

# Official Journal of the European Union

L 248



English edition

Legislation

Volume 64

13 July 2021

## Contents

### I *Legislative acts*

#### REGULATIONS

- ★ **Regulation (EU) 2021/1133 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EU) No 603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 and (EU) 2019/818 as regards the establishment of the conditions for accessing other EU information systems for the purposes of the Visa Information System** ..... 1
- ★ **Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System** ..... 11

EN

Acts whose titles are printed in light type are those relating to day-to-day management of agricultural matters, and are generally valid for a limited period.

The titles of all other acts are printed in bold type and preceded by an asterisk.



## I

*(Legislative acts)*

## REGULATIONS

## REGULATION (EU) 2021/1133 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 7 July 2021

**amending Regulations (EU) No 603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 and (EU) 2019/818 as regards the establishment of the conditions for accessing other EU information systems for the purposes of the Visa Information System**

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular point (e) of Article 78(2), point (d) of Article 82(1), point (a) of Article 87(2), and Article 88(2) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee <sup>(1)</sup>,

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure <sup>(2)</sup>,

Whereas:

- (1) The Visa Information System (VIS) was established by Council Decision 2004/512/EC <sup>(3)</sup> to serve as the technological solution for exchanging visa data between Member States. Regulation (EC) No 767/2008 of the European Parliament and of the Council <sup>(4)</sup> laid down the purpose, functionalities and responsibilities for the VIS, as well as the conditions and procedures for the exchange of short-stay visa data between Member States to facilitate the examination of applications for short-stay visas and related decisions. Regulation (EC) No 810/2009 of the European Parliament and of the Council <sup>(5)</sup> set out the rules on the registration of biometric identifiers in the VIS. The access of law enforcement authorities of the Member States and of the European Union Agency for Law Enforcement Cooperation (Europol) to the VIS was established by Council Decision 2008/633/JHA <sup>(6)</sup>. That Decision should be integrated into Regulation (EC) No 767/2008, to bring it in line with the current Treaty framework.

<sup>(1)</sup> OJ C 440, 6.12.2018, p. 154.

<sup>(2)</sup> Position of the European Parliament of 13 March 2019 (OJ C 23, 21.1.2021, p. 286) and position of the Council at first reading of 27 May 2021 (OJ C 227, 14.6.2021, p. 20). Position of the European Parliament of 7 July 2021 (not yet published in the Official Journal).

<sup>(3)</sup> Council Decision 2004/512/EC of 8 June 2004 establishing the Visa information System (VIS) (OJ L 213, 15.6.2004, p. 5).

<sup>(4)</sup> Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) (OJ L 218, 13.8.2008, p. 60).

<sup>(5)</sup> 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) (OJ L 243, 15.9.2009, p. 1).

<sup>(6)</sup> Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (OJ L 218, 13.8.2008, p. 129).

- (2) Interoperability between certain EU information systems was established by Regulations (EU) 2019/817 <sup>(7)</sup> and (EU) 2019/818 <sup>(8)</sup> of the European Parliament and of the Council so that those systems and their data supplement each other with a view to improving the effectiveness and efficiency of border checks at the external borders of the Union, contributing to preventing and combating illegal immigration and contributing to a high level of security within the area of freedom, security and justice of the Union, including the maintenance of public security and public policy and safeguarding security in the territories of the Member States.
- (3) Interoperability between the EU information systems allows those systems to supplement each other in order to facilitate the correct identification of persons, contribute to fighting identity fraud, improve and harmonise data quality requirements of the relevant EU information systems, facilitate the technical and operational implementation by Member States of existing and future EU information systems, strengthen and simplify the data security and data protection safeguards that govern the relevant EU information systems, streamline the law enforcement access to the VIS, the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS) and Eurodac, and support the purposes of the VIS, Schengen Information System (SIS), the EES, the ETIAS, Eurodac and the European Criminal Records Information System for third-country nationals (ECRIS-TCN).
- (4) The interoperability components cover the VIS, the SIS, the EES, the ETIAS, Eurodac and ECRIS-TCN, as well as Europol data to enable Europol data to be queried simultaneously with those EU information systems. It is therefore appropriate to use those interoperability components for the purpose of carrying out automated queries and when accessing the VIS for law enforcement purposes. The European search portal (ESP) established by Regulation (EU) 2019/818 should be used to enable fast, seamless, efficient, systematic and controlled access by Member States' authorities to the EU information systems, the Europol data and the Interpol databases needed to perform their tasks, in accordance with their access rights, and to support the objectives of the VIS.
- (5) The ESP will enable the data stored in the VIS and the data stored in the other EU information systems concerned to be queried in parallel.
- (6) The comparison of data stored in the VIS against data stored in other information systems and databases should be automated. If such a comparison reveals the existence of a correspondence, known as a 'hit', between any of the personal data or combination thereof in an application and a record, file or alert in those other information systems or databases, or with personal data in the ETIAS watchlist, the application should be verified manually by an operator from the competent authority. The assessment of hits performed by the competent authority should be taken into account for the decision whether to issue a short-stay visa, a long-stay visa or a residence permit.
- (7) This Regulation lays down the manner in which interoperability and the conditions for the consultation of the data stored in SIS, Eurodac and ECRIS-TCN as well as of the Europol data by the VIS automated process for the purpose of identifying hits are to be implemented. As a result, it is necessary to amend Regulations (EU) No 603/2013 <sup>(9)</sup>, (EU) 2016/794 <sup>(10)</sup>, (EU) 2018/1862 <sup>(11)</sup>, (EU) 2019/816 <sup>(12)</sup> and (EU) 2019/818 of the European Parliament and of the Council in order to connect the VIS to the other EU information systems and to Europol data.

<sup>(7)</sup> Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27).

<sup>(8)</sup> Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (OJ L 135, 22.5.2019, p. 85).

<sup>(9)</sup> 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).

<sup>(10)</sup> Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).

<sup>(11)</sup> Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56).

<sup>(12)</sup> Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 (OJ L 135, 22.5.2019, p. 1).

- (8) The conditions under which, on the one hand, the visa authorities are able to consult data stored in Eurodac and, on the other, the VIS designated authorities are able to consult Europol data, certain SIS data and data stored in ECRIS-TCN for the purposes of the VIS should be safeguarded by clear and precise rules regarding the access by those authorities to those data, the type of queries and categories of data, all of which should be limited to what is strictly necessary for the performance of the duties of those authorities. In the same vein, the data stored in the VIS application file should be visible only to those Member States that are operating the underlying information systems in accordance with the arrangements for their participation.
- (9) Regulation (EU) 2021/1134 of the European Parliament and of the Council <sup>(13)</sup> allocates new tasks to Europol such as the provision of opinions following consultation requests by the VIS designated authorities and the ETIAS National Units. To implement those tasks, it is therefore necessary to amend Regulation (EU) 2016/794 accordingly.
- (10) In order to support the VIS objective of assessing whether an applicant for a short-stay visa, a long-stay visa or a residence permit could pose a threat to public policy or public security, the VIS should be able to verify whether any correspondence exists between data in the VIS application files and the ECRIS-TCN data in the Common Identity Repository (CIR) established by Regulation (EU) 2019/818 in regard to which Member States hold information on third-country nationals and stateless persons concerning convictions for a terrorist offence or any other criminal offence listed in the Annex to Regulation (EU) 2018/1240 of the European Parliament and of the Council <sup>(14)</sup> if it is punishable by a custodial sentence or a detention order for a maximum period of at least three years under national law.
- (11) A hit indicated by ECRIS-TCN should not by itself be taken to mean that the third-country national concerned has been convicted in the Member States that are indicated. The existence of previous convictions should be confirmed only on the basis of information received from the criminal records of the Member States concerned.
- (12) This Regulation is without prejudice to Directive 2004/38/EC of the European Parliament and of the Council <sup>(15)</sup>.
- (13) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union (TEU) and to the Treaty on the Functioning of the European Union (TFEU), Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Given that this Regulation, insofar as it relates to SIS as governed by Regulation (EU) 2018/1862, builds upon the Schengen *acquis*, Denmark shall, in accordance with Article 4 of that Protocol, decide within a period of six months after the Council has decided on this Regulation whether it will implement it in its national law.
- (14) Insofar as it relates to SIS as governed by Regulation (EU) 2018/1862, Ireland is taking part in this Regulation, in accordance with Article 5(1) of Protocol No 19 on the Schengen *acquis* integrated into the framework of the European Union, annexed to the TEU and to the TFEU, and Article 6(2) of Council Decision 2002/192/EC <sup>(16)</sup>. Furthermore, insofar as it relates to Europol, Eurodac and ECRIS-TCN, in accordance with Articles 1 and 2 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the TEU and to the TFEU, and without prejudice to Article 4 of that Protocol, Ireland is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

<sup>(13)</sup> Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System (see page 11 of this Official Journal).

<sup>(14)</sup> Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018, p. 1).

<sup>(15)</sup> Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (OJ L 158, 30.4.2004, p. 77).

<sup>(16)</sup> Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen *acquis* (OJ L 64, 7.3.2002, p. 20).

