the request.
3. Where an ex post verification determines that the access to VIS data was not justified, all the authorities that accessed such data shall erase the information accessed from the VIS and shall inform the central access points of the erasure.

Article 22n

Conditions for access to VIS data by designated authorities of Member States

1. Designated authorities shall have ~~may~~ access the VIS for consultation if all of the following conditions are met:
 - (a) access for consultation is necessary and proportionate for the purpose of the prevention, detection or investigation of a terrorist offences or another serious criminal offence;
 - (b) access for consultation is necessary and proportionate in a specific case;
 - (c) reasonable grounds exist to consider that the consultation of the VIS data will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category covered by this Regulation;
 - ~~(d) where a query to the CIR was launched in accordance with Article 22 of Regulation 2018/XX [on interoperability], the reply received as referred to in paragraph 5 of [Article 22 of Regulation reveals that data is stored in the VIS.]~~
- ~~2. The condition provided in point (d) of paragraph 1 does not need to be fulfilled for situations where the access to the VIS is needed as a tool to consult the visa history or the periods of authorised stay on the territory of the Member States of a known suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence.~~

3. Consultation of the VIS shall be limited to searching with any of the following data in the individual file:
 - (a) surname(s) (family name), first name(s) (given names), date of birth, nationality or nationalities and/or sex;
 - (b) type and number of travel document or documents, three letter code of the issuing country and date of expiry of the validity of the travel document;
 - (c) visa sticker number or number of the long-stay visa or residence document and the date of expiry of the validity of the visa, long-stay visa or residence document, as applicable;
 - (d) fingerprints, including latent fingerprints;
 - (e) facial image.
4. Consultation of the VIS shall, in the event of a **matchhit**, give access to the data listed in this paragraph as well as to any other data taken from the individual file, including data entered in respect of any document issued, refused, annulled, revoked or extended. Access to the data referred to in point (4)(1) of Article 9 as recorded in the application file shall only be given if consultation of that data was explicitly requested in a reasoned request and approved by independent verification.

Article 22o

Access to VIS for identification of persons in specific circumstances

By derogation from Article 22n(1), designated authorities shall not be obliged to fulfil the conditions laid down in that paragraph to access the VIS for the purpose of identification of persons who had gone missing, abducted or identified as victims of trafficking in human beings or persons who are not able to identify themselves or unidentified human remains, in the event of a natural disaster or an accident ~~natural disasters~~ and in respect of whom there are reasonable grounds to consider that consultation of VIS data will support their identification, and/or contribute in investigating specific cases of human trafficking. In such circumstances, the designated authorities may search in the VIS with the fingerprints of those persons.

Where the fingerprints of those persons cannot be used or the search with the fingerprints fails, the search shall be carried out with the data referred to in points (a) and (b) of Article 9(4) or points (a) and (b) of Article 22c(2) or Article 22d.

Consultation of the VIS shall, in the event of a **matchhit**, give access to any of the data in Article 9, Article 22c or Article 22d as well as to the data in Article 8(3) and (4) or Article 22a(3).

Article 22p

Procedure and conditions for access to VIS data by Europol

1. Europol shall have access to consult the VIS where all the following conditions are met:
 - (a) the consultation is necessary and proportionate to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences falling under Europol's mandate;
 - (b) the consultation is necessary and proportionate in a specific case;
 - (c) reasonable grounds exist to consider that the consultation of the VIS data will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category covered by this Regulation;
 - (d) where a query to the CIR was launched in accordance with Article 22 of Regulation 2018/XX [*on interoperability*], the reply received as referred to in Article 22(3) of that Regulation ~~reveals~~ indicates that data is stored in the VIS.
2. The conditions laid down in Article 22n(2), (3) and (4) shall apply accordingly.
3. Europol's designated authority may submit a reasoned electronic request for the consultation of all data or a specific set of data stored in the VIS to the Europol central access point referred to in Article 22l(2~~3~~). Upon receipt of a request for access the Europol central access point shall verify whether the conditions for access referred to in paragraphs 1 and 2 are fulfilled. If all conditions for access are fulfilled, the duly authorised staff of the central access point(s) shall process the requests. The VIS data accessed shall be transmitted to the operating units referred to in Article 22l(1) in such a way as not to compromise the security of the data.
4. The processing of information obtained by Europol from consultation with VIS data shall be subject to the authorisation of the Member State of origin. That authorisation shall be obtained via the Europol national unit of that Member State.

Article 22q

Logging and documentation

1. Each Member State and Europol shall ensure that all data processing operations resulting from requests to access to VIS data in accordance with Chapter III~~be~~ are logged or documented for the purposes of checking the admissibility of the request, monitoring the lawfulness of the data processing and data integrity and security, and self-monitoring.

2. The log or documentation shall show, in all cases:

- (a) the exact purpose of the request for access to VIS data, including the terrorist offence or other serious criminal offence concerned and, for Europol, the exact purpose of the request for access;
- (b) the national file reference;
- (c) the date and exact time of the request for access by the central access point to the VIS Central System;
- (d) the name of the authority which requested access for consultation;
- (e) where applicable, the decision taken with regard to the ex-post verification;
- (f) the data used for consultation;
- (g) in accordance with national rules or with Regulation (EU) 2016/794, the unique user identity of the ~~official~~ duly authorised staff who carried out the search and of the official who ordered the search.

3. Logs and documentation shall be used only for monitoring the lawfulness of data processing and for ensuring data integrity and security. Only logs which do not contain personal data may be used for the monitoring and evaluation referred to in Article 50 of this Regulation. The supervisory authority ~~established~~ designated in accordance with Article 41(1) of Directive (EU) 2016/680, which is responsible for checking the admissibility of the request and monitoring the lawfulness of the data processing and data integrity and security, shall have access to these logs at its request for the purpose of fulfilling its duties.

Article 22r

Conditions for access to VIS data by designated authorities of a Member State in respect of which this Regulation has not yet been put into effect

1. Access to the VIS for consultation by designated authorities of a Member State in respect of which this Regulation has not yet been put into effect shall take place where the following conditions are met:

- (a) the access is within the scope of their powers;
- (b) the access is subject to the same conditions as referred to in Article 22n(1);
- (c) the access is preceded by a duly reasoned written or electronic request to a designated authority of a Member State to which this Regulation applies; that authority shall then request the national central access point(s) to consult the VIS.

2. A Member State in respect of which this Regulation has not yet been put into effect shall make its visa information available to Member States to which this Regulation applies, on the basis of a duly reasoned written or electronic request, subject to compliance with the conditions laid down in Article 22n(1).

* Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 180, 29.6.2013, p. 1).

CHAPTER IV

RETENTION AND AMENDMENT OF THE DATA

Article 23

Retention period for data storage

1. Each 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, the long-stay visa or the residence permit, if a visa, a long-stay visa or a residence permit has been issued;

(b) on the new expiry date of the visa, the long-stay visa ~~or the residence permit~~, if a visa, or a long-stay visa ~~or a residence permit~~ has been extended;

(c) on the date of the ~~creation of the application file~~ creation of the withdrawal by the document holder applicant or the decision of the responsible authority in the VIS, if the application has been withdrawn, closed or discontinued;

(d) on the date of the decision of the responsible authority if a visa, a long-stay visa or a residence permit has been refused, annulled, ~~shortened~~, withdrawn or revoked, as applicable.

2. Upon expiry of the period referred to in paragraph 1, the VIS shall automatically erase the file and the link(s) to this file as referred to in Article 8(3) and (4) and Article ~~22a~~22a(3) ~~and (5)~~.

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 shall be transmitted in accordance with the procedure in Article 16(3).

Where the inaccurate data refers to links created pursuant to Article 8(3) or (4), and Article 22a(3), or where a link is missing, the responsible Member State shall make the necessary verifications and provide an answer within 3 working days ~~48 hours~~, and, as the case may be, rectify the link. If no answer is provided within the set timeframe, the requesting Member State shall rectify the link and notify the responsible Member State of the rectification made via VISMail.

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, the files and the links referred to in Article 8(3) and (4) and in, Article 22a(3) relating to him or her shall be erased 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 shall ~~may~~ be transmitted by the VISMail.

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.

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

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 (⁹), 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.

8a. ~~The Management Authority Eu-LISA~~ shall be permitted to use anonymised real personal data of the ~~VIS production~~ system for testing purposes in the following circumstances:

(a) for diagnostics and repair when faults are discovered with the ~~Central System~~ VIS operation;

(b) for testing new technologies and techniques relevant to ~~enhance the performance of the Central System or transmission of data to it~~ the VIS operation.

In such cases, the security measures, access control and logging activities at the testing environment shall be equal to the ones for the ~~VIS production~~ system. Real personal data adopted for testing shall be rendered anonymous in such a way that the data-subject is no longer identifiable.

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 (¹⁰), 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, shall be located in Sankt Johann im Pongau (Austria).

Both sites may be used simultaneously for active operation of the VIS provided that the second site remains capable of ensuring its operation in case of failure of the system.

[...]

Article 29

Responsibility for the use and quality 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, up-to-date and of an adequate level of quality and completeness 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 or the CIR and the communication infrastructure between the central VIS or the CIR 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.

2a. The management authority together with the Commission shall develop and maintain automated data quality control mechanisms and procedures for carrying out quality checks on the data in VIS and shall provide regular reports to the Member States. The management authority shall also provide a ~~regular~~ report at least once a year to the Member States and Commission on the data quality controls.

This mechanism, procedures and the interpretation of data quality compliance shall be established by means of implementing measures in accordance with the procedure referred to in Article 49(2).

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 29a

Specific rules for entering data

1. Entering data referred to in Articles 9, 22c and 22d into the VIS shall be subject to the following ~~preliminary~~ conditions:

(a) data pursuant to Articles 9, 22c and 22d and Article 6(4) may only be sent to the VIS following a quality check performed by the responsible national authorities;

(b) data pursuant to Articles 9, 22c and 22d and Article 6(4) will be processed by the VIS, following a quality check performed by the VIS pursuant to paragraph 2.

2. Quality checks shall be performed by VIS, as follows:

(a) when creating application files or files of third country nationals in VIS, quality checks shall be performed on the data referred to in Articles 9, 22c and 22d; should these checks fail to meet the established quality criteria, the responsible authority(ies) shall be automatically notified by the VIS;

(b) the automated procedures pursuant to Article 9(a)(3) and 22b(2) may be triggered by the VIS only following a quality check performed by the VIS pursuant to this Article; should these checks fail to meet the established quality criteria, the responsible authority(ies) shall be automatically notified by the VIS;

(c) quality checks on facial images and fingerprints ~~daetylographic data~~ shall be performed when creating application files of third country nationals in VIS, to ascertain the fulfilment of minimum data quality standards allowing biometric matching;

(d) quality checks on the data pursuant to Article 6(4) shall be performed when storing information on the national designated authorities in the VIS.