- (15) As regards Iceland and Norway, this Regulation constitutes, insofar as it relates to SIS as governed by Regulation (EU) 2018/1862, a development of the provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latter's association with the implementation, application and development of the Schengen *acquis* <sup>(17)</sup> which fall within the area referred to in Article 1, point G, of Council Decision 1999/437/EC <sup>(18)</sup>.
- (16) As regards Switzerland, this Regulation constitutes, insofar as it relates to SIS as governed by Regulation (EU) 2018/1862, a development of the provisions of the Schengen *acquis* within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* <sup>(19)</sup> which fall within the area referred to in Article 1, point G, of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/149/JHA <sup>(20)</sup>.
- (17) As regards Liechtenstein, this Regulation constitutes, insofar as it relates to SIS as governed by Regulation (EU) 2018/1862, a development of the provisions of the Schengen *acquis* within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* <sup>(21)</sup> which fall within the area referred to in Article 1, point G, of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU <sup>(22)</sup>.
- (18) For this Regulation to fit into the existing legal framework, Regulations (EU) No 603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 and (EU) 2019/818 should be amended accordingly,

HAVE ADOPTED THIS REGULATION:

#### Article 1

### Amendments to Regulation (EU) No 603/2013

Regulation (EU) No 603/2013 is amended as follows:

- (1) the following Chapter is inserted:

‘CHAPTER VIa

#### ACCESS BY VISA AUTHORITIES

Article 22a

#### Access to Eurodac by the competent visa authorities

The competent visa authorities shall have access to Eurodac to consult data in a read-only format for the purpose of manually verifying hits triggered by the automated queries carried out by VIS pursuant to Article 9a of Regulation (EC) No 767/2008 of the European Parliament and of the Council (\*) and examining and deciding on visa applications in accordance with Article 21 of Regulation (EC) No 810/2009 of the European Parliament and of the Council (\*\*).

<sup>(17)</sup> OJ L 176, 10.7.1999, p. 36.

<sup>(18)</sup> Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis* (OJ L 176, 10.7.1999, p. 31).

<sup>(19)</sup> OJ L 53, 27.2.2008, p. 52.

<sup>(20)</sup> Council Decision 2008/149/JHA of 28 January 2008 on the conclusion on behalf of the European Union of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L 53, 27.2.2008, p. 50).

<sup>(21)</sup> OJ L 160, 18.6.2011, p. 21.

<sup>(22)</sup> Council Decision 2011/350/EU of 7 March 2011 on the conclusion, on behalf of the European Union, of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*, relating to the abolition of checks at internal borders and movement of persons (OJ L 160, 18.6.2011, p. 19).

## Article 22b

**Interoperability with VIS**

From the date of the start of operations of VIS pursuant to Article 11 of Regulation (EU) 2021/1134 of the European Parliament and of the Council (\*\*\*) Eurodac shall be connected to the European search portal established by Article 6 of Regulation (EU) 2019/818 of the European Parliament and of the Council (\*\*\*\*) to enable the automated processing pursuant to Article 9a of Regulation (EC) No 767/2008.

- (\*) Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of information between Member States on short-stay visas, long-stay visas, and residence permits (VIS Regulation) (OJ L 218, 13.8.2008, p. 60).
- (\*\*) 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) (OJ L 243, 15.9.2009, p. 1).
- (\*\*\*) Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System (OJ L 248, 13.7.2021, p. 11).
- (\*\*\*\*) Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (OJ L 135, 22.5.2019, p. 85).;

(2) the following Article is inserted:

*'Article 28a***Keeping of records or logs for the purposes of interoperability with VIS**

When consulting Eurodac as referred to in Article 22a of this Regulation, a record or log of each data processing operation carried out within Eurodac and VIS shall be kept in accordance with Article 28 of this Regulation and Article 34 of Regulation (EC) No 767/2008.;

## Article 2

**Amendments to Regulation (EU) 2016/794**

Regulation (EU) 2016/794 is amended as follows:

(1) in Article 4(1), the following point is added:

- '(q) provide an opinion following a consultation request referred to in Article 9e(4), Article 9g(4) and Article 22b(14) and (16) of Regulation (EC) No 767/2008 of the European Parliament and of the Council (\*).

- (\*) Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of information between Member States on short-stay visas, long-stay visas, and residence permits (VIS Regulation) (OJ L 218, 13.8.2008, p. 60).;

(2) Article 21 is amended as follows:

(a) the title is replaced by the following:

'Access by Eurojust, OLAF and, only for purposes of ETIAS, by the European Border and Coast Guard Agency and, only for purposes of VIS, by the VIS designated authorities to information stored by Europol';

(b) the following paragraph is inserted:

'1b. Europol shall take all appropriate measures to enable the VIS designated authorities, for the purposes of Regulation (EC) No 767/2008, to have indirect access on the basis of a hit/no hit system to data provided for the purposes of point (a) of Article 18(2) of this Regulation, without prejudice to any restrictions indicated by the Member State, Union body, third country or international organisation providing the information in question, in accordance with Article 19(2) of this Regulation.

In the case of a hit, Europol shall initiate the procedure by which the information that generated the hit may be shared, in accordance with the decision of the provider of the information to Europol. Such information may be shared only to the extent that the data generating the hit are necessary for the performance of the VIS designated authorities' tasks related to VIS.

Paragraphs 2 to 7 of this Article shall apply accordingly.'

### Article 3

## Amendments to Regulation (EU) 2018/1862

Regulation (EU) 2018/1862 is amended as follows:

- (1) the following article is inserted:

*'Article 18a*

### **Keeping of logs for the purposes of interoperability with VIS**

Logs of each data processing operation carried out within SIS and VIS pursuant to Article 50a of this Regulation shall be kept in accordance with Article 18 of this Regulation and Article 34 of Regulation (EC) No 767/2008 of the European Parliament and of the Council (\*).

(\*) Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of information between Member States on short-stay visas, long-stay visas and residence permits (VIS Regulation) (OJ L 218, 13.8.2008, p. 60).';

- (2) in Article 44(1), the following point is added:

'(g) manually verifying hits triggered by automated queries from the VIS and assessing whether the applicant for a visa, a long-stay visa or a residence permit could pose a threat to public policy or public security, in accordance with Articles 9d and 9g or Article 22b, of Regulation (EC) No 767/2008.';

- (3) the following article is inserted:

*'Article 50a*

### **Interoperability with VIS**

From the date of the start of operations of VIS pursuant to Article 11 of Regulation (EU) 2021/1134 of the European Parliament and of the Council (\*) the SIS Central System shall be connected to the ESP to enable the automated processing pursuant to in Articles 9a and 22b of Regulation (EC) No 767/2008.

(\*) Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System (OJ L 248, 13.7.2021, p. 11).';



## Article 4

**Amendments to Regulation (EU) 2019/816**

Regulation (EU) 2019/816 is amended as follows:

(1) in Article 1, the following point is added:

- ‘(d) the conditions under which data in ECRIS-TCN may be used by the VIS designated authorities as referred to in Article 9d and Article 22b(13) of Regulation (EC) No 767/2008 of the European Parliament and of the Council (\*) for the purpose of assessing whether an applicant for a visa, a long-stay visa or a residence permit could pose a threat to public policy or internal security as referred to in point (i) of Article 2(1) and point (a) of Article 2(2) of that Regulation.

(\*) Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of information between Member States on short-stay visas, long-stay visas and residence permits (VIS Regulation) (OJ L 218, 13.8.2008, p. 60).’;

(2) in Article 2, the following paragraph is added:

‘This Regulation also supports the VIS objective of assessing whether the applicant for a visa, a long-stay visa or a residence permit could pose a threat to public policy or internal security, in accordance with Regulation (EC) No 767/2008.’;

(3) in Article 3, point (6) is replaced by the following:

- ‘(6) ‘competent authorities’ means the central authorities, Eurojust, Europol and the EPPO, and the VIS designated authorities as referred to in Article 9d and Article 22b(13) of Regulation (EC) No 767/2008, which are competent to access or query ECRIS-TCN in accordance with this Regulation.’;

(4) Article 5 is amended as follows:

(a) in paragraph 1, the following point is added:

- ‘(c) a flag indicating, for the purposes of Regulation (EC) No 767/2008, that the third-country national concerned has been convicted of a terrorist offence or any other criminal offence listed in the Annex to Regulation (EU) 2018/1240 if it is punishable by a custodial sentence or a detention order for a maximum period of at least three years under national law, including the code of the convicting Member State.’;

(b) paragraph 1a is replaced by the following:

- ‘1a. The CIR shall contain the data referred to in point (b) of paragraph 1 and the following data of point (a) of paragraph 1: surname (family name), first names (given names), date of birth, place of birth (town and country), nationality or nationalities, gender, previous names, if applicable, where available pseudonyms or aliases, where available, the type and number of the person’s travel documents, as well as the name of the issuing authority.

The CIR may contain the data referred to in paragraph 3 as well as, in the cases referred to in point (c) of paragraph 1, the code of the convicting Member State. The remaining ECRIS-TCN data shall be stored in the central system.’;

(c) the following paragraph is added:

- ‘7. Where hits are identified following the automated processing referred to in Article 27a of Regulation (EC) No 767/2008, the flags and the code of the convicting Member State referred to in point (c) of paragraph 1 of this Article shall be accessible and searchable only by the VIS Central System for the purposes of the verifications pursuant to Article 7a of this Regulation in conjunction with point (e) of Article 9a(4) or point (e) of Article 22b(3) of Regulation (EC) No 767/2008.

Without prejudice to the first subparagraph of this paragraph, the flags and the code of the convicting Member State referred to in point (c) of paragraph 1 shall not be visible to any authority other than the central authority of the convicting Member State having created the flagged record.’;

(5) in Article 7, paragraph 7 is replaced by the following:

‘7. In the event of a hit, the central system or the CIR shall automatically provide the competent authority with information on the Member States holding criminal record information on the third-country national, along with the associated reference numbers referred to in Article 5(1) and any corresponding identity information. Such identity information shall be used only for the purpose of verifying the identity of the third-country national concerned. The result of a search in the central system shall be used only for the purpose of:

- (a) making a request pursuant to Article 6 of Framework Decision 2009/315/JHA;
- (b) making a request as referred to in Article 17(3) of this Regulation; or
- (c) assessing whether the applicant for a visa, a long-stay visa or a residence permit could pose a threat to public policy or internal security, in accordance with Regulation (EC) No 767/2008.’;

(6) the following Article is inserted:

*‘Article 7a*

#### **Use of ECRIS-TCN for VIS verifications**

1. From the date of the start of operations of VIS pursuant to Article 11 of Regulation (EU) 2021/1134 of the European Parliament and of the Council (\*) ECRIS-TCN shall be connected to the ESP to enable the automated processing pursuant to Articles 9a and 22b of Regulation (EC) No 767/2008 to query ECRIS-TCN and compare the relevant data in the VIS with the relevant ECRIS-TCN data in the CIR flagged pursuant to point (c) of Article 5(1) of this Regulation.

2. For the purpose of performing the tasks pursuant to Regulation (EC) No 767/2008, the VIS designated authorities as referred to in Article 9d and Article 22b(13) of that Regulation shall have the right to access only those ECRIS-TCN data in the CIR to which a flag has been added pursuant to point (c) of Article 5(1) of this Regulation.

---

(\*) Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System (OJ L 248, 13.7.2021, p. 11).;

(7) Article 8 is amended as follows:

- (a) paragraph 2 is replaced by the following:

‘2. Upon expiry of the retention period referred to in paragraph 1, the central authority of the convicting Member State shall erase the data record, including any fingerprint data, facial images or flags as referred to in point (c) of Article 5(1), from the central system and the CIR. In cases where the data related to a conviction for a terrorist offence or any other criminal offence as referred to in point (c) of Article 5(1) are erased from the national criminal record, but information on other convictions of the same person is retained, only the flag referred to in point (c) of Article 5(1) shall be removed from the data record. Where possible the erasure shall be done automatically, and in any event no later than one month after the expiry of the retention period.’;

- (b) the following paragraph is added:

‘3. By way of derogation from paragraphs 1 and 2, the flags referred to in point (c) of Article 5(1) shall be erased automatically 25 years after the creation of the flag as regards convictions related to terrorist offences, and 15 years after the creation of the flag as regards convictions related to other criminal offences.’;

(8) in Article 24, paragraph 1 is replaced by the following:

‘1. The data entered into the central system and the CIR shall be processed only for the purposes of the identification of the Member States holding the criminal records information of third-country nationals, or to support the VIS objective of assessing whether the applicant for a visa, a long-stay visa or a residence permit could pose a threat to public policy or internal security in accordance with Regulation (EC) No 767/2008. The data entered into the CIR shall also be processed in accordance with Regulation (EU) 2019/818 for facilitating and assisting in the correct identification of persons registered in the ECRIS-TCN in accordance with this Regulation.’;

(9) the following Article is inserted:

*‘Article 31a*

#### **Keeping of logs for the purposes of interoperability with VIS**

For the consultations referred to in Article 7a of this Regulation, a log of each ECRIS-TCN data processing operation carried out within the CIR and VIS shall be kept in accordance with Article 34 of Regulation (EC) No 767/2008.’.

#### *Article 5*

#### **Amendments to Regulation (EU) 2019/818**

Regulation (EU) 2019/818 is amended as follows:

(1) in Article 4, point 20 is replaced by the following:

‘(20) ‘designated authorities’ means the Member State designated authorities as defined in point (3a) of Article 4 of Regulation (EC) No 767/2008, point (26) of Article 3(1) of Regulation (EU) 2017/2226 and point (21) of Article 3(1) of Regulation (EU) 2018/1240;’;

(2) in Article 18, the following paragraph is inserted:

‘1a. For the purposes of Articles 9a and 22b of Regulation (EC) No 767/2008, the CIR shall also store, logically separated from the data referred to in paragraph 1 of this Article, the data referred to in point (c) of Article 5(1) of Regulation (EU) 2019/816. The data referred to in point (c) of Article 5(1) of Regulation (EU) 2019/816 shall be accessible only in the manner referred to in Article 5(7) of that Regulation.’;

(3) in Article 68, the following paragraph is inserted:

‘1a. Without prejudice to paragraph 1 of this Article, the ESP shall start operations, for the purposes of the automated processing pursuant to Articles 9a and 22b of Regulation (EC) No 767/2008 only, from the date of the start of operations of VIS pursuant to Article 11 of Regulation (EU) 2021/1134 of the European Parliament and of the Council (\*).

(\*) Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System (OJ L 248, 13.7.2021, p. 11).’.

#### *Article 6*

#### **Entry into force**

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

This Regulation shall apply from the date of the start of operation of VIS pursuant to Article 11 of Regulation (EU) 2021/1134.

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

Done at Strasbourg, 7 July 2021.

*For the European Parliament*  
*The President*  
D. M. SASSOLI

*For the Council*  
*The President*  
A. LOGAR

---

**REGULATION (EU) 2021/1134 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**  
**of 7 July 2021**

**amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System**

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty of the Functioning of the European Union, and in particular points (a), (b), (d) and (e) of Article 77(2) and point (a) of Article 87(2) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee <sup>(1)</sup>,

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure <sup>(2)</sup>,

Whereas:

- (1) The Visa Information System (VIS) was established by Council Decision 2004/512/EC <sup>(3)</sup> to serve as the technological solution for exchanging visa data between Member States. Regulation (EC) No 767/2008 of the European Parliament and of the Council <sup>(4)</sup> laid down the purpose, functionalities and responsibilities for the VIS, as well as the conditions and procedures for the exchange of short-stay visa data between Member States to facilitate the examination of applications for short-stay visas and related decisions. Regulation (EC) No 810/2009 of the European Parliament and of the Council <sup>(5)</sup> set out the rules on the registration of biometric identifiers in the VIS. Council Decision 2008/633/JHA <sup>(6)</sup> laid down the conditions under which Member States' designated authorities and the European Union Agency for Law Enforcement Cooperation (Europol) are able to obtain access for the consultation of the VIS for the purposes of preventing, detecting and investigating terrorist offences and other serious criminal offences. The VIS started operations on 11 October 2011 and was gradually rolled out in all Member States' consulates between October 2011 and February 2016.
- (2) The objectives of the VIS are to improve the implementation of the common visa policy, consular cooperation and consultation between central visa authorities by facilitating the exchange of data between Member States on applications and on the decisions relating thereto, in order to: facilitate the visa application procedure; prevent 'visa shopping'; facilitate the fight against identity fraud; facilitate checks at external border crossing points and within the Member States' territory; assist in the identification of any person who does not or no longer fulfils the

<sup>(1)</sup> OJ C 440, 6.12.2018, p. 154.

<sup>(2)</sup> Position of the European Parliament of 13 March 2019 (OJ C 23, 21.1.2021, p. 286) and position of the Council at first reading of 27 May 2021 (OJ C 235, 17.6.2021, p. 1). Position of the European Parliament of 7 July 2021 (not yet published in the Official Journal).

<sup>(3)</sup> Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS) (OJ L 213, 15.6.2004, p. 5).

<sup>(4)</sup> Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) (OJ L 218, 13.8.2008, p. 60).

<sup>(5)</sup> 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) (OJ L 243, 15.9.2009, p. 1).

<sup>(6)</sup> Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (OJ L 218, 13.8.2008, p. 129).

conditions for entry to, stay or residence on the territory of the Member States; facilitate the determination of the Member State responsible for examining an application for international protection under Regulation (EU) No 604/2013 of the European Parliament and of the Council <sup>(7)</sup>; and contribute to the prevention of threats to the internal security of any of the Member States.

- (3) In its communication of 6 April 2016 entitled 'Stronger and Smarter Information Systems for Borders and Security', the Commission outlined the need for the Union to strengthen and improve its information systems, data architecture and information exchange in the area of border management, law enforcement and counter-terrorism and emphasised the need to improve the interoperability of information systems. The Communication also identified a need to address information gaps, including on third-country nationals holding a long-stay visa.
- (4) In its 2016 roadmap to enhance information exchange and information management and in its conclusions of 8 June 2017 on the way forward to improve information exchange and ensure the interoperability of EU information systems, the Council invited the Commission to undertake a feasibility study for the establishment of a central EU repository containing information on long-stay visas and residence permits. On that basis, the Commission conducted two studies which concluded that developing a repository would be technically feasible and that re-using the VIS structure would be the best technical option, and that it would be necessary and proportionate to extend the scope of the VIS to include information on long-stay visas and residence permits.
- (5) In its communication of 27 September 2017 entitled 'Delivery of the European Agenda on Migration', the Commission stated that the Union's common visa policy is not only an essential tool for facilitating tourism and business, but also a key tool to prevent security risks and risks of irregular migration to the Union. In that communication, the Commission acknowledged the need to further adapt the common visa policy to current challenges, taking into account new IT solutions and balancing the benefits of facilitated visa travel with improved migration, security and border management. It stated in that communication that the VIS legal framework would be revised, with the aim of further improving visa processing, including as regards data protection related aspects and access for law enforcement authorities, further expanding the use of the VIS for new categories and uses of data and to make full use of the interoperability instruments.
- (6) In its communication of 14 March 2018 on adapting the common visa policy to new challenges, the Commission reaffirmed that the VIS legal framework would be revised, as part of a broader process of reflection on the interoperability of information systems.
- (7) Article 21 of the Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders <sup>(8)</sup> (Schengen Convention) provides holders of valid residence permits or long-stay visas with a right to free movement within the territory of the contracting parties to the Agreement for a period of not more than 90 days in any 180 days, by instituting the mutual recognition of the residence permits and long-stay visas issued by those contracting parties. There are currently no means of checking whether applicants for or holders of such residence permits and long-stay visas could pose a threat to the security of the Member States other than the Member State processing the application for a long-stay visa or residence permit. In order to address the existing information gap, information on applicants for and holders of long-stay visas and residence permits should be stored in the VIS. As regards those documents, the purpose of the VIS should be to support a high level of security, which is particularly important for the Schengen area as an area without internal border controls, by contributing to the assessment of whether an applicant is considered to pose a threat to public policy, internal security or public health. It should also aim to improve the effectiveness and efficiency of checks at the external borders and of checks within the territory of the Member States carried out in accordance with Union or national law. The VIS should also assist in the identification, in particular in order to facilitate the return of any

<sup>(7)</sup> Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 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 (OJ L 180, 29.6.2013, p. 31).