3. Quality standards shall be established for the storage of the data referred to in paragraph 1 and 2 of this Article. The specification of these standards shall be laid down in implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 49(2).

[...]

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.

By way of derogation from the first subparagraph, and without prejudice to Regulation (EU) 2016/679, the data referred to in Article 9(4)(a) to ,-(b), (e), (cc), (k) and (m); and Article 9(6) and 9(7) or Article 22c(2)(a) to ,-(b), (e), (ee), (d), (g) and (h) or Article 22d(a) to ,-(b), (e), (ee), (d) and (g) may be transferred or made available to a third country or to an international organisation listed in the Annex, only if necessary in individual cases for the purpose of proving the identity of third-country nationals, and only for the purpose of return in accordance with Directive 2008/115/EC, or of resettlement in accordance with the Regulation ...[Resettlement Framework Regulation], or of national resettlement schemes and provided that the Member State which entered the data in the VIS has given its approval.

~~¹⁸2. 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.~~

2. Personal data obtained from the VIS by a Member State or by Europol to prevent, detect or investigate terrorist offences or other serious criminal offences for law enforcement purposes shall not be transferred or made available to any third country, international organisation or private entity established in or outside the Union. The prohibition shall also apply where those data are further processed at national level or between Member States pursuant to Directive (EU) 2016/680.

3. By way of derogation from paragraph 2, the data referred to in points (a) to (cc) of Article 9(4), points (a) to (cc) of Article 22c(2), points (a) to (c) of Article 22d may be transferred by the designated authority to a third country or international organisation in individual cases, only where all of the following conditions are met:

¹⁸ This deletion is suggested by the Commission in its proposal.

(a) there is an exceptional case of urgency where there is:

(i) an imminent danger associated with a terrorist offence; or

(ii) an imminent danger to the life of a person and that danger is associated with a serious criminal offence;

(b) the transfer of data is necessary for the prevention, detection or investigation in the territory of the Member States or in the third country concerned of such a terrorist offence or serious criminal offence;

(c) the designated authority has access to such data in accordance with the procedure and the conditions set out in Articles 22m and 22n;

(d) the transfer is carried out in accordance with the applicable conditions set out in Directive (EU) 2016/680, in particular Chapter V thereof;

(e) a duly motivated written or electronic request from the third country has been submitted.

Where a transfer is made pursuant to the first subparagraph of this paragraph, such a transfer shall be documented and the documentation shall, on request, be made available to the supervisory authority established in accordance with Article 41(1) of Directive (EU) 2016/680, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.

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 34

Keeping of logs

1. Each Member State, the European Border and Coast Guard Agency and the Management Authority shall keep logs of all **their** data processing operations within the VIS. These logs shall show the purpose of access referred to in Article 6(1), Article 6b20a(1), Article 22k(1) and Articles 15 to 22 and 22g to 22j, 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 Article 15(2), Article 18, Article 19(1), Article 6a20(1), Article 21(1), Article 22(1), Article 22g, Article 22h, Article 22i, Article 22j, Article 45a, and Article 45d and the name of the authority entering or retrieving the data. In addition, each Member State shall keep logs of the staff duly authorised to enter or retrieve the data.

2. For the operations listed in Article 45b a log of each data processing operation carried out within the VIS and the EES shall be kept in accordance with this Article and Article 41 of the Regulation (EU) 2017/2226 establishing an Entry/Exit System (EES).

3. Such logs may be used only for the data-protection monitoring of the admissibility of data processing as well as to ensure data security. The logs shall be protected by appropriate measures against unauthorised access and modification and shall be 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.

[...]

CHAPTER VI

RIGHTS AND SUPERVISION ON DATA PROTECTION

Article 36a¹⁹

Data protection

1. Regulation (EC) No 45/2001 shall apply to the processing of personal data by the European Border and Coast Guard Agency and the Management Authority.

2. Regulation (EU) 2016/679 shall apply to the processing of personal data by the visa authorities assessing applications and carrying out verifications pursuant to Articles 9c *[and ...]*²⁰ and 22b, by border authorities and by immigration authorities.

Where the processing of personal data is performed by competent authorities assessing the applications for the purposes of the prevention, detection or investigation of terrorist offences or other serious criminal offences, Directive (EU) 2016/680 shall apply.

Where the visa authority decides on the issue, refusal, revocation or annulment of a visa, Regulation (EU) 2016/679 shall apply.

3. Directive (EU) 2016/680 shall apply to the processing of personal data by Member States' designated authorities for the purposes of Article 2(1)(h) and 2(2)(c) of this Regulation.

4. Regulation (EU) 2016/794 shall apply to the processing of personal data by Europol pursuant to Articles 9ca and 22b of this Regulation.

Article 36b²¹

Data processor

1. The European Border and Coast Guard Agency and the Management Authority, respectively, are to be considered processor in accordance with point (e) of Article 2 of Regulation (EC) No 45/2001 in relation to the processing of personal data in the VIS.

2. The Management Authority shall ensure that the VIS is operated in accordance with this Regulation.

¹⁹ Was 38a in the previous version. No substantial changes otherwise.

²⁰ To be added when the respective provisions are agreed.

²¹ Was 38b in the previous version. No substantial changes otherwise.

Article 37

Right of information

1. Third country nationals and the persons referred to in Articles 9(4)(f), ~~22c(2)(e) or 22d(e)~~ 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~~ 22k and Europol;

*(ca) the fact that the VIS may be accessed by the Member States and Europol **to prevent, detect or investigate terrorist offences or other serious criminal offences** ~~for law enforcement purposes~~;*

(d) the data retention period;

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

(ea) the fact that personal data stored in the VIS may be transferred to a third country or an international organisation in accordance with Article 31 and to Member States in accordance with Council Decision (EU) 2017/1908;*

(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 third country national when the data, the facial image photograph and the fingerprint data as referred to in points (4), (5) and (6) of Article 9, Article 22c(2) and Article 22d (a) to (g) are collected, and where necessary, orally, in a language and manner that the data subject understands or is reasonably presumed to understand. Children must be informed in an age-appropriate manner, ~~using leaflets, and/or infographics and/or demonstrations specifically designed to explain the fingerprinting procedure.~~

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 14 of Regulation (EU) 2016/679.

* COUNCIL DECISION (EU) 2017/1908 of 12 October 2017 on the putting into effect of certain provisions of the Schengen acquis relating to the Visa Information System in the Republic of Bulgaria and Romania

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 Articles 15, 16 and 17 of Regulation (EU) 2016/679, Articles 14, 15 and 16 of Directive (EU) 2016/680, Article 47 of Regulation [XXX] on SIS in the field of border checks, Article 65 of Regulation [XXX] on SIS in the field of police cooperation and judicial cooperation in criminal matters and Interpol's Rules on the Processing of Personal Data~~, 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 **for the application**, the authorities of the Member State with which the request was lodged shall contact the authorities of the Member State responsible **for the application** within a period of seven 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.

3a. A Member State responsible for the application may provide to the data subject information concerning any of the data subject's personal data in other databases queried only if the Member States/Europol which entered the data in the in the queried database first gives the Member State responsible for the application an opportunity to state its position.

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.*

7. A Member State shall take a decision not to provide information to the data subject, in whole or in part, in accordance with national law, to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the data subject concerned, in order to:

(a) avoid obstructing official or legal inquiries, investigations or procedures;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect public security;

(d) protect national security; or

(e) protect the rights and freedoms of others.

In cases referred to in the first subparagraph, the Member State shall inform the data subject in writing, without undue delay, of any refusal or restriction of access and of the reasons for the refusal or restriction. Such information may be omitted where its provision would undermine any of the reasons set out in points (a) to (e) of the first subparagraph. The Member State shall inform the data subject of the possibility of lodging a complaint with a supervisory authority or of seeking a judicial remedy.

The Member State shall document the factual or legal reasons on which the decision not to provide information to the data subject is based. That information shall be made available to the supervisory authorities.

For such cases, the data subject shall also be able to exercise his or her rights through the competent supervisory authorities.

**Article 38a²²
Data protection**

~~1. Regulation (EC) No 45/2001 shall apply to the processing of personal data by the European Border and Coast Guard Agency and the Management Authority.~~

~~2. Regulation (EU) 2016/679 shall apply to the processing of personal data by the central visa authorities assessing applications and carrying out verifications pursuant to Articles 9c *and ...*²³ and 22b, by border authorities and by immigration authorities.~~

~~Where the processing of personal data is performed by competent authorities assessing the applications for the purposes of the prevention, detection or investigation of terrorist offences or other serious criminal offences, Directive (EU) 2016/680 shall apply.~~

~~Where the visa authority decides on the issue, refusal, revocation or annulment of a visa, Regulation (EU) 2016/679 shall apply.~~

²² Moved upwards (new 36a).

²³ To be added when the respective provisions are agreed.

~~3. Directive (EU) 2016/680 shall apply to the processing of personal data by Member States' designated authorities for the purposes of Article 2(1)(h) and 2(2)(e) of this Regulation.~~

~~4. Regulation (EU) 2016/794 shall apply to the processing of personal data by Europol pursuant to Articles 9ea and 22b of this Regulation.~~

Article 38b²⁴

Data processor

~~1. The European Border and Coast Guard Agency and the Management Authority, respectively, are to be considered processor in accordance with point (e) of Article 2 of Regulation (EC) No 45/2001 in relation to the processing of personal data in the VIS.~~

~~2. The Management Authority shall ensure that the VIS is operated in accordance with this Regulation.~~

[...]

Article 43

Cooperation between National Supervisory Authorities and the European Data Protection Supervisor

1. The European Data Protection Supervisor shall act in close cooperation with national supervisory authorities with respect to specific issues requiring national involvement, in particular if the European Data Protection Supervisor or a national supervisory authority finds major discrepancies between practices of Member States or finds potentially unlawful transfers using the communication channels of the interoperability components, or in the context of questions raised by one or more national supervisory authorities on the implementation and interpretation of this Regulation.

2. In the cases referred to in paragraph 1, coordinated supervision shall be ensured in accordance with Article 62 of Regulation (EU) XXXX/2018 [revised Regulation 45/2001].

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.

[...]

²⁴ Moved upwards (new 36b).

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.

3. The technical specifications for the quality, resolution and use of fingerprints and of the facial image for biometric verification and identification in the VIS shall be laid down in implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 49(2).