<sup>(8)</sup> Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders (OJ L 239, 22.9.2000, p. 19).

person who does not or no longer fulfils the conditions for entry to, stay or residence on the territory of the Member States. It should also contribute to the prevention, detection and investigation of terrorist offences or other serious criminal offences; ensure the correct identification of persons; facilitate the application of Regulation (EU) No 604/2013 and of Directive 2013/32/EU of the European Parliament and of the Council<sup>(9)</sup>; and support the objectives of the Schengen Information System (SIS).

- (8) Decisions 2004/512/EC and 2008/633/JHA should be integrated into Regulation (EC) No 767/2008 in order to consolidate the rules on the establishment and use of the VIS in a single Regulation.
- (9) Regulation (EC) No 767/2008 should also lay down the architecture of the VIS. The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) should be responsible for the technical development and operational management of the VIS and its components. Where eu-LISA cooperates with external contractors in any VIS-related tasks, it should closely monitor the activities of the contractor to ensure compliance with Regulation (EC) No 767/2008, in particular provisions on security, confidentiality and data protection. The operational management of the VIS should not be entrusted to private companies or private organisations.
- (10) When adopting Regulation (EC) No 810/2009, it was recognised that the issue of the sufficient reliability of fingerprints of children below the age of 12 for identification and verification purposes and, in particular, how fingerprints evolve with age, would have to be addressed at a later stage on the basis of the results of a study that was to be carried out under the responsibility of the Commission. A study entitled “Fingerprint Recognition for Children”, which was carried out in 2013 by the Joint Research Centre, concluded that fingerprint recognition of children aged between six and 12 years is achievable with a satisfactory level of accuracy under certain conditions. A second study entitled “Automatic fingerprint recognition: from children to elderly” confirmed that finding in December 2017 and provided further insight into the effect of aging on fingerprint quality. On that basis, in 2017 the Commission conducted a further study entitled “Feasibility and implications of lowering the fingerprinting age for children and on storing a scanned copy of the visa applicants’ travel document in the Visa Information System (VIS)”, which was finalised in 2018 and looked into the necessity and proportionality of lowering the fingerprinting age in the visa procedure for children to six years. That study found that lowering the fingerprinting age would contribute better to achieving the VIS objectives, in particular in relation to the facilitation of the fight against identity fraud and of checks at external border crossing points. It also found that lowering the fingerprinting age could bring additional benefits by strengthening the prevention and fight against the abuse of children’s rights, in particular by enabling the identification or verification of the identity of children who are third-country nationals in the Schengen area and who are in a situation where their rights have been, or may be, violated, for example because they are child victims of trafficking in human beings, missing children or unaccompanied minors applying for asylum. At the same time, children are a particularly vulnerable group and collecting their biometric data should be subject to stricter safeguards, including limiting the retention period for data storage, and the purposes for which those data may be used should be limited to situations where it is in the child’s best interests. The study that was finalised in 2018 also showed that fingerprints of elderly persons are of lower quality and medium accuracy and recommended measures to mitigate those shortcomings. Member States should follow the recommendations identified in that study with the objective of improving the quality of fingerprints and biometric matching.
- (11) The best interests of the child are a primary consideration for Member States with respect to all procedures provided for in this Regulation. The child’s well-being, safety and security and the views of the child are to be taken into consideration and given due weight in accordance with the child’s age and maturity. The VIS is particularly relevant where there is a risk of a child being a victim of trafficking.

<sup>(9)</sup> Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection (OJ L 180, 29.6.2013, p. 60).

- (12) The visa procedure and the VIS should benefit from the technological developments related to facial image recognition. Taking live facial images upon submission of applications should be the rule when recording the facial image of applicants in the VIS, also when processing applications for long-stay visas and residence permits, where this is allowed by national law. Taking live facial images upon submission of applications will also contribute to addressing biometric vulnerabilities such as 'face-morphing' used for identity fraud. Only facial images taken live should be used for biometric matching.
- (13) Biometric data, which in the context of this Regulation entails fingerprints and facial images, are unique and therefore much more reliable than alphanumeric data for the purpose of identifying a person. However, biometric data constitute sensitive personal data. This Regulation lays down the basis and safeguards for processing such data for the purpose of identifying the persons concerned.
- (14) The personal data provided by the applicant for a short-stay visa should be processed by the VIS to assess whether the entry of the applicant into the territory of the Member States could pose a threat to public policy, internal security or public health and to assess the risk of irregular migration of the applicant. As regards applicants for a long-stay visa or a residence permit, such assessments should be limited to assessing whether the third-country national could pose a threat to public policy, internal security or public health.
- (15) The assessment of such risks cannot be carried out without processing the personal data related to the applicant's identity, travel document, and other relevant data. Each item of personal data in an application should be compared with the data present in a record, file or alert registered in the following information systems and databases: the VIS, the SIS, the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS), Eurodac, the European Criminal Records Information System for third-country nationals (ECRIS-TCN) as far as convictions related to terrorist offences or other serious criminal offences are concerned, the Europol data, the Interpol Stolen and Lost Travel Document database (Interpol SLTD), the Interpol Travel Documents Associated with Notices database (Interpol TDAWN), the ETIAS watchlist referred to in Regulation (EU) 2018/1240 of the European Parliament and of the Council <sup>(10)</sup>, and against specific risk indicators. The categories of personal data that should be used for comparison should be limited to the categories of data present in the queried information systems and databases, the ETIAS watchlist or the specific risk indicators.
- (16) Interoperability between certain EU information systems was established by Regulations (EU) 2019/817 <sup>(11)</sup> and (EU) 2019/818 <sup>(12)</sup> of the European Parliament and of the Council so that those systems and their data supplement each other with a view to improving the effectiveness and efficiency of border checks at the external borders of the Union, contributing to preventing and combating illegal immigration and contributing to a high level of security within the area of freedom, security and justice of the Union, including the maintenance of public security and public policy and safeguarding security in the territories of the Member States.
- (17) Interoperability between the EU information systems allows those systems to supplement each other in order to facilitate the correct identification of persons, contribute to fighting identity fraud, improve and harmonise data quality requirements of the relevant EU information systems, facilitate the technical and operational implementation by Member States of existing and future EU information systems, strengthen and simplify the data security and data protection safeguards that govern the relevant EU information systems, streamline the law enforcement access to the VIS, the EES, the ETIAS and Eurodac, and support the purposes of the VIS, the SIS, the EES, the ETIAS, Eurodac and the ECRIS-TCN.

<sup>(10)</sup> Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018, p. 1).

<sup>(11)</sup> Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27).

<sup>(12)</sup> Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (OJ L 135, 22.5.2019, p. 85).



- (18) The interoperability components cover the VIS, the SIS, the EES, the ETIAS, Eurodac and the ECRIS-TCN, as well as Europol data to enable Europol data to be queried simultaneously with those EU information systems. It is therefore appropriate to use those interoperability components for the purpose of carrying out automated queries and when accessing the VIS for law enforcement purposes. The European search portal (ESP) established by Regulation (EU) 2019/817 should be used to enable fast, seamless, efficient, systematic and controlled access by Member States' authorities to the EU information systems, the Europol data and the Interpol databases needed to perform their tasks, in accordance with their access rights, and to support the objectives of the VIS.
- (19) The ESP will enable the data stored in the VIS and the data stored in the other EU information systems concerned to be queried in parallel.
- (20) The comparison of data stored in the VIS against data stored in other information systems and databases should be automated. If such a comparison reveals the existence of a correspondence, known as a 'hit', between any of the personal data or combination thereof in an application and a record, file or alert in those other information systems or databases, or with personal data in the ETIAS watchlist, the application should be verified manually by an operator from the competent authority. Depending on the type of data triggering the hit, the hit should be manually verified and assessed by the competent visa or immigration authority, by the ETIAS National Unit referred to in Regulation (EU) 2018/1240 or by a central authority designated by the Member State (VIS designated authority). As hits generated by law enforcement or judicial systems or databases are generally more sensitive, they should not be verified and assessed by consulates, but rather by the VIS designated authorities or the ETIAS National Units. Member States should be able to designate more than one authority as a VIS designated authority. The SIRENE Bureau should be designated as the VIS designated authority only if it is allocated sufficient additional resources enabling it to fulfil that task. The assessment of the hits performed by the competent authority should be taken into account for the decision whether to issue a short-stay visa or when assessing whether the applicant for a long-stay visa or residence permit could pose a threat to the public policy, internal security or public health of the Member States.
- (21) As the VIS will be part of the common framework of interoperability, it is necessary that the development of new features and processes be fully coherent with features and processes in the other EU information systems that are part of that framework. The automated queries that will be launched by the VIS with the purpose of finding whether information on applicants for a visa or residence permit is known to other EU information systems will result in hits against those other EU information systems. A similar system of queries is currently present in only one other system, namely ETIAS, while the concept of hits is also found in the EES, including in relation to the EES-VIS interoperability, and in the SIS.
- (22) The refusal of an application for a short-stay visa should not be based solely on the automated processing of personal data in the applications for a visa.
- (23) Applicants who have been refused a short-stay visa on the basis of information resulting from VIS processing should have the right to appeal. Appeals should be conducted in the Member State that has taken the decision on the application and in accordance with the national law of that Member State. The safeguards and rules on appeal under Regulation (EC) No 810/2009 apply.
- (24) The use of specific risk indicators corresponding to previously identified security, irregular migration or high epidemic risks should contribute to analysing the application for a short-stay visa. The criteria used for defining the specific risk indicators should in no circumstances be based solely on the applicant's sex or age. They are not in any circumstances to be based on information revealing the applicant'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. To the extent possible and where relevant, the rules, procedures and governance structure for the specific risk indicators should be aligned with those for the ETIAS screening rules, as laid down in Articles 9, 10 and 33 of Regulation (EU) 2018/1240. The specific risk indicators should be defined, established, assessed *ex ante*, implemented, evaluated *ex post*, revised and deleted by the ETIAS Central Unit referred to in Regulation (EU) 2018/1240 following the consultation of a VIS Screening Board

composed of representatives of the central visa authorities and the agencies involved. To help ensure the respect of fundamental rights in the implementation of the specific risk indicators, a VIS Fundamental Rights Guidance Board should be established. The secretariat for its meetings should be provided by the Fundamental Rights Officer of the European Border and Coast Guard Agency.

- (25) The continuous emergence of new forms of security risks, new patterns of irregular migration and high epidemic risks requires effective responses and needs to be countered with modern means. Since modern means entail the processing of important amounts of personal data, appropriate safeguards should be introduced to keep the interference with the rights to respect for private and family life and to the protection of personal data limited to what is necessary and proportionate in a democratic society.
- (26) It should be ensured that at least a similar level of checks is applied to applicants for a short-stay visa, or third-country nationals who apply for a long-stay visa or a residence permit, as for third-country nationals applying for a travel authorisation in accordance with Regulation (EU) 2018/1240. To that end, the ETIAS watchlist, consisting of data related to persons who are suspected of having committed or taken part in a terrorist offence or other serious criminal offence or persons regarding whom there are factual indications or reasonable grounds to believe that they will commit a terrorist offence or other serious criminal offence, should be used for verifications in respect of those categories of third-country nationals as well.
- (27) In order to fulfil their obligation under the Schengen Convention, international carriers should verify whether third-country nationals who are required to hold a short-stay visa, a long-stay visa or a residence permit are in possession of a valid short-stay visa, long-stay visa or residence permit by sending a query to the VIS. That verification should be made possible through the daily extraction of VIS data into a separate read-only database allowing the extraction of a minimum necessary subset of data to enable a query leading to an OK/NOT OK answer. The application file itself should not be accessible to international carriers. The technical specifications for accessing the VIS through the carrier gateway should limit the impact on passenger travel and international carriers to the extent possible. To that end, integration with the carrier gateways for the EES and ETIAS should be considered.
- (28) With a view to limiting the impact of the obligations set out in this Regulation on international carriers transporting groups overland by coach, user-friendly mobile solutions should be made available.
- (29) The assessment of the appropriateness, compatibility and coherence of provisions referred to in Article 26 of the Schengen Convention as referred to in the preamble to Regulation (EU) 2018/1240 for the purposes of the ETIAS regarding the provisions for overland transport by coaches should be extended to cover also the relevant provisions of this Regulation.
- (30) Regulation (EC) No 767/2008 should specify the authorities of the Member States which are authorised to have access to the VIS to enter, amend, erase or consult data on applications for and decisions on long-stay visas and residence permits for the specific purposes set out in that Regulation, and, to the extent necessary, for the performance of their tasks.
- (31) Any processing of VIS data on long-stay visas and residence permits should be proportionate to the objectives pursued and necessary for the performance of tasks of the competent authorities. Therefore, access by certain competent authorities to data regarding persons who have held valid residence permits recorded in the VIS for a period of 10 years or more without interruption should be restricted.
- (32) When using the VIS, the competent authorities should ensure that the human dignity and integrity of the persons whose data are requested are respected and that they do not discriminate against such persons on grounds of sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

- (33) It is imperative that law enforcement authorities have the most up-to-date information if they are to perform their tasks in the fight against terrorism and other serious forms of crime. The access of law enforcement authorities of the Member States and of Europol to the VIS was established by Decision 2008/633/JHA. That Decision should be integrated into Regulation (EC) No 767/2008, to bring it in line with the current Treaty framework.
- (34) Access to VIS data for law enforcement purposes has already proven to be useful in identifying people who died in violent circumstances or helping investigators to make substantial progress in cases related to trafficking in human beings, terrorism or drug trafficking. Therefore, the VIS data related to long stays should also be available to the designated authorities of the Member States and to Europol, subject to the conditions set out in this Regulation.
- (35) Given that Europol plays a key role with respect to cooperation between Member States' authorities in the field of cross-border crime investigation in supporting Union-wide crime prevention, analyses and investigation, Europol's current access to the VIS within the framework of its tasks should be codified and streamlined, taking into account also recent developments of the legal framework such as Regulation (EU) 2016/794 of the European Parliament and of the Council <sup>(13)</sup>.
- (36) Access to the VIS for the purpose of preventing, detecting or investigating terrorist offences or other serious criminal offences constitutes an interference with the fundamental rights to respect for private and family life and to the protection of personal data of persons whose personal data are processed in the VIS. Any such interference must be carried out in accordance with the law, which must be formulated with sufficient precision to allow individuals to adjust their conduct and which must protect individuals against arbitrariness and indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise. Any such interference with fundamental rights is possible only if necessary in a democratic society to protect a legitimate and proportionate interest and if it is proportionate to the legitimate objective to be achieved.
- (37) Regulation (EU) 2019/817 provides the possibility for a Member State police authority which has been so empowered by national legislation, to identify a person by means of the biometric data of that person taken during an identity check. However, specific circumstances may exist where the identification of a person is necessary in the interests of that person. Such cases include situations where a missing or abducted person or a victim of human trafficking is found. In such cases, law enforcement authorities should be provided with quick access to VIS data in order to enable the fast and reliable identification of the person, without the need to fulfil all the preconditions and additional safeguards for law enforcement access.
- (38) The comparison of data on the basis of a latent fingerprint, which is the dactyloscopic trace that might be found at a crime scene, is fundamental in the field of police cooperation. The possibility to compare a latent fingerprint with the fingerprint data which is stored in the VIS where there are reasonable grounds for believing that the perpetrator or victim is registered in the VIS should provide the law enforcement authorities with a very valuable tool in preventing, detecting or investigating terrorist offences or other serious criminal offences, when for example the only evidence at a crime scene is latent fingerprints.
- (39) It is necessary to designate the competent authorities of the Member States as well as the central access point through which the requests for access to VIS data are made and to keep a list of the operating units within the designated authorities that are authorised to request such access for the specific purposes for the prevention, detection or investigation of terrorist offences or other serious criminal offences.
- (40) Requests for access to data stored in the VIS Central System should be made by the operating units within the designated authorities to the central access point and should be justified. The operating units within the designated authorities that are authorised to request access to VIS data should not act as a verifying authority. The central

<sup>(13)</sup> Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).

access points should act independently of the designated authorities and should be responsible for ensuring, in an independent manner, strict compliance with the conditions for access as established in this Regulation. In exceptional cases of urgency, where early access is necessary to respond to a specific and actual threat related to terrorist offences or other serious criminal offences, the central access point should process the request for access immediately and carry out the verification only afterwards.

- (41) To protect personal data and to exclude the possibility of systematic searches by law enforcement authorities, the processing of VIS data should only take place in specific cases and when it is necessary for the purpose of preventing, detecting or investigating terrorist offences or other serious criminal offences. The designated authorities and Europol should only request access to the VIS when they have reasonable grounds to believe that such access will provide information that will substantially assist them in preventing, detecting or investigating a terrorist offence or other serious criminal offence.
- (42) The personal data stored in the VIS should be kept for no longer than is necessary for the purposes of the VIS. It is appropriate to store the data related to third-country nationals for a period of five years in order to enable data to be taken into account for the assessment of the applications for short-stay visas, to enable detection of overstay after the end of the validity period and in order to conduct security assessments of third-country nationals who obtained them. The data on previous uses of a document could facilitate the issuance of future short-stay visas. A shorter storage period would not be sufficient for ensuring the stated purposes. The data should be erased after a period of five years, unless there are grounds to erase them earlier.
- (43) Regulation (EU) 2016/679 of the European Parliament and of the Council <sup>(14)</sup> applies to the processing of personal data by the Member States in application of Regulation (EC) No 767/2008. The processing of personal data by law enforcement authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties is governed by Directive (EU) 2016/680 of the European Parliament and of the Council <sup>(15)</sup>.
- (44) Members of the European Border and Coast Guard (EBCG) teams, as well as teams of staff involved in return-related tasks are entitled by Regulation (EU) 2019/1896 of the European Parliament and the Council <sup>(16)</sup> to consult EU information systems and databases where necessary for fulfilling their operational tasks specified in the operational plan on border checks, border surveillance and return, under the authority of the host Member State. For the purpose of facilitating that consultation and enabling effective access by the teams to VIS data, they should be given access to the VIS. Such access should follow the conditions and limitations of access applicable to the Member States' authorities competent under each specific purpose for which VIS data can be consulted.
- (45) The return of third-country nationals who do not fulfil or no longer fulfil the conditions for entry to, stay or residence on the territory of the Member States in accordance with Directive 2008/115/EC of the European Parliament and of the Council <sup>(17)</sup>, is an essential component of the comprehensive efforts to tackle irregular migration and represents an important reason of substantial public interest.