Article 45a

Use of data for reporting and statistics

1. The duly authorised staff of the competent authorities of Member States, the Commission, the Management Authority ~~eu-LISA~~ and the European Border and Coast Guard Agency established by Regulation (EU) 2016/1624 shall have access to consult the following data, solely for the purposes of reporting and statistics without allowing for individual identification:

(a) status information;

(b) the competent authority, including its location;

(c) sex, date of birth and ~~current~~ nationalities of the applicant;

(d) Member State of first entry, only as regards ~~short-stay~~ visas, if applicable;

- (e) date and place of the application and the decision concerning the application (issued or refused)²⁵;
- (f) the type of document issued, i.e. whether airport transit visa ATV, uniform or limited territorial validity visa LTV, long stay visa or residence permit;
- (g) the type of the travel document ~~and the three letter code of the issuing country~~, only as regards ~~short stay~~ visas;
- (h) the grounds indicated for any decision concerning the document or the application, only as regards ~~short stay~~ visas; as regards long stay visas and residence permits, the decision concerning the application (whether to issue or to refuse the application and on which ground);
- (i) the competent authority, including its location, which refused the application and the date of the refusal, only as regards ~~short stay~~ visas;
- (j) the cases in which the same applicant applied for a ~~short stay~~ visa from more than one visa authority, indicating these visa authorities, their location and the dates of refusals, ~~only as regards short stay visas~~;
- (k) ~~As regards short stay visas~~, main purpose(s) of the journey; ~~as regards long stay visas and residence permit, the purpose of the application~~;
- (ka) visa applications processed in representation pursuant to Article 8 of Regulation (EC) No 810/2009;
 - (l) the data entered in respect of any document withdrawn, annulled, revoked or whose validity is extended, as applicable;
 - (m) ~~where applicable~~, the expiry date of the long stay visa or residence permit;
 - (n) the number of persons exempt from the requirement to give fingerprints pursuant to Article 13(7) of Regulation (EC) No 810/2009.
 - (o) 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);
 - (p) 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);
 - (q) 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);~~;~~

²⁵ Revert the original Commission proposal (i.e. no change).

- (r) the cases in which a person who applied for a visa, a long-stay visa or a residence permit are found in Eurodac in the course of the query in accordance with Article 9a(3) or 22b(2):
- (s) as regards visas, links to the previous application file on that applicant as well as links of the application files of the persons travelling together.

~~A technical solution shall be made available to Member States in order to facilitate the querying of VIS for the purpose of managing users request and generating statistics. The Commission shall adopt implementing acts concerning the specifications of the technical solution. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 49(2).²⁶~~

The duly authorised staff of the European Border and Coast Guard Agency shall have access to consult the data referred to in the first subparagraph for the purpose of carrying out risk analyses and vulnerability assessments as referred to in Articles 11 and 13 of Regulation (EU) 2016/1624.

2. For the purpose of paragraph 1 of this Article, the Management Authority eu-LISA shall store the data referred to in that paragraph in the central repository for reporting and statistics referred to in [Article 39 of the Regulation 2018/XX *[on interoperability]*]

3. The procedures put in place by the Management Authority eu-LISA to monitor the functioning of the VIS referred to in Article 50(1) shall include the possibility to produce regular statistics for ensuring that monitoring.

4. Every quarter, the Management Authority eu-LISA shall compile statistics based on the VIS data on ~~short-stay~~ visas referred to in Article 4, point 1 showing, for each location where a visa was lodged, in particular:

- (a) ~~total of airport transit visas applied for, including for multiple entry airport transit visas~~ number of airport transit (A) visas, as referred to in point 5 of Article 2 of Regulation (EC) No 810/2009, applied for; number of A visas issued, disaggregated by single airport transit and multiple airport transits; number of A visas refused;
- (b) ~~total of visas issued, including multiple entry airport transit A visas~~ number of short-stay (C) visas, as referred to in point 2(a) of Article 2 of Regulation (EC) No 810/2009, applied for (and disaggregated by the main purpose of the journey); number of C visas issued, disaggregated by issued for single entry or multiple entry and the latter divided by length of validity (6 months or below, 1 year, 2 years, 3 years, 4 years, 5 years); number of visas with limited territorial validity issued (LTV); number of C visas refused;
- (c) ~~total of multiple entry visas issued;~~
- (d) ~~total of visas not issued, including multiple entry airport transit A visas;~~

²⁶ Moved back to Art. 50 (In EES, ETIAS and also in Interoperability, it is under the monitoring).

- ~~(e) total of uniform visas applied for, including multiple entry uniform visas;~~
- ~~(f) total of visas issued, including multiple entry visas;~~
- ~~(g) total of multiple entry visas issued, divided by length of validity (below 6 months or below, 1 year, 2 years, 3 years, 4 years, 5 years);~~
- ~~(h) total of uniform visas not issued, including multiple entry visas;~~
- ~~(i) total of visas with limited territorial validity issued.~~

The daily statistics shall be stored in the central repository for reporting and statistics.

5. Every quarter, the Management Authority ~~eu-LISA~~ shall compile statistics based on the VIS data on long-stay visas and residence permits showing, for each location, in particular:

- (a) total of long-stay visas applied for, issued, refused, extended and withdrawn;
- (b) total of residence permits applied for, issued, refused, extended and withdrawn.

6. At the end of each year, statistical data shall be compiled in the form of quarterly statistics for that year. The statistics shall contain a breakdown of data for each Member State.

7. At the request of the Commission, the Management Authority ~~eu-LISA~~ shall provide it with statistics on specific aspects related to the implementation of the common visa policy or of the migration and asylum policy, including on aspects pursuant to the application of Regulation (EU) No 1053/2013.

Article 45b

Access to data for verification by carriers

1. In order to fulfil their obligation under point (b) of Article 26(1) of the Convention implementing the Schengen Agreement, air carriers, sea carriers and international carriers transporting groups overland by coach ~~or train~~²⁷ shall send a query to the VIS in order to verify whether or not third country nationals ~~holding a subject to short stay visa, a long stay visa or a residence permit requirement~~ are in possession of a valid ~~short stay visa, long stay visa or residence permit, as applicable. For this purpose, as regards short stay visas, carriers shall provide the data listed under points (a), (b) and (c) of Article 9(4) of this Regulation and~~ or, as regards long stay visa or residence permit the data listed under points (a), (b) and (c) of Article 22c, ~~as applicable.~~

2. For the purpose of implementing paragraph 1 or for the purpose of resolving any potential dispute arising from its application, the Management Authority ~~eu-LISA~~ shall keep logs of all data processing operations carried out within the carrier gateway by carriers. Those logs shall show the date and time of each operation, the data used for interrogation, the data transmitted by the carrier gateway and the name of the carrier in question.

Logs shall be stored for a period of two years. Logs shall be protected by appropriate measures against unauthorised access.

²⁷ Revert the original Commission proposal (i.e. no change).

3. Secure access to the carrier gateway referred to in Article 1(2)(h) of Decision 2004/512/EC ~~as amended by this Regulation~~ shall allow carriers to proceed with the query consultation referred to in paragraph 1 prior to the boarding of a passenger. For this purpose, the carrier shall send the query to be permitted to consult the VIS using the data contained in the machine readable zone of the travel document.

4. The VIS shall respond by indicating whether or not the person has a valid visa, long-stay visa or residence permit, providing the carriers with an OK/NOT OK answer.

5. An authentication scheme, reserved exclusively for carriers, shall be set up in order to allow access to the carrier gateway for the purposes of paragraph 2 to the duly authorised members of the carriers' staff. The authentication scheme shall be adopted by the Commission by means of implementing acts in accordance with the examination procedure referred to in Article 49(2).

Article 45c

Fall-back procedures in case of technical impossibility to access data by carriers

1. Where it is technically impossible to proceed with the consultation query referred to in Article 45b(1), because of a failure of any part of the VIS or for other reasons beyond the carriers' control, the carriers shall be exempted of the obligation to verify the possession of holding a valid visa, long-stay visa or residence permit ~~travel document~~ by using the carrier gateway. Where such failure is detected by the Management Authority, it shall notify the carriers and the Member States. It shall also notify the carriers when the failure is remedied. Where such failure is detected by the carriers, they may notify the Management Authority. The Management Authority shall inform the Member States without delay about the notification of the carriers.

2. The details of the fall-back procedures shall be laid down in an implementing act adopted in accordance with the examination procedure referred to in Article 49(2).

Article 45d

Access to VIS data by European Border and Coast Guard teams

1. To exercise the tasks and powers pursuant to Article 40(1) of Regulation (EU) 2016/1624 of the European Parliament and of the Council* and in addition to the access provided for in Article 40(8) of that Regulation, the members of the European Border and Coast Guard teams, as well as teams of staff involved in return-related operations, shall, within their mandate, have the right to access and search data entered in VIS.

2. To ensure the access referred to in paragraph 1, the European Border and Coast Guard Agency shall designate a specialised unit with duly empowered European Border and Coast Guard officials as the central access point. The central access point shall verify that the conditions to request access to the VIS laid down in Article 45e are fulfilled.

Article 45e

Conditions and procedure for access to VIS data by European Border and Coast Guard teams

1. In view of the access referred to in paragraph 1 of Article 45d, a European Border and Coast Guard team may submit a request for the consultation of all data or a specific set of data stored in the VIS to the European Border and Coast Guard central access point referred to in Article 45d(2). The request shall refer to the operational plan on border checks, border surveillance and/or return of that Member State on which the request is based. Upon receipt of a request for access, the European Border and Coast Guard central access point shall verify whether the conditions for access referred to in paragraph 2 are fulfilled. If all conditions for access are fulfilled, the duly authorised staff of the central access point shall process the requests. The VIS data accessed shall be transmitted to the team in such a way as not to compromise the security of the data.
2. For the access to be granted, the following conditions shall apply:
 - a) the host Member State authorises the members of the team to consult VIS in order to fulfil the operational aims specified in the operational plan on border checks, border surveillance and return, and
 - b) the consultation of VIS is required for performing the specific tasks entrusted to the team by the host Member State.
3. In accordance with Article 40(3) of Regulation (EU) 2016/1624, members of the teams, as well as teams of staff involved in return-related tasks may only act in response to information obtained from the VIS under instructions from and, as a general rule, in the presence of border guards or staff involved in return-related tasks of the host Member State in which they are operating. The host Member State may authorise members of the teams to act on its behalf.
4. In case of doubt or if the verification of the identity of the visa holder, long stay visa holder or residence permit holder fails, the member of the European Border and Coast Guard team shall refer the person to a border guard of the host Member State.
5. Consultation of the VIS data by members of the teams shall take place as follows:
 - a) When exercising tasks related to border checks pursuant to Regulation (EU) 2016/399, the members of the teams shall have access to VIS data for verification at external border crossing points in accordance with Articles 18 or 22g of this Regulation respectively;
 - b) When verifying whether the conditions for entry to, stay or residence on the territory of the Member States are fulfilled, the members of the teams shall have access to the VIS data for verification within the territory of third country nationals in accordance with Articles 19 or 22h of this Regulation respectively;
 - c) When identifying any person that may not or may no longer fulfil the conditions for the entry to, stay or residence on the territory of the Member States, the members of the teams shall have access to VIS data for identification in accordance with Article ~~6a20~~ of this Regulation.

6. Where such access and search reveal the existence of a **matchhit** in VIS, the host Member State shall be informed thereof.

7. Every log of data processing operations within the VIS by a member of the European Border and Coast Guard teams or teams of staff involved in return-related tasks shall be kept by the Management Authority in accordance with the provisions of Article 34.

8. Every instance of access and every search made by the European Border and Coast Guard Agency shall be logged in accordance with the provisions of Article 34 and every use made of data accessed by the European Border and Coast Guard Agency shall be registered.

9. Except where necessary to perform the tasks for the purposes of the Regulation establishing a European Travel Information and Authorisation System (ETIAS), no parts of VIS shall be connected to any computer system for data collection and processing operated by or at the European Border and Coast Guard Agency nor shall the data contained in VIS to which the European Border and Coast Guard Agency has access be transferred to such a system. No part of VIS shall be downloaded. The logging of access and searches shall not be construed as constituting to be the downloading or copying of VIS data.

10. Measures to ensure security of data as provided for in Articles 32 shall be adopted and applied by the European Border and Coast Guard Agency.

[...]

Article 49

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011 of the European Parliament and of the Council*.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply. Where the Committee delivers no opinion, the Commission shall not adopt the draft implementing act and the third subparagraph of Article 5(4) of Regulation (EU) No 182/2011 shall apply.

Article 49a

~~Advisory group~~

~~An Advisory Group shall be established by eu LISA and provide it with the expertise related to the VIS in particular in the context of the preparation of its annual work programme and its annual activity report.~~

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. Every two years ~~the Management Authority~~ ~~eu-LISA~~ shall submit to the European Parliament, the Council and the Commission a report on the technical functioning of VIS, including the security thereof.
4. While respecting the provisions of national law on the publication of sensitive information, ~~and without prejudice to limitations necessary to protect security and public order, prevent crime and guarantee that any national investigation will not be jeopardised~~²⁸, each Member State and Europol shall prepare annual reports on the effectiveness of access to VIS data for ~~law enforcement~~ purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences, containing information and statistics on:
 - (t) the exact purpose of the consultation including the type of terrorist or serious criminal offence;
 - (u) reasonable grounds given for the substantiated suspicion that the suspect, perpetrator or victim is covered by this Regulation;
 - (v) the number of requests for access to the VIS for law enforcement purposes;
 - (w) the number and type of cases which have ended in successful identifications.

Member States' and Europol's annual reports shall be transmitted to the Commission by 30 June of the subsequent year.

4a. A technical solution shall be made available to Member States in order to facilitate the querying of VIS for the purpose of managing users request and generating statistics. The Commission shall adopt implementing acts concerning the specifications of the technical solution. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 49(2).²⁹

5. Every four years, 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.

²⁸ Revert the original Commission proposal (i.e. no change). This is because to provision is an agreed language (cf. Art. 72(8) of the EES Regulation).

²⁹ Moved back from Art. 45a.

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 5.

ANNEX

List of international organisations referred to in Article 31(1)

Article 2

Amendments to Decision 2004/512/EC

Council Decision 2004/512/EC establishing the Visa Information System (VIS) is amended as follows:

Article 1

1. A system for the exchange of visa data between Member States, hereinafter referred to as ‘the Visa Information System’ (VIS), is hereby established, which shall enable authorised national authorities to enter and update visa data and to consult these data electronically.

2. The Visa Information System shall be based on a centralised architecture and consist of:

(a) the common identity repository as referred to in [Article 17(2)(a) of Regulation 2018/XX on interoperability],

(b) a central information system, hereinafter referred to as ‘the Central Visa Information System’ (VIS),

(c) an interface in each Member State, hereinafter referred to as ‘the National Interface’ (NI-VIS) which shall provide the connection to the relevant central national authority of the respective Member State, or a National Uniform Interface (NUI) in each Member State based on common technical specifications and identical for all Member States enabling the Central System to connect to the national infrastructures in Member States,

(d) a communication infrastructure between the VIS and the National Interfaces;

(e) a Secure Communication Channel between the VIS and the EES Central System;

(f) a secure communication infrastructure between the VIS Central System and the central infrastructures of the European search portal established by [Article 6 of Regulation 2017/XX on interoperability], shared biometric matching service established by [Article 12 of Regulation 2017/XX on interoperability], the common identity repository established by [Article 17 of Regulation 2017/XX on interoperability] and the multiple-identity detector (MID) established by [Article 25 of Regulation 2017/XX on interoperability];

(g) a mechanism of consultation on applications and exchange of information between central visa authorities ('VISMail');

(h) a carrier gateway;

(i) a secure web service enabling communication between the VIS, on the one hand and ~~the~~ the carrier gateway, and the international systems (Interpol systems/databases), on the other hand;

(j) a repository of data for the purposes of reporting and statistics.

The Central System, the National Uniform Interfaces, the web service, the carrier gateway and the Communication Infrastructure of the VIS shall share and re-use as much as technically possible the hardware and software components of respectively the EES Central System, the EES National Uniform Interfaces, the ETIAS carrier gateway, the EES web service and the EES Communication Infrastructure).

Article 3

Amendments to Regulation (EU) No 810/2009

Regulation (EU) No 810/2009 is amended as follows:

Article 10

General rules for lodging an application

1. Without prejudice to the provisions of Articles 13, 42, 43 and 45, applicants shall appear in person when lodging an application.

2. Consulates may waive the requirement referred to in paragraph 1 when the applicant is known to them for his integrity and reliability.

3. When lodging the application, the applicant shall:

(a) present an application form in accordance with Article 11;

(b) present a travel document in accordance with Article 12;

(c) present a photograph in accordance with the standards set out in Regulation (EC) No 1683/95, ~~unless his facial image is being taken live in accordance with Article 13; or, upon a first application and subsequently at least every 59 months following that, in accordance with the standards set out in Article 13 of this Regulation.~~

(ca) as a general rule, allow his facial image, as defined in point 15 of Article 4 of the VIS Regulation, taken live in accordance with Article 13, ~~where applicable;~~

(d) allow the collection of his fingerprints in accordance with Article 13, where applicable;

(e) pay the visa fee in accordance with Article 16;

(f) provide supporting documents in accordance with Article 14 and Annex II;

(g) where applicable, produce proof of possession of adequate and valid travel medical insurance in accordance with Article 15.

Article 13

Biometric identifiers

1. Member States shall collect biometric identifiers of the applicant comprising a facial image photograph of him and his 10 fingerprints in accordance with the safeguards laid down in the Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms, in the Charter of Fundamental Rights of the European Union and in the United Nations Convention on the Rights of the Child.

2. At the time of submission of the first application and subsequently at least every 59 months thereafter, the applicant shall be required to appear in person. At that time, the following biometric identifiers of the applicant shall be collected:

- a facial image taken live as defined in point 15 of Article 4 of the VIS Regulation ~~a photograph taken live and collected digitally at the time of the application;~~
- his 10 fingerprints taken flat and collected digitally.

3. Where fingerprints and a live facial image ~~live photograph~~ of sufficient quality were collected from the applicant and entered in the VIS as part of an application lodged less than 59 months before the date of the new application, these {data} may be copied to the subsequent application; otherwise these data must be collected anew. Before copying a facial image, the changes of the applicants' appearance, in particular in cases of young children shall be taken into consideration whenever possible.

However, where there is reasonable doubt regarding the identity of the applicant, the consulate shall collect fingerprints within the period specified in the first subparagraph.

Furthermore, if at the time when the application is lodged, it cannot be immediately confirmed that the fingerprints were collected within the period specified in the first subparagraph, **the applicant may request that they shall be collected again.**

~~4. In accordance with Article 9(5) of the VIS Regulation, the The photograph attached to each application shall be entered in the VIS. The applicant shall not be required to appear in person for this purpose.~~

~~The technical requirements for the photograph shall be in accordance with the international standards as set out in the International Civil Aviation Organization (ICAO) document 9303 Part 1, 6th edition.~~

The facial image of third country nationals referred to in paragraph 2 shall have sufficient image resolution and quality to be used in automated biometric matching.³⁰

~~5. Fingerprints shall be taken in accordance with ICAO standards and Commission Decision 2006/648/EC of 22 September 2006 laying down the technical specifications on the standards for biometric features related to the development of the Visa Information System (20).~~

³⁰ Moved from point 8 of Article 9 of the VIS proposal.

6. *The biometric identifiers shall be collected by qualified and duly authorised staff of the authorities competent in accordance with Article 4(1), (2) and (3). Under the supervision of the consulates, the biometric identifiers may also be collected by qualified and duly authorised staff of an honorary consul as referred to in Article 42 or of an external service provider as referred to in Article 43. The Member State(s) concerned shall, where there is any doubt, provide for the possibility of verifying at the consulate fingerprints which have been taken by the external service provider.*

7. *The following applicants shall be exempt from the requirement to give fingerprints:*

(a) children under the age of 6;

(b) persons for whom fingerprinting is physically impossible. If the fingerprinting of fewer than 10 fingers is possible, the maximum number of fingerprints shall be taken. However, should the impossibility be temporary, the applicant shall be required to give the fingerprints at the following application. The authorities competent in accordance with Article 4(1), (2) and (3) shall be entitled to ask for further clarification of the grounds for the temporary impossibility. Member States shall ensure that appropriate procedures guaranteeing the dignity of the applicant are in place in the event of there being difficulties in enrolling;

(c) heads of State or government and members of a national government with accompanying spouses, and the members of their official delegation when they are invited by Member States' governments or by international organisations for an official purpose;

(d) sovereigns and other senior members of a royal family, when they are invited by Member States' governments or by international organisations for an official purpose;

(e) persons who are required to appear as witness before international courts and tribunals in the territory of the Member States and their appearance in person to lodge the visa application would put them in serious danger.

7a. Applicants referred to in paragraph 7(a), (c), (d) and (e) shall also be exempt from their facial images taken live. In these cases, a photograph ~~according ICAO regulation 9303~~ referred to in Article 10(3)(c) shall be presented.