<sup>(14)</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

<sup>(15)</sup> Directive (EU) 2016/680 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

<sup>(16)</sup> Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624 (OJ L 295, 14.11.2019, p. 1).

<sup>(17)</sup> Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals (OJ L 348, 24.12.2008, p. 98).

- (46) In order to enhance third countries' cooperation on readmission of irregular migrants and to facilitate the return of illegally staying third-country nationals whose data might be stored in the VIS, copies of the travel document of applicants should be stored in the VIS. Contrary to information extracted from the VIS, copies of travel documents are a proof of nationality more widely recognised by third countries.
- (47) Personal data stored in the VIS should not be transferred or made available to any third country or international organisation. As an exception to that rule, however, it should be possible to transfer such personal data to a third country or to an international organisation where such a transfer is subject to strict conditions and necessary in individual cases in order to assist with the identification of a third-country national in relation to his or her return or resettlement. In the absence of an adequacy decision by means of an implementing act pursuant to Regulation (EU) 2016/679 or of appropriate safeguards to which transfers are subject pursuant to that Regulation, it should exceptionally be possible to transfer VIS data to a third country or to an international organisation for the purposes of return or resettlement only where the transfer is necessary for important reasons of public interest as referred to in that Regulation.
- (48) It should also be possible to transfer personal data obtained by Member States pursuant to Regulation (EC) No 767/2008 to a third country in an exceptional case of urgency, where there is an imminent danger associated with a terrorist offence or where there is an imminent danger to the life of a person associated with a serious criminal offence. An imminent danger to the life of a person should be understood as covering a danger arising from a serious criminal offence committed against that person such as grievous bodily injury, illicit trade in human organs or tissue, kidnapping, illegal restraint and hostage-taking, sexual exploitation of children and child pornography, and rape. Such data should be transferred to a third country only if the reciprocal provision of any information on visa records held by the requesting third country to the Member States operating the VIS is ensured.
- (49) Regulation (EU) 2018/1725 of the European Parliament and the Council <sup>(18)</sup> applies to the activities of the Union institutions, bodies, offices and agencies when carrying out the tasks for which they are responsible with regard to the operational management of the VIS.
- (50) The consultation of 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 <sup>(19)</sup>, is a compulsory element of the short-stay visa examination procedure. Visa authorities should systematically implement that obligation and therefore that list should be incorporated in the VIS to enable automatic verification of the recognition of the applicant's travel document.
- (51) Without prejudice to Member States' responsibility for the accuracy of data entered in the VIS, eu-LISA should be responsible for reinforcing data quality by developing and maintaining a central data quality monitoring tool, and for providing reports at regular intervals to the Member States.
- (52) In order to enable better monitoring of the use of the VIS to analyse trends concerning migratory pressure and border management, eu-LISA should be able to develop a capability for statistical reporting to the Member States, the Commission, and the European Border and Coast Guard Agency without jeopardising data integrity. Therefore, eu-LISA should store certain statistics in the central repository for reporting and statistics in accordance with Regulation (EU) 2019/817. None of the statistics produced should contain personal data.

<sup>(18)</sup> Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

<sup>(19)</sup> Decision No 1105/2011/EU of the European Parliament and of the Council of 25 October 2011 on the list of travel documents which entitle the holder to cross the external borders and which may be endorsed with a visa and on setting up a mechanism for establishing this list (OJ L 287, 4.11.2011, p. 9).

- (53) This Regulation is without prejudice to the application of Directive 2004/38/EC of the European Parliament and of the Council <sup>(20)</sup>.
- (54) Specific provisions should apply to third-country nationals who are subject to a visa requirement, who are family members of a Union citizen to whom Directive 2004/38/EC applies or of a third-country national enjoying the right of free movement under Union law, and who do not hold a residence card as referred to in Directive 2004/38/EC. Article 21(1) of the Treaty on the Functioning of the European Union (TFEU) provides that every Union citizen has the right to move and reside freely within the territory of the Member States, subject to the limitations and conditions laid down in the Treaties and laid down by the measures adopted to give those limitations and conditions effect. Those limitations and conditions are laid down in Directive 2004/38/EC.
- (55) As confirmed by the Court of Justice of the European Union, such family members not only have the right to enter the territory of the Member State but also to obtain an entry visa for that purpose. Member States must grant such persons every facility to obtain the necessary visas which must be issued free of charge as soon as possible and on the basis of an accelerated procedure.
- (56) The right to obtain a visa is not unconditional as it can be denied to family members on grounds of public policy, public security or public health pursuant to Directive 2004/38/EC. Against that background, the personal data of family members can be verified only where the data relate to their identification and their status and only insofar as those data are relevant for the assessment of the security or public health threat that they could represent. The examination of the visa applications of such family members should be made exclusively against the security or public health concerns, and not those related to migration risks.
- (57) Since the objectives of this Regulation cannot be sufficiently achieved by the Member States but can rather, by reason of the need to ensure the implementation of a common policy on visas, a high level of security within the area without controls at the internal borders and the gradual establishment of an integrated management system for the external borders, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.
- (58) This Regulation establishes strict access rules to the VIS and the necessary safeguards. It also provides for individuals' rights of access, rectification, erasure and remedies in particular the right to a judicial remedy and the supervision of data processing operations by independent public authorities. Additional safeguards are introduced by this Regulation to cover for the specific needs of the new categories of data that will be processed by the VIS. This Regulation therefore respects the fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the European Union, in particular the right to human dignity, the right to liberty and security, the respect for private and family life, the protection of personal data, the right to asylum and protection of the principle of non-refoulement and protection in the event of removal, expulsion or extradition, the right to non-discrimination, the rights of the child and the right to an effective remedy.
- (59) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the TEU and to the TFEU, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Given that this Regulation builds upon the Schengen *acquis*, Denmark shall, in accordance with Article 4 of that Protocol, decide within a period of six months after the Council has decided on this Regulation whether it will implement it in its national law.

<sup>(20)</sup> Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (OJ L 158, 30.4.2004, p. 77).

- (60) This Regulation constitutes a development of the provisions of the Schengen *acquis* in which Ireland does not take part, in accordance with Council Decision 2002/192/EC <sup>(21)</sup>; Ireland is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.
- (61) As regards Iceland and Norway, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latter's association with the implementation, application and development of the Schengen *acquis* <sup>(22)</sup> which fall within the area referred to in Article 1, points A, B, C and F, of Council Decision 1999/437/EC <sup>(23)</sup>.
- (62) As regards Switzerland, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* <sup>(24)</sup> which fall within the area referred to in Article 1, points A, B, C and F, of Council Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/146/EC <sup>(25)</sup> and with Article 3 of Council Decision 2008/149/JHA <sup>(26)</sup>.
- (63) As regards Liechtenstein, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* <sup>(27)</sup> which fall within the area referred to in Article 1, points A, B, C and F, of Council Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU <sup>(28)</sup> and with Article 3 of Council Decision 2011/349/EU <sup>(29)</sup>.
- (64) As regards Cyprus, Bulgaria, Romania and Croatia, the provisions of this Regulation constitute provisions building upon, or otherwise relating to, the Schengen *acquis* within, respectively, the meaning of Article 3(2) of the 2003 Act of Accession, Article 4(2) of the 2005 Act of Accession read in conjunction with Council Decision (EU) 2017/1908 <sup>(30)</sup> and Article 4(2) of the 2011 Act of Accession.

<sup>(21)</sup> Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen *acquis* (OJ L 64, 7.3.2002, p. 20).

<sup>(22)</sup> OJ L 176, 10.7.1999, p. 36.

<sup>(23)</sup> Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis* (OJ L 176, 10.7.1999, p. 31).

<sup>(24)</sup> OJ L 53, 27.2.2008, p. 52.

<sup>(25)</sup> Council Decision 2008/146/EC of 28 January 2008 on the conclusion, on behalf of the European Community, of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L 53, 27.2.2008, p. 1).

<sup>(26)</sup> Council Decision 2008/149/JHA of 28 January 2008 on the conclusion on behalf of the European Union of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L 53, 27.2.2008, p. 50).

<sup>(27)</sup> OJ L 160, 18.6.2011, p. 21.

<sup>(28)</sup> Council Decision 2011/350/EU of 7 March 2011 on the conclusion, on behalf of the European Union, of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*, relating to the abolition of checks at internal borders and movement of persons (OJ L 160, 18.6.2011, p. 19).

<sup>(29)</sup> Council Decision 2011/349/EU of 7 March 2011 on the conclusion on behalf of the European Union of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* relating in particular to judicial cooperation in criminal matters and police cooperation (OJ L 160, 18.6.2011, p. 1).

<sup>(30)</sup> 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 (OJ L 269, 19.10.2017, p. 39).

- (65) Decisions 2004/512/EC and 2008/633/JHA should be repealed. The references to the repealed Decisions should be construed as references to Regulation (EC) No 767/2008 and should be read in accordance with the correlation tables in Annexes I and II, respectively.
- (66) Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 should be amended.
- (67) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council <sup>(31)</sup> and delivered an opinion on 12 December 2018 <sup>(32)</sup>,

HAVE ADOPTED THIS REGULATION:

#### Article 1

### Amendments to Regulation (EC) No 767/2008

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

- (1) the title is replaced by the following:

**“Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of information between Member States on short-stay visas, long-stay visas and residence permits (VIS Regulation)”;**

- (2) Article 1 is amended as follows:

- (a) the first paragraph is replaced by the following:

“This Regulation establishes the Visa Information System (VIS) and defines the purpose and functionalities of and the responsibilities for the system. 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 related decisions.”;

- (b) the following paragraph is inserted after the first paragraph:

“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.”;

- (3) Article 2 is replaced by the following:

#### “Article 2

#### **Purpose of the VIS**

1. The purpose of the VIS is to improve the implementation of the common visa policy for short stays, consular cooperation and consultation between visa authorities by facilitating the exchange of data between Member States on applications and on the decisions relating thereto, in order to:

- (a) facilitate the visa application procedure;
- (b) prevent the bypassing of the criteria for the determination of the Member State responsible for examining the visa application;
- (c) facilitate the fight against fraud;
- (d) facilitate checks at external border crossing points and within the territory of the Member States;

<sup>(31)</sup> Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 008, 12.1.2001, p.1).

<sup>(32)</sup> OJ C 50, 8.2.2019, p. 4.



- (e) assist in the identification and return of any person who does not or no longer fulfils the conditions for entry to, stay or residence on the territory of the Member States;
- (f) assist in the identification of persons in specific circumstances as referred to in Article 22p;
- (g) 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) contribute to the prevention, detection and investigation of terrorist offences or other serious criminal offences;
- (i) contribute to the prevention of threats to the internal security of any of the Member States;
- (j) contribute to 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, persons wanted for arrest or for surrender or extradition purposes, missing persons or vulnerable persons, persons sought to assist with a judicial procedure and 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 applications and decisions related thereto, in order to:

- (a) support a high level of security in all Member States by contributing to the assessment of whether the applicant for or holder of a long-stay visa or a residence permit is considered to pose a threat to public policy, internal security or public health;
- (b) facilitate checks at external border crossing points and within the territory of the Member States;
- (c) assist in the identification and return of any person who does not or no longer fulfils the conditions for entry to, stay or residence on the territory of the Member States;
- (d) contribute to the prevention, detection and investigation of terrorist offences or other serious criminal offences;
- (e) contribute to the correct identification of persons;
- (f) assist in the identification of persons in specific circumstances as referred to in Article 22p;
- (g) facilitate the application of Regulation (EU) No 604/2013 and of Directive 2013/32/EU;
- (h) support the objectives of the SIS related to alerts in respect of third-country nationals subject to a refusal of entry, persons wanted for arrest, for surrender or extradition purposes, missing persons or vulnerable persons, persons sought to assist with a judicial procedure and persons for discreet checks, inquiry checks or specific checks.

#### *Article 2a*

### **Architecture**

1. The VIS shall be based on a centralised architecture and shall consist of:

- (a) the common identity repository (CIR) established by Article 17(1) of Regulation (EU) 2019/817;
- (b) a central information system (the 'VIS Central System');
- (c) national uniform interfaces (NUIs) in each Member State, based on common technical specifications and identical for all Member States, enabling the VIS Central System to connect to the national infrastructures in Member States;
- (d) a communication infrastructure between the VIS Central System and the NUIs;
- (e) a secure communication channel between the VIS Central System and the Central System of the Entry/Exit System (EES);

- (f) a secure communication infrastructure between the VIS Central System and:
  - (i) the central infrastructures of the European search portal (ESP) established by Article 6 of Regulation (EU) 2019/817;
  - (ii) the shared biometric matching service established by Article 12 of Regulation (EU) 2019/817;
  - (iii) the CIR; and
  - (iv) the multiple-identity detector established by Article 25 of Regulation (EU) 2019/817;
- (g) a mechanism for consultation with regard to applications and the exchange of information between visa authorities (VISMail);
- (h) a carrier gateway;
- (i) a secure web service enabling communication between the VIS Central System on the one hand and the carrier gateway and international systems (Interpol databases) on the other hand;
- (j) a repository of data for the purposes of reporting and statistics.

The VIS Central System, the NUIs, the web service, the carrier gateway and the VIS communication infrastructure shall share and re-use as much as technically possible the hardware and software components of, respectively, the EES Central System, the EES national uniform interfaces, the ETIAS carrier gateway, the EES web service and the EES communication infrastructure.

2. There shall be at least two NUIs as referred to in point (c) of paragraph 1 for each Member State, which shall provide the physical connection between Member States and the physical network of the VIS. The connection through the communication infrastructure referred to in point (d) of paragraph 1 shall be encrypted. The NUIs shall be located at Member State premises. The NUIs shall be used exclusively for purposes established by Union legislative acts.

3. The VIS Central System shall perform technical supervision and administration functions and have a backup VIS Central System, capable of ensuring all functionalities of the VIS Central System in the event of failure of that system. The VIS Central System shall be located in Strasbourg (France) and the backup VIS Central System shall be located in Sankt Johann im Pongau (Austria).

4. The communication infrastructure shall support and contribute to ensuring the uninterrupted availability of the VIS. It shall include redundancies for the connections between the VIS Central System and the backup VIS Central System and redundancies for the connections between each NUI on the one hand and the VIS Central System and the backup VIS Central System on the other hand. The communication infrastructure shall provide an encrypted virtual private network dedicated to VIS data and to communication among Member States and between Member States and eu-LISA.

5. eu-LISA shall implement technical solutions to ensure the uninterrupted availability of the VIS either through the simultaneous operation of the VIS Central System and the backup VIS Central System, provided that the backup VIS Central System remains capable of ensuring the operation of the VIS in the event of a failure of the VIS Central System, or through duplication of the system or its components.

\* Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 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 (OJ L 180, 29.6.2013, p. 31).

\*\* Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection (OJ L 180, 29.6.2013, p. 60).";

(4) Article 3 is deleted;

(5) Article 4 is amended as follows:

(a) points (3), (4) and (5) are replaced by the following:

“3. ‘visa authorities’ means the authorities in each Member State which are responsible for examining and for taking decisions on visa applications or for taking decisions on whether to annul, revoke or extend visas, including the central visa authorities and the authorities responsible for issuing visas at the border;

3a. ‘designated authority’ means an authority designated by a Member State pursuant to Article 22l(1) as responsible for the prevention, detection or investigation of terrorist offences or other serious criminal offences;

3b. ‘VIS designated authority’ means an authority designated by a Member State pursuant to Article 9d(1) as responsible for the manual verification and follow-up action with regard to hits referred to in that paragraph;

3c. ‘ETIAS Central Unit’ means the unit established within the European Border and Coast Guard Agency pursuant to Article 7 of Regulation (EU) 2018/1240 of the European Parliament and of the Council \*;

4. ‘application form’ means the harmonised application form for a Schengen Visa set out in Annex I to Regulation (EC) No 810/2009;

5. ‘applicant’ means a person who has lodged an application for a visa, long-stay visa or residence permit;

\* Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018, p. 1).”;

(b) points (12), (13) and (14) are replaced by the following:

“12. ‘VIS data’ means all data stored in the VIS Central System and in the CIR in accordance with Articles 9 to 14 and 22a to 22f;

13. ‘identity data’ means the data referred to in point (4)(a) and (aa) of Article 9 and point (d) of Article 22a(1);

14. ‘fingerprint data’ means the VIS data relating to fingerprints;

15. ‘facial image’ means digital image of the face;

16. ‘hit’ means the existence of a correspondence established by an automated comparison of the personal data recorded in an application file of the VIS with the specific risk indicators referred to in Article 9j or with the personal data present in a record, file or alert registered in the VIS, in another EU information system as referred to in Article 9a or 22b (EU information systems), in Europol data or in Interpol databases queried by the VIS;

17. ‘Europol data’ means personal data processed by Europol for the purpose referred to in point (a) of Article 18(2) of Regulation (EU) 2016/794 of the European Parliament and of the Council \*;

18. ‘residence permit’ means a residence permit issued by a Member State in accordance with the uniform format laid down by Council Regulation (EC) No 1030/2002 \*\* and a document as referred to in point (16) (b) of Article 2 of Regulation (EU) 2016/399;

19. ‘long-stay visa’ means an authorisation issued by a Member State as provided for in Article 18 of the Schengen Convention;

20. ‘supervisory authorities’ means the supervisory authority referred to in Article 51(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council \*\*\* and the supervisory authority referred to in Article 41 of Directive (EU) 2016/680 of the European Parliament and of the Council \*\*\*\*;

21. 'law enforcement' means the prevention, detection or investigation of terrorist offences or other serious criminal offences;
22. 'terrorist offence' means any of the offences under national law referred to in Articles 3 to 14 of Directive (EU) 2017/541 of the European Parliament and of the Council \*\*\*\* or, for the Member States which are not bound by that Directive, the offences under national law equivalent to one of those offences;
23. 'serious criminal offence' means an offence which corresponds or is equivalent to one of the offences referred to in Article 2(2) of Council Framework Decision 2002/584/JHA \*\*\*\*\*, if it is punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years.

\* Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).

\*\* Council Regulation (EC) No 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third-country nationals (OJ L 157, 15.6.2002, p. 1).

\*\*\* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

\*\*\*\* Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

\*\*\*\*\* Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, p. 6).