7b. In exceptional cases where the quality and resolution specifications set for the live enrolment of the facial image cannot be met, the facial image may be extracted electronically from the chip of the electronic Machine Readable Travel Document (eMRTD). Before extracting the data from the chip, the authenticity and integrity of the chip data shall be confirmed using the complete valid certificate chain, unless this is technically impossible or impossible due to the unavailability of valid certificates. In such cases, the facial image shall only be inserted into the individual file in the VIS pursuant to Article 9 and 22c of the VIS Regulation after electronic verification that the facial image recorded in the chip of the eMRTD corresponds to the live facial image of the third-country national concerned.³¹

~~³²8. In the cases referred to in paragraph 7, the entry 'not applicable' shall be introduced in the VIS in accordance with Article 8(5) of the VIS Regulation.~~

³¹ Moved from point 8 of Article 9 of the VIS proposal with some adjustments.

³² This deletion is suggested by the Commission in its proposal.

Article 21

Verification of entry conditions and risk assessment

1. In the examination of an application for a uniform visa, it shall be ascertained whether the applicant fulfils the entry conditions set out in Article 5(1)(a), (c), (d) and (e) of the Schengen Borders Code, and particular consideration shall be given to assessing whether the applicant presents a risk of illegal immigration or a risk to the security of the Member States and whether the applicant intends to leave the territory of the Member States before the expiry of the visa applied for.

2. In respect of each application the VIS shall be consulted in accordance with Articles 8(2), 15 and 9a of the Regulation (EC) No 767/2008. Member States shall ensure that full use is made of all search criteria pursuant to these articles, in order to avoid false rejections and identifications.

3. While checking whether the applicant fulfils the entry conditions, the consulate shall verify:

(a) that the travel document presented is not false, counterfeit or forged;

(b) the applicant's justification for the purpose and conditions of the intended stay, and that he has 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 in a position to acquire such means lawfully;

(c) whether the applicant is a person for whom an alert has been issued in the Schengen Information System (SIS) for the purpose of refusing entry;

(d) that the applicant is not 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 no alert has been issued in Member States' national databases for the purpose of refusing entry on the same grounds;

(e) that the applicant is in possession of adequate and valid travel medical insurance, where applicable.

3a. For the purpose of assessing the entry conditions provided for in paragraph 3, the **visa authority consulate** shall take into account the result of the verifications pursuant to Article 9c of the Regulation (EC) No 767/2008 of the following databases:

(a) SIS and the SLTD to check whether the travel document used for the application corresponds to a travel document reported lost, stolen, **misappropriated** or invalidated in the and whether the travel document used for the application corresponds to a travel document recorded in a file in the Interpol TDAWN;

(b) the ETIAS Central System to check whether the applicant correspond to a refused, revoked or annulled application for travel authorisation or to data from the watchlist referred to in Article 34 of Regulation (EU) 2018/XX for the purposes of establishing a European Travel Information and Authorisation System];

- (c) the VIS to check whether the data provided in the application concerning the travel document correspond to another application for a visa associated with different identity data, as well as whether the applicant has been subject to a decision to refuse, revoke or annul a ~~short stay~~ visa;
- (d) the EES to check whether the applicant is currently reported as overstayer, whether he has been reported as overstayer in the past or whether the applicant was refused entry in the past;
- (e) the Eurodac to check whether the applicant was subject to a withdrawal or rejection of the application for international protection [or registered in Eurodac due to illegal entry and stay];
- (f) the Europol data to check whether the data provided in the application corresponds to data recorded in this database;
- (g) [the ECRIS-TCN system to check whether the applicant corresponds to a person whose data is recorded in this database for terrorist offences or other serious criminal offences;]
- (h) the SIS to check whether the applicant is subject to an alert in respect of persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant or wanted for arrest for extradition purposes.;
- (i) the SIS to check whether the applicant is subject to an alert for the purpose of refusing entry in accordance with Article 24 of Regulation (EU) ... of the European Parliament and of the Council [SIS Borders];
- (j) **the SIS to check if the applicant is subject to an alert on persons subject to a return decision.**

The **visa authority consulate** shall have access to the application file and the linked application file(s), if any, as well as to all the results of the verifications pursuant to Article 9c of Regulation (EC) No 767/2008.

3b. The ~~consulate~~-**visa authority**³³ shall consult the multiple-identity detector together with the common identity repository referred to in Article 4(37) of Regulation 2018/XX [*on interoperability*] or the SIS or both to assess the differences in the linked identities and shall carry out any additional verification necessary to take a decision on the status and colour of the link as well as to take a decision on the issuance or refusal of the visa of the person concerned.

In accordance with Article 59(1) of Regulation 2018/XX [*on interoperability*], this paragraph shall apply only as from the start of operations of the multiple-identity detector.

4. The **consulate visa authority** shall verify, using the information obtained from the EES, whether the applicant will not exceed with the intended stay the maximum duration of authorised stay in the territory of the Member States, irrespective of possible stays authorised under a national long-stay visa or a residence permit issued by another Member State.

³³ Revert the original Commission proposal (i.e. no change).

5. *The means of subsistence for the intended stay shall be assessed in accordance with the duration and the purpose of the stay and by reference to average prices in the Member State(s) concerned for board and lodging in budget accommodation, multiplied by the number of days stayed, on the basis of the reference amounts set by the Member States in accordance with Article 34(1)(c) of the Schengen Borders Code. Proof of sponsorship and/or private accommodation may also constitute evidence of sufficient means of subsistence.*

6. *In the examination of an application for an airport transit visa, the consulate shall in particular verify:*

(a) that the travel document presented is not false, counterfeit or forged;

(b) the points of departure and destination of the third-country national concerned and the coherence of the intended itinerary and airport transit;

(c) proof of the onward journey to the final destination.

7. *The examination of an application shall be based notably on the authenticity and reliability of the documents submitted and on the veracity and reliability of the statements made by the applicant.*

8. *During the examination of an application, consulates may in justified cases call the applicant for an interview and request additional documents.*

9. *A previous visa refusal shall not lead to an automatic refusal of a new application. A new application shall be assessed on the basis of all available information.*

Article 21a

Specific risk indicators

1. Assessment of security or illegal immigration or a high epidemic risks shall be supported by ~~based on~~:

(a) statistics generated by the EES indicating abnormal rates of overstayers and refusals of entry for a specific group of travellers holding a visa;

(b) statistics generated by the VIS in accordance with Article 45a of Regulation (EC) No 767/2008 indicating abnormal rates of refusals of visa applications due to an irregular migration, security or public health risk associated with a specific group of travellers;

(c) statistics generated by the VIS in accordance with Article 45a of Regulation (EC) No 767/2008 and the EES indicating correlations between information collected through the application form and overstay or refusals of entry;

(d) information substantiated by factual and evidence-based elements provided by Member States concerning specific security risk indicators or threats identified by that Member State;

- (e) information substantiated by factual and evidence-based elements provided by Member States concerning abnormal rates of overstayers and refusals of entry for a specific group of travellers for that Member State;
- (f) information concerning specific high epidemic risks provided by Member States as well as epidemiological surveillance information and risk assessments provided by the European Centre for Disease Prevention and Control (ECDC) and disease outbreaks reported by the World Health Organisation (WHO).

2. The Commission shall adopt an implementing act specifying the risks referred to in paragraph 1. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 52(2).

3. Based on the specific risks determined in accordance with paragraph 2 specific risk indicators shall be established, consisting of a combination of data including one or several of the following:

- (a) age range, sex, nationality;
- (b) country and city of residence;
- (c) Member State(s) of destination;
- (d) Member State of first entry;
- (e) purpose of travel;
- (f) current occupation.

4. The specific risk indicators shall be targeted and proportionate. They shall in no circumstances be based solely on a person's sex or age. They shall in no circumstances be based on information revealing a person's race, colour, ethnic or social origin, genetic features, language, political or any other opinions, religion or philosophical belief, trade union membership, membership of a national minority, property, birth, disability or sexual orientation.

5. The specific risk indicators shall be adopted by the Commission by implementing act. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 52(2).

6. The specific risk indicators shall be used by the ~~visa authorities consulate~~³⁴ when assessing whether the applicant presents a risk of illegal immigration, a risk to the security of the Member States, or a high epidemic risk in accordance to Article 21(1).

7. The specific risks and the specific risk indicators shall be regularly reviewed by the Commission.

³⁴ Revert the original Commission proposal (i.e. no change).

Article 46
Compilation of statistics

The Commission shall, by 1 March each year, publish the compilation of the following annual statistics on visas per consulate and border crossing point where individual Member States process visa applications:

- (a) number of airport transit visas applied for, issued and refused;
- (b) number of uniform single entry, and multiple entry visa applied for, issued (disaggregated by length of validity: 6 months or below, 1, 2, 3, 4 and 5 years) and refused;
- (c) number of visas with limited territorial validity issued.

These statistics shall be compiled on the basis of the reports generated by the central repository of data of the VIS in accordance with Article ~~17~~ 45a of Regulation (EC) No 767/2008.

Article 57

Monitoring and evaluation

1. Two years after all the provisions of this Regulation have become applicable, the Commission shall produce an evaluation of its application. This overall evaluation shall include an examination of the results achieved against objectives and of the implementation of the provisions of this Regulation, without prejudice to the reports referred to in paragraph 3.

2. The Commission shall transmit the evaluation referred to in paragraph 1 to the European Parliament and the Council. On the basis of the evaluation, the Commission shall submit, if necessary, appropriate proposals with a view to amending this Regulation.

~~3. The Commission shall present, three years after the VIS is brought into operation and every four years thereafter, a report to the European Parliament and to the Council on the implementation of Articles 13, 17, 40 to 44 of this Regulation, including the implementation of the collection and use of biometric identifiers, the suitability of the ICAO standard chosen, compliance with data protection rules, experience with external service providers with specific reference to the collection of biometric data, the implementation of the 59-month rule for the copying of fingerprints and the organisation of the procedures relating to applications. The report shall also include, on the basis of Article 17(12), (13) and (14) and of Article 50(4) of the VIS Regulation, the cases in which fingerprints could factually not be provided or were not required to be provided for legal reasons, compared with the number of cases in which fingerprints were taken. The report shall include information on cases in which a person who could factually not provide fingerprints was refused a visa. The report shall be accompanied, where necessary, by appropriate proposals to amend this Regulation.~~

~~4. The first of the reports referred to in paragraph 3 shall also address the issue of the sufficient reliability for identification and verification purposes of fingerprints of children under the age of 12 and, in particular, how fingerprints evolve with age, on the basis of the results of a study carried out under the responsibility of the Commission.~~

Article 4
Amendments to Regulation (EU) No 2017/2226

Regulation (EU) No 2017/2226 is amended as follows:

Article 9

Access to the EES for entering, amending, erasing and consulting data

1. Access to the EES for entering, amending, erasing and consulting the data referred to in Article 14 and Articles 16 to 20 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 23 to 35. That access shall be limited to the extent necessary for the performance of the tasks of those national authorities in accordance with those purposes and shall be proportionate to the objectives pursued.

2. Each Member State shall designate the competent national authorities which shall be border authorities, visa authorities and immigration authorities for the purposes of this Regulation. The duly authorised staff of the competent national authorities shall have access to the EES to enter, amend, erase or consult data. Each Member State shall communicate a list of those competent national authorities to eu-LISA without delay. That list shall specify for which purpose each authority is to have access to the data stored in the EES.

The EES shall provide the functionality for the centralised management of this list. The detailed rules on managing this functionality shall be laid down in implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 68(2) of this Regulation.

3. The authorities entitled to consult or access the EES data in order to prevent, detect and investigate terrorist offences or other serious criminal offences shall be designated in accordance with Chapter IV.

Article 13

Web service

1. In order to enable third-country nationals to verify at any moment the remaining authorised stay, a secure internet access to a web service hosted by eu-LISA in its technical sites shall allow third-country nationals to provide the data required pursuant to point (b) of Article 16(1) together with their intended date of entry or exit, or both. On that basis, the web service shall provide third-country nationals with an OK/NOT OK answer, as well as the information on the remaining authorised stay.

2. By way of derogation from paragraph 1, for an intended stay in a Member State which does not yet apply the Schengen acquis in full but operates the EES, the web service shall not provide any information on the authorised stay based on a short-stay visa or a national short-stay visa.

In the case referred to in the first subparagraph, the web service shall enable third-country nationals to verify the compliance with the overall limit of 90 days in any 180-day period and to receive information on the remaining authorised stay under that limit. This information shall be provided for stays in the 180-day period preceding the consultation of the web service or their intended date of entry or exit, or both.

3. In order to fulfil their obligation under point (b) of Article 26(1) of the Convention implementing the Schengen Agreement, carriers shall use the web service to verify whether a ~~short-stay~~ visa is valid, including if the number of authorised entries have already been used or if the holder has reached the maximum duration of the authorised stay or, as the case may be, if the visa is valid for the territory of the port of destination of that travel. Carriers shall provide the data listed under points (a), (b) and (c) of Article 16(1) of this Regulation. On that basis, the web service shall provide carriers with an OK/NOT OK answer. Carriers may store the information sent and the answer received in accordance with the applicable law. Carriers shall establish an authentication scheme to ensure that only authorised staff may access the web service. It shall not be possible to regard the OK/NOT OK answer as a decision to authorise or refuse entry in accordance with Regulation (EU) 2016/399.

4. For the purpose of implementing Article 26(2) of the Convention implementing the Schengen Agreement or for the purpose of resolving any potential dispute arising from Article 26 of the Convention implementing the Schengen Agreement, eu-LISA shall keep logs of all data processing operations carried out within the web service by carriers. Those logs shall show the date and time of each operation, the data used for interrogation, the data transmitted by the web service and the name of the carrier in question.

Logs shall be stored for a period of two years. Logs shall be protected by appropriate measures against unauthorised access.

5. The web service shall make use of a separate read-only database updated on a daily basis via a one-way extraction of the minimum necessary subset of EES and VIS data. eu-LISA shall be responsible for the security of the web service, for the security of the personal data it contains and for the process of extracting the personal data into the separate read-only database.

6. The web service shall not enable carriers to verify whether third-country nationals holding a national short-stay visa issued for one or two entries have already used the number of entries authorised by that visa.

7. The Commission shall adopt implementing acts concerning the detailed rules on the conditions for the operation of the web service and the data protection and security rules applicable to the web service. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 68(2).

Amendment of data and advance data erasure

1. The Member State responsible shall have the right to amend data which it has entered in the EES by rectifying, completing or erasing the data.

2. If the Member State responsible has evidence to suggest that data recorded in the EES are factually inaccurate or incomplete or that data were processed in the EES in breach of this Regulation, it shall check the data concerned and shall, if necessary, rectify or complete them in, or erase them from, the EES without delay and, where applicable, from the list of identified persons referred to in Article 12(3). The data may also be checked and rectified, completed or erased at the request of the person concerned in accordance with Article 52.

3. By way of derogation from paragraphs 1 and 2 of this Article, where a Member State other than the Member State responsible has evidence to suggest that data recorded in the EES are factually inaccurate or incomplete or that data were processed in the EES in breach of this Regulation, it shall check the data concerned, provided it is possible to do so without consulting the Member State responsible and shall, if necessary, rectify or complete them in, or erase them from, the EES without delay and, where applicable, from the list of identified persons referred to in Article 12(3). Where it is not possible to check the data without consulting the Member State responsible, it shall contact the authorities of the Member State responsible within seven days, following which the Member State responsible shall check the accuracy of the data and the lawfulness of their processing within one month. The data may also be checked and rectified, completed or erased at the request of the third-country national concerned in accordance with Article 52.

4. Where a Member State has evidence to suggest that visa-related data recorded in the EES are factually inaccurate or incomplete or that such data were processed in the EES in breach of this Regulation, it shall first check the accuracy of those data against the VIS and shall, if necessary, rectify or complete them in, or erase them from, the EES. Where the data recorded in the VIS are the same as those recorded in the EES, it shall inform the Member State responsible for entering those data in the VIS immediately ~~through the infrastructure of the VIS~~ in accordance with Article 24(2) of Regulation (EC) No 767/2008. The Member State responsible for entering the data in the VIS shall check those data and shall, if necessary, immediately rectify or complete them in, or erase them from, the VIS and inform the Member State concerned which shall, if necessary, rectify or complete them in, or erase them from, the EES without delay and, where applicable, the list of identified persons referred to in Article 12(3).

5. The data of identified persons referred to in Article 12 shall be erased without delay from the list referred to in that Article and shall be rectified or completed in the EES where the third-country national concerned provides evidence, in accordance with the national law of the Member State responsible or of the Member State to which the request has been made, that he or she was forced to exceed the duration of authorised stay due to unforeseeable and serious events, that he or she has acquired a legal right to stay or in case of errors. Without prejudice to any available administrative or non-judicial remedy, that third-country national shall have access to an effective judicial remedy to ensure the data are rectified, completed or erased.

6. Where a third-country national has acquired the nationality of a Member State or has fallen under the scope of Article 2(3) before the expiry of the applicable period referred to in Article 34, the individual file and the entry/exit records linked to that individual file in accordance with Articles 16 and 17 and the refusal of entry records linked to that individual file in accordance with Article 18 shall, without delay, and in any event not later than five working days from the date on which that third-country national has acquired the nationality of a Member State or has fallen under the scope of Article 2(3) before the expiry of the period referred to in Article 34, be erased from the EES, as well as, where applicable, from the list of identified persons referred to in Article 12(3), by:

(a) the Member State the nationality of which he or she has acquired; or

(b) the Member State that issued the residence permit or card or long-stay visa.

Where a third-country national has acquired the nationality of Andorra, Monaco or San Marino or where a third-country national is in a possession of a passport issued by the Vatican City State, he or she shall inform the competent authorities of the Member State he or she next enters of that change. That Member State shall erase his or her data without delay from the EES. The third-country national in question shall have access to an effective judicial remedy to ensure that the data are erased.

7. The EES Central System shall immediately inform all Member States of the erasure of EES data and where applicable from the list of identified persons referred to in Article 12(3).

8. Where a Member State other than the Member State responsible has rectified, completed or erased data in accordance with this Regulation, that Member State shall become the Member State responsible for the rectification, completion or erasure. The EES shall record all rectifications, completions and erasures of data.

Article 5

Amendments to Regulation (EU) 2016/399

Regulation (EU) 2016/399 is amended as follows:

Article 8

Border checks on persons

1. Cross-border movement at external borders shall be subject to checks by border guards. Checks shall be carried out in accordance with this chapter.

The checks may also cover the means of transport and objects in the possession of the persons crossing the border. The law of the Member State concerned shall apply to any searches which are carried out.

2. On entry and on exit, persons enjoying the right of free movement under Union law shall be subject to the following checks:

(a) verification of the identity and the nationality of the person and of the authenticity and validity of the travel document for crossing the border, including by consulting the relevant databases, in particular:

(1) the SIS;

(2) Interpol's Stolen and Lost Travel Documents (SLTD) database;

(3) national databases containing information on stolen, misappropriated, lost and invalidated travel documents.

If the travel document contains an electronic storage medium (chip), the authenticity and integrity of the chip data shall be confirmed using the complete valid certificate chain, unless this is technically impossible or, in the case of a travel document issued by a third country, impossible due to the unavailability of valid certificates.

(b) verification that a person enjoying the right of free movement under Union law is not considered to be a threat to the public policy, internal security, public health or international relations of any of the Member States, including by consulting the SIS and other relevant Union databases. This is without prejudice to the consultation of national and Interpol databases.

Where there are doubts as to the authenticity of the travel document or the identity of its holder, at least one of the biometric identifiers integrated into the passports and travel documents issued in accordance with Regulation (EC) No 2252/2004 shall be verified. Where possible, such verification shall also be carried out in relation to travel documents not covered by that Regulation.

For persons whose entry is subject to a registration in the EES pursuant to Article 6a of this Regulation, a verification of their identity in accordance with Article 23(2) of Regulation (EU) 2017/2226 and, where applicable, an identification in accordance with Article 23(4) of that Regulation shall be carried out.

2a. Where the checks against the databases referred to in points (a) and (b) of paragraph 2 would have a disproportionate impact on the flow of traffic, a Member State may decide to carry out those checks on a targeted basis at specified border crossing points, following an assessment of the risks related to the public policy, internal security, public health or international relations of any of the Member States.

The scope and duration of the temporary reduction to targeted checks against the databases shall not exceed what is strictly necessary and shall be defined in accordance with a risk assessment carried out by the Member State concerned. The risk assessment shall state the reasons for the temporary reduction to targeted checks against the databases, take into account, inter alia, the disproportionate impact on the flow of traffic and provide statistics on passengers and incidents related to cross-border crime. It shall be updated regularly.

Persons who, in principle, are not subject to targeted checks against the databases, shall, as a minimum, be subject to a check with a view to establishing their identity on the basis of the production or presentation of travel documents. Such a check shall consist of a rapid and straightforward verification of the validity of the travel document for crossing the border, and of the presence of signs of falsification or counterfeiting, where appropriate by using technical devices, and, in cases where there are doubts about the travel document or where there are indications that such a person could represent a threat to the public policy, internal security, public health or international relations of the Member States, the border guard shall consult the databases referred to in points (a) and (b) of paragraph 2.

The Member State concerned shall transmit its risk assessment and updates thereto to the European Border and Coast Guard Agency ('the Agency'), established by Regulation (EU) 2016/1624 of the European Parliament and of the Council (⁹), without delay and shall report every six months to the Commission and to the Agency on the application of the checks against the databases carried out on a targeted basis. The Member State concerned may decide to classify the risk assessment or parts thereof.

2b. Where a Member State intends to carry out targeted checks against the databases pursuant to paragraph 2a, it shall notify the other Member States, the Agency and the Commission accordingly without delay. The Member State concerned may decide to classify the notification or parts thereof.

Where the Member States, the Agency or the Commission have concerns about the intention to carry out targeted checks against the databases, they shall notify the Member State in question of those concerns without delay. The Member State in question shall take those concerns into account.

2c. The Commission shall, by 8 April 2019, transmit to the European Parliament and the Council an evaluation of the implementation and consequences of paragraph 2.

2d. With regard to air borders, paragraphs 2a and 2b shall apply for a maximum transitional period of six months from 7 April 2017.

In exceptional cases, where, at a particular airport, there are specific infrastructural difficulties requiring a longer period of time for adaptations in order to allow for the carrying-out of systematic checks against the databases without having a disproportionate impact on the flow of traffic, the six-month transitional period referred to in the first subparagraph may be prolonged for that particular airport by a maximum of 18 months in accordance with the procedure specified in the third subparagraph.

For that purpose, the Member State shall, at the latest three months before the expiry of the transitional period referred to in the first subparagraph, notify the Commission, the Agency and the other Member States of the specific infrastructural difficulties in the airport concerned, the envisaged measures to remedy them and the required period of time for their implementation.

Where specific infrastructural difficulties requiring a longer period for adaptations exist, the Commission, within one month of receipt of the notification referred to in the third subparagraph and after consulting the Agency, shall authorise the Member State concerned to prolong the transitional period for the airport concerned and, where relevant, shall set the length of such prolongation.

2e. The checks against the databases referred to in points (a) and (b) of paragraph 2 may be carried out in advance on the basis of passenger data received in accordance with Council Directive 2004/82/EC (¹⁰) or in accordance with other Union or national law.

Where those checks are carried out in advance on the basis of such passenger data, the data received in advance shall be checked at the border crossing point against the data in the travel document. The identity and the nationality of the person concerned, as well as the authenticity and the validity of the travel document for crossing the border, shall also be verified.

2f. By way of derogation from paragraph 2, persons enjoying the right of free movement under Union law who cross the internal land borders of the Member States for which the verification in accordance with the applicable Schengen evaluation procedures has already been successfully completed, but for which the decision on the lifting of controls on their internal borders pursuant to the relevant provisions of the relevant Acts of Accession has not yet been taken, may be subject to the checks on exit referred to in paragraph 2 only on a non-systematic basis, based on a risk assessment.

3. On entry and exit, third-country nationals shall be subject to thorough checks as follows:

(a) thorough checks on entry shall comprise verification of the conditions governing entry laid down in Article 6(1) and, where applicable, of documents authorising residence and the pursuit of a professional activity. This shall include a detailed examination covering the following aspects:

(i) verification of the identity and the nationality of the third-country national and of the authenticity and validity of the travel document for crossing the border, including by consulting the relevant databases, in particular:

(1) the SIS;

(2) Interpol's SLTD database;

(3) national databases containing information on stolen, misappropriated, lost and invalidated travel documents.

For passports and travel documents containing an electronic storage medium (chip), the authenticity and integrity of the chip data shall be checked, subject to the availability of valid certificates.

With the exception of third-country nationals for whom an individual file is already registered in the EES, where the travel document contains a facial image recorded in the electronic storage medium (chip) and that facial image can be technically accessed, this verification shall include the verification of that facial image, by comparing electronically that facial image with the live facial image of the third-country national concerned. If technically and legally possible, this verification may be done by verifying the live fingerprints against the fingerprints recorded in the electronic storage medium (chip).

(ii) verification that the travel document is accompanied, where applicable, by the requisite visa or residence permit;

(iii) for persons whose entry or whose refusal of entry is subject to a registration in the EES pursuant to Article 6a of this Regulation, a verification of their identity in accordance with Article 23(2) of Regulation (EU) 2017/2226 and, where applicable, an identification in accordance with Article 23(4) of that Regulation;

(iiia) for persons whose entry or whose refusal of entry is subject to a registration in the EES pursuant to Article 6a of this Regulation, verification that the third-country national has not reached or exceeded the maximum duration of authorised stay on the territory of the Member States and, for third-country nationals holding a visa issued for one or two entries, verification that they have respected the number of the maximum authorised entries, by consulting the EES in accordance with Article 23 of Regulation (EU) 2017/2226;

(iv) verification regarding the point of departure and the destination of the third-country national concerned and the purpose of the intended stay, checking, if necessary, the corresponding supporting documents;

(v) verification that the third-country national concerned has sufficient means of subsistence for the duration and purpose of the intended stay, for his or her return to the country of origin or transit to a third country into which he or she is certain to be admitted, or that he or she is in a position to acquire such means lawfully;

(vi) verification that the third-country national concerned, his or her means of transport and the objects he or she is transporting are not likely to jeopardise the public policy, internal security, public health or international relations of any of the Member States. Such verification shall include direct consultation of the data and alerts on persons and, where necessary, objects included in the SIS and other relevant Union databases, and the action to be performed, if any, as a result of an alert. This is without prejudice to the consultation of national and Interpol databases;

(b) if the third country national holds a visa referred to in Article 6(1)(b), the thorough checks on entry shall also comprise verification of the identity of the holder of the visa and of the authenticity of the visa, by consulting the Visa Information System (VIS) in accordance with Article 18 of Regulation (EC) No 767/2008;

(ba) if the third-country national holds a long stay visa or a residence permit, the thorough checks on entry shall ~~also~~ comprise verification of the identity of the holder of the long-stay visa or residence permit and the authenticity and validity of the long-stay visa or residence permit by consulting the Visa Information System (VIS) in accordance with Article 22g of Regulation (EC) No 767/2008;

In circumstances where verification of the document holder or of the document in accordance with Article 22g of that Regulation, as applicable, fails or where there are doubts as to the identity of the holder, the authenticity of the document and/or the travel document, the duly authorised staff of those competent authorities shall proceed to a verification of the document chip.

~~(c) by way of derogation, the VIS may be consulted using the number of the visa sticker in all cases and, on a random basis, the number of the visa sticker in combination with the verification of fingerprints where:~~

~~(i) traffic of such intensity arises that the waiting time at the border crossing point becomes excessive;~~

~~(ii) all resources have already been exhausted as regards staff, facilities and organisation; and~~

~~(iii) on the basis of an assessment there is no risk related to internal security and illegal immigration.~~

~~However, in all cases where there is doubt as to the identity of the holder of the visa and/or the authenticity of the visa, the VIS shall be consulted systematically using the number of the visa sticker in combination with the verification of fingerprints.~~

~~This derogation may be applied only at the border crossing point concerned for as long as the conditions referred to in points (i), (ii) and (iii) are met;~~

~~(d) the decision to consult the VIS in accordance with point (c) shall be taken by the border guard in command at the border crossing point or at a higher level.~~

~~The Member State concerned shall immediately notify the other Member States and the Commission of any such decision;~~

~~(e) each Member State shall transmit once a year a report on the application of point (c) to the European Parliament and the Commission, which shall include the number of third-country nationals who were checked in the VIS using the number of the visa sticker only and the length of the waiting time referred to in point (c)(i);~~

~~(f) points (c) and (d) shall apply for a maximum period of three years, beginning three years after the VIS has started operations. The Commission shall, before the end of the second year of application of points (c) and (d), transmit to the European Parliament and to the Council an evaluation of their implementation. On the basis of that evaluation, the European Parliament or the Council may invite the Commission to propose appropriate amendments to this Regulation;~~

(g) thorough checks on exit shall comprise:

(i) verification of the identity and the nationality of the third-country national and of the authenticity and validity of the travel document for crossing the border, including by consulting the relevant databases, in particular:

(1) the SIS;

(2) Interpol's SLTD database;

(3) national databases containing information on stolen, misappropriated, lost and invalidated travel documents.

For passports and travel documents containing an electronic storage medium (chip), the authenticity and integrity of the chip data shall be checked, subject to the availability of valid certificates.

With the exception of third-country nationals for whom an individual file is already registered in the EES, where the travel document contains a facial image recorded in the electronic storage medium (chip) and that facial image can be technically accessed, this verification shall include the verification of that facial image, by comparing electronically that facial image with the live facial image of the concerned third-country national. If technically and legally possible, this verification may be done by verifying the live fingerprints against the fingerprints recorded in the electronic storage medium (chip);

(ii) verification that the third-country national concerned is not considered to be a threat to the public policy, internal security, public health or international relations of any of the Member States, including by consulting the SIS and other relevant Union databases. This is without prejudice to the consultation of national and Interpol databases;

(iii) for persons whose exit is subject to a registration in the EES pursuant to Article 6a of this Regulation, a verification of their identity in accordance with Article 23(2) of Regulation (EU) 2017/2226 and, where applicable, an identification in accordance with Article 23(4) of that Regulation;

(iv) or persons whose exit is subject to a registration in the EES pursuant to Article 6a of this Regulation, verification that the third-country national has not exceeded the maximum duration of authorised stay on the territory of the Member States, by consulting the EES in accordance with Article 23(3) of Regulation (EU) 2017/2226;

(h) in addition to the checks referred to in point (g) thorough checks on exit may also comprise:

(i) verification that the person is in possession of a valid visa, if required pursuant to Regulation (EC) No 539/2001, except where he or she holds a valid residence permit; such verification may comprise consultation of the VIS in accordance with Article 18 of Regulation (EC) No 767/2008;

(i) for the purpose of the identification of any person who does not fulfil, or who no longer fulfils, the conditions for entry, stay or residence on the territory of the Member States, the VIS may be consulted in accordance with Article ~~6a~~20 of Regulation (EC) No 767/2008 and the EES may be consulted in accordance with Article 27 of Regulation (EU) 2017/2226;

(ia) the checks against the databases referred to in point (a)(i) and (vi) and point (g) may be carried out in advance on the basis of passenger data received in accordance with Directive 2004/82/EC or with other Union or national law.

Where those checks are carried out in advance on the basis of such passenger data, the data received in advance shall be checked at the border crossing point against the data in the travel document. The identity and the nationality of the person concerned, as well as the authenticity and validity of the travel document for crossing the border, shall also be verified;

(ib) where there are doubts as to the authenticity of the travel document or the identity of the third-country national, the checks, where possible, shall include the verification of at least one of the biometric identifiers integrated into the travel documents.

4. Where facilities exist and if requested by the third-country national, such thorough checks shall be carried out in a private area.

5. Without prejudice to the second subparagraph, third-country nationals subject to a thorough second line check shall be given written information in a language which they understand or may reasonably be presumed to understand, or in another effective way, on the purpose of, and the procedure for, such a check.

This information shall be available in all the official languages of the Union and in the language(s) of the country or countries bordering the Member State concerned and shall indicate that the third-country national may request the name or service identification number of the border guards carrying out the thorough second line check, the name of the border crossing point and the date on which the border was crossed.

6. Checks on a person enjoying the right of free movement under Union law shall be carried out in accordance with Directive 2004/38/EC.

7. Detailed rules governing the information to be registered are laid down in Annex II.

8. Where Article 5(2)(a) or (b) applies, Member States may also provide derogations from the rules set out in this Article.

9. The third-country nationals shall be informed of the maximum number of days of authorised stay, which shall take into account the number of entries and the length of stay authorised by the visa. That information shall be provided either by the border guard at the moment of the border checks or by means of equipment installed at the border crossing point enabling the third-country national to consult the web service as referred to in Article 13(1) and (2) of Regulation (EU) 2017/2226.

Article 7

Amendments to Regulation (EU) XXX on establishing a framework for interoperability between EU information systems (borders and visa) [interoperability Regulation]

Regulation (EU) XXX on establishing a framework for interoperability between EU information systems (borders and visa) [interoperability Regulation] is amended as follows:

Article 13

Data stored in the shared biometric matching service

1. The shared BMS shall store the biometric templates that it shall obtain from the following biometric data:

(a) the data referred to in Article 16(1)(d) and Article 17(1)(b) and (c) of Regulation (EU) 2017/2226;

(b) the data referred to in Article 9(5), 9(6), Article 22c(2)(f) and (g) and Article 22d(f) and (g) of Regulation (EC) No 767/2008;

(c) [the data referred to in Article 20(2)(w) and (x) of the Regulation on SIS in the field of border checks];

(d) the data referred to in Article 20(3)(w) and (x) of the Regulation on SIS in the field of law enforcement;

(e) the data referred to in Article 4(3)(t) and (u) of the Regulation on SIS in the field of illegal return];

(f) [the data referred to in Article 13(a) of the Eurodac Regulation];

(g) [the data referred to in Article 5(1)(b) and Article 5(2) of the ECRIS-TCN Regulation].

2. The shared BMS shall include in each biometric template a reference to the information systems in which the corresponding biometric data is stored.

3. Biometric templates shall only be entered in the shared BMS following an automated quality check of the biometric data added to one of the information systems performed by the shared BMS to ascertain the fulfilment of a minimum data quality standard.

4. The storage of the data referred to in paragraph 1 shall meet the quality standards referred to in Article 37(2).

Article 18

The common identity repository data

1. The CIR shall store the following data – logically separated – according to the information system from which the data was originated:

(a) the data referred to in [Article 16(1)(a) to (d) and Article 17(1)(a) to (c) of the EES Regulation];

(b) the data referred to in Article 9(4)(a), ~~(b) and (c)~~ to (cc), Article 9 (5) and (6), Article 22c(2)(a) to (cc), (f) and (g), and Article 22d(a), (b), (c), (f) and (g) of Regulation (EC) No 767/2008;

(c) [the data referred to in Article 15(2)(a) to (e) of the [ETIAS Regulation];]

(d)– (not applicable)

(e)– (not applicable)

2. *For each set of data referred to in paragraph 1, the CIR shall include a reference to the information systems to which the data belongs.*

3. *The storage of the data referred to in paragraph 1 shall meet the quality standards referred to in Article 37(2).*

Article 26

Access to the multiple-identity detector

1. For the purposes of the manual identity verification referred to in Article 29, access to the data referred to in Article 34 stored in the MID shall be granted to:

(a) border authorities when creating or updating an individual file as provided for in Article 14 of the [EES Regulation];

(b) competent authorities referred to in Article 6(1) ~~and (2)~~ of Regulation (EC) No 767/2008 when creating or updating an application file or an individual file in the VIS in accordance with ~~Article 8 or Article 22a~~ of Regulation (EC) No 767/2008;

(c) [the ETIAS Central Unit and the ETIAS National Units when carrying out the assessment referred to in Articles 20 and 22 of the ETIAS Regulation;]

(d)– (not applicable);

(e) the SIRENE Bureaux of the Member State creating a [SIS alert in accordance with the Regulation on SIS in the field of border checks];

(f)– (not applicable).

2. *Member State authorities and EU bodies having access to at least one EU information system included in the common identity repository or to the SIS shall have access to the data referred to in Article 34(a) and (b) regarding any red links as referred to in Article 32.*

Article 27

Multiple-identity detection

1. A multiple-identity detection in the common identity repository and the SIS shall be launched where:

(a) an individual file is created or updated in [the EES in accordance with Article 14 of the EES Regulation];

(b) an application file or an individual file is created or updated in the VIS in accordance with ~~Article 8, or Article 22a~~ of Regulation (EC) No 767/2008;

(c) [an application file is created or updated in the ETIAS in accordance with Article 17 of the ETIAS Regulation;]

(d)– (not applicable);

(e) [an alert on a person is created or updated in the SIS in accordance with Chapter V of the Regulation on SIS in the field of border checks];

(f)– (not applicable).

2. Where the data contained within an information system as referred to in paragraph 1 contains biometric data, the common identity repository (CIR) and the Central-SIS shall use the shared biometric matching service (shared BMS) in order to perform the multiple-identity detection. The shared BMS shall compare the biometric templates obtained from any new biometric data to the biometric templates already contained in the shared BMS in order to verify whether or not data belonging to the same third-country national is already stored in the CIR or in the Central SIS.

3. In addition to the process referred to in paragraph 2, the CIR and the Central-SIS shall use the European search portal to search the data stored in the CIR and the Central-SIS using the following data:

(a) surname (family name); first name(s) (given name(s)); date of birth, sex and nationality(ies) as referred to in Article 16(1)(a) of the [EES Regulation];

(b) surname (family name); first name(s) (given name(s)); date of birth, sex and nationality(ies) as referred to in Article 9(4)(a), in Article 22c(2)(a) and in Article 22d(a) of Regulation (EC) No 767/2008;

(c) [surname (family name); first name(s) (given name(s)); surname at birth; date of birth, place of birth, sex and nationality(ies) as referred to in Article 15(2) of the ETIAS Regulation;]

(d)– (not applicable);

(e) [surname(s); forename(s); name(s) at birth, previously used names and aliases; date of birth, place of birth, nationality(ies) and sex as referred to in Article 20(2) of the Regulation on SIS in the field of border checks;]

(f)– (not applicable);

(g)– (not applicable);

(h)– (not applicable).

4. The multiple-identity detection shall only be launched in order to compare data available in one information system with data available in other information systems.

Article 29

Manual verification of different identities

1. Without prejudice to paragraph 2, the authority responsible for verification of different identities shall be:

(a) the border authority for hits that occurred when creating or updating an individual in [the EES in accordance with Article 14 of the EES Regulation];

(b) the competent authorities referred to in Article 6(1) ~~and (2)~~ of Regulation (EC) No 767/2008 for ~~hit~~ matches that occurred when creating or updating an application file or an individual file in the VIS in accordance with ~~Article 8 or Article 22a~~ of Regulation (EC) No 767/2008;

(c) [the ETIAS Central Unit and the ETIAS National Units for hits that occurred in accordance with Articles 18, 20 and 22 of the ETIAS Regulation;]

(d)– (not applicable);

(e) the SIRENE Bureaux of the Member State for hits that occurred when creating a SIS alert in accordance with the [Regulations on SIS in the field of border checks];

(f)– (not applicable).

The multiple-identity detector shall indicate the authority responsible for the verification of different identities in the identity verification file.

2. The authority responsible for the verification of different identities in the identity confirmation file shall be the SIRENE Bureau of the Member State that created the alert where a link is created to data contained:

(a) in an alert in respect of persons wanted for arrest or for surrender or extradition purposes as referred to in Article 26 of [the Regulation on SIS in the field of law enforcement];

(b) in an alert on missing or vulnerable persons as referred to in Article 32 of [the Regulation on SIS in the field of law enforcement];

(c) in an alert on persons sought to assist with a judicial procedure as referred to in Article 34 of [the Regulation on SIS in the field of law enforcement];

(d)[in an alert on return in accordance with the Regulation on SIS in the field of illegal return];

(e) in an alert on persons for discreet checks, inquiry checks or specific checks as referred to in Article 36 of [the Regulation on SIS in the field of law enforcement];

(f) in an alert on unknown wanted persons for identification according to national law and search with biometric data as referred to in Article 40 of [the Regulation on SIS in the field of law enforcement].

3. Without prejudice to paragraph 4, the authority responsible for verification of different identities shall have access to the related data contained in the relevant identity confirmation file and to the identity data linked in the common identity repository and, where relevant, in the SIS, and shall assess the different identities and shall update the link in accordance with Articles 31, 32 and 33 and add it to the identity confirmation file without delay.

4. Where the authority responsible for the verification of different identities in the identity confirmation file is the border authority creating or updating an individual file in the EES in accordance with Article 14 of the EES Regulation, and where a yellow link is obtained, the border authority shall carry out additional verifications as part of a second-line check. During this second-line check, the border authorities shall have access to the related data contained in the relevant identity confirmation file and shall assess the different identities and shall update the link in accordance with Articles 31 to 33 and add it to the identity confirmation file without delay.

5. Where more than one link is obtained, the authority responsible for the verification of different identities shall assess each link separately.

6. Where data reporting a hit was already linked, the authority responsible for the verification of different identities shall take into account the existing links when assessing the creation of new links.

Article 8

Repeal of Decision 2008/633/JHA

Decision 2008/633/JHA is repealed. References to Decision 2008/633 shall be construed as references to Regulation (EC) No 767/2008 and shall be read in accordance with the correlation table in Annex 2.

Article 9
Entry into force and application

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

2. The Commission shall adopt a decision setting the date on which VIS starts operations pursuant to this Regulation, after the verification that the following conditions are met:

(a) the Management Authority has notified the Commission of the successful completion of all testing activities with regard to CS-VIS; and

(b) Member States have notified the Commission that they have made the necessary technical and legal arrangements to process data pursuant to this Regulation.

~~The date of application of this Regulation shall be determined by the Commission once it has verified all relevant legal and technical requirements to apply this Regulation, such as but not limited to the modifications required in the Central Visa Information System; the establishment and the modifications of the IT systems and components referred to in Article 9a of this Regulation.~~

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.