\*\*\*\*\* Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p.1).";

(6) Articles 5 and 6 are replaced by the following:

"Article 5

### Categories of data

1. Only the following categories of data shall be recorded in the VIS:
  - (a) alphanumeric data:
    - (i) on the visa applicant and on visas requested, issued, refused, annulled, revoked or extended referred to in points (1) to (4) of Article 9 and in Articles 10 to 14;
    - (ii) on the applicant for a long-stay visa or a residence permit and on long-stay visas and residence permits requested, issued, refused, withdrawn, revoked, annulled, extended or renewed as referred to in Article 22a and Articles 22c to 22f;
    - (iii) regarding the hits referred to in Articles 9a and 22b and the reasoned opinions referred to in Articles 9e, 9g and 22b;
  - (b) facial images as referred to in point (5) of Article 9 and in point (j) of Article 22a(1);
  - (c) fingerprint data as referred to in point (6) of Article 9 and in point (k) of Article 22a(1);
  - (ca) scans of the biographic data page of the travel document referred to in point (7) of Article 9 and in point (h) of Article 22a(1);
  - (d) links to other applications as referred to in Article 8(3) and (4) and Article 22a(4).

- 1a. The CIR shall contain the data referred to in points (4)(a) to (ca) and points (5) and (6) of Article 9 and in points (d) to (g), (j) and (k) of Article 22a(1). The remaining VIS data shall be stored in the VIS Central System.
- 1b. Verification and identification in the VIS by means of a facial image shall be possible only against facial images recorded in the VIS with an indication that the facial image was taken live upon submission of the application, in accordance with point (5) of Article 9 and point (j) of Article 22a(1).
2. Without prejudice to the recording of data processing operations pursuant to Article 34, the messages transmitted by the VISMail in accordance with Article 16, Article 24(2) and Article 25(2) shall not be recorded in the VIS.

#### 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 set out in 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 Commission shall adopt implementing acts to lay down detailed rules on managing the functionality referred to in paragraph 2 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 49(2).

#### Article 6

#### Access for entering, amending, erasing and consulting data

1. Access to the VIS for entering, amending or erasing the data referred to in Article 5(1) shall be reserved exclusively to the duly authorised staff of the visa authorities and to the authorities competent to collect or decide on an application for a long-stay visa or residence permit in accordance with Article 22a to 22f. The number of duly authorised members of staff shall be limited by the actual needs of their service.
2. Access to the VIS to consult the data shall be reserved exclusively for the duly authorised staff of the national authorities of each Member State and of the Union bodies which are competent for the purposes of Articles 15 to 22, Articles 22g to 22m and Article 45e of this Regulation, as well as for the purposes laid down in Articles 20 and 21 of Regulation (EU) 2019/817.

Such access shall be limited to the extent that the data are required for the performance of the tasks of those authorities and Union bodies in accordance with those purposes, and proportionate to the objectives pursued.

- 2a. By way of derogation from the provisions on the use of data provided for in Chapters II, III and IIIa, fingerprint data and facial images of children shall only be used to search the VIS and, in the case of a hit, shall only be accessed to verify the child's identity:
  - (a) in the visa application procedure in accordance with Article 15; or
  - (b) at the external borders or within the territory of the Member States in accordance with Article 18, 19 or 20 or with Article 22g, 22h or 22i.

Where the search with alphanumerical data cannot be performed due to the lack of a travel document, the fingerprint data of children may also be used to search the VIS in the asylum procedure in accordance with Article 21, 22, 22j or 22k.

- 2b. By way of derogation from the provisions on the use of data provided for in Article 22h, in the case of persons who have held valid residence permits recorded in the VIS for a period of 10 years or more without interruption, the authorities competent for carrying out checks within the territory of the Member States shall only have access to the VIS to consult the data referred to in points (d), (e) and (f) of Article 22c and the status information of the residence permit.

- 2c. By way of derogation from the provisions on the use of data provided for in Article 22i, in the case of persons who have held valid residence permits recorded in the VIS for a period of 10 years or more without interruption, the authorities competent for carrying out checks within the territory of the Member States shall only have access to the VIS to consult the data referred to in points (d), (e) and (f) of Article 22c and the status information of the residence permit. Where the person does not present a valid travel document or where there are doubts as to the authenticity of the travel document presented or where the verification pursuant to Article 22h has failed, the competent authorities shall also have access the VIS to consult the data referred to in points (d) to (g) and (i) of Article 22a(1).
- 2d. By way of derogation from the provisions on the use of data provided for in Articles 22j and 22k, the competent asylum authorities shall not have access to VIS data of persons who have held valid residence permits recorded in the VIS in accordance with Chapter IIIa for a period of 10 years or more without interruption.
- 2e. By way of derogation from the provisions on the use of data provided for in Chapter IIIb, the Member States' designated authorities and Europol shall not have access to VIS data of persons who have held valid residence permits recorded in the VIS in accordance with Chapter IIIa for a period of 10 years or more without interruption.
- 2f. By way of derogation from the provisions on the use of data provided for in Articles 45e and 45f, the members of the European Border and Coast Guard teams, with the exception of border management teams, shall not have access to VIS data of persons who have held valid residence permits recorded in the VIS in accordance with Chapter IIIa for a period of 10 years or more without interruption.
3. Each Member State shall designate the competent authorities the duly authorised staff of which shall have access to the VIS to enter, amend, erase or consult VIS data. Each Member State shall without delay communicate a list of those authorities to the Commission and eu-LISA, in accordance with Article 45b. The list shall specify the purpose for which each authority may process VIS data. Each Member State may at any time amend or replace the list which it communicated and shall inform the Commission and eu-LISA accordingly.

The authorities entitled to consult or access the VIS for the purposes of prevention, detection and investigation of terrorist offences or other serious criminal offences shall be designated in accordance with Chapter IIIb.

4. In addition to the communications mentioned in paragraph 3, each Member State shall communicate to eu-LISA without delay a list of the operating units of the national competent authorities having access to the VIS for the purposes of this Regulation. The list shall specify the purpose for which each operating unit is to have access to VIS data. The VIS shall provide the functionality for the centralised management of those lists.

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

---

\* Decision No 1105/2011/EU of the European Parliament and of the Council of 25 October 2011 on the list of travel documents which entitle the holder to cross the external borders and which may be endorsed with a visa and on setting up a mechanism for establishing this list (OJ L 287, 4.11.2011, p. 9).";

(7) in Article 7, paragraph 2 is replaced by the following:

"2. Each competent authority shall ensure that processing of personal data within the VIS does not result in discrimination against applicants for or holders of visas, long-stay visas and residence permits on the grounds of sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

When processing personal data within the VIS each competent authority shall fully respect human dignity and the fundamental rights and principles recognised by the Charter of Fundamental Rights of the European Union, including the right to respect for one's private life and to the protection of personal data.

Particular attention shall be paid to children, the elderly and persons with a disability.

3. The best interests of the child shall be a primary consideration for Member States with respect to all procedures under this Regulation, in accordance with the safeguards laid down in the United Nations Convention on the Rights of the Child.

The well-being, safety and security of the child shall be taken into consideration, especially where there is a risk that the child may be a victim of human trafficking. The views of the child shall also be taken into consideration, giving appropriate weight to the age and maturity of the child.”;

(8) the title of Chapter II is replaced by the following:

“ENTRY AND USE OF DATA ON VISAS BY VISA AUTHORITIES”;

(9) Article 8 is amended as follows:

(a) paragraph 1 is replaced by the following:

“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 three working days by entering the data referred to in Article 9 in the VIS, in so far as those data are required to be provided by the applicant.”;

(b) paragraph 5 is replaced by the following:

“5. Where particular data are not required to be provided for legal reasons or cannot be provided, the specific data fields shall be marked as ‘not applicable’. The absence of fingerprints shall be indicated by “VIS 0”; furthermore, the system shall permit a distinction to be made between the cases pursuant to points (a) to (e) of Article 13(7) of Regulation (EC) No 810/2009.

6. Upon creation of the application file in accordance with the procedures referred to in paragraphs 1 to 5 of this Article, the VIS shall automatically launch the queries pursuant to Article 9a and return results. The competent visa authority shall consult the VIS for the purpose of examining the application in accordance with Article 15.”;

(10) Article 9 is amended as follows:

(a) point (4) is amended as follows:

(i) points (a) to (ca) are replaced by the following:

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

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

(b) the type and number of the travel document;

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

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

(ii) point (l) is replaced by the following:

“(l) current occupation (job group) and employer; for students: name of educational establishment;”;

(iii) the following point is added:

“(n) if applicable, the fact that the applicant applies as a family member of a Union citizen to whom Directive 2004/38/EC of the European Parliament and of the Council \* applies or of a third-country national enjoying the right of free movement equivalent to that of Union citizens under an agreement between the Union and its Member States, on the one hand, and a third country, on the other;

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

(b) points (5) and (6) are replaced by the following:

“5. a facial image of the applicant, in accordance with Article 13 of Regulation (EC) No 810/2009, with an indication of whether the facial image was taken live upon submission of the application;

6. fingerprints of the applicant, in accordance with Article 13 of Regulation (EC) No 810/2009;

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

(c) the following paragraphs are added:

“The applicant shall indicate his or her current occupation (job group) on a predetermined list.

The Commission shall adopt delegated acts in accordance with Article 48a to lay down the predetermined list of occupations (job groups).”;

(11) the following articles are inserted:

“Article 9a

#### **Queries of other information systems and databases**

1. The application files shall be processed automatically by the VIS to identify hits in accordance with this Article. The VIS shall examine each application file individually.

2. When an application file is created, the VIS shall check whether the travel document related to that application is recognised in accordance with Decision No 1105/2011/EU, by performing an automatic search against the list of recognised travel documents referred to in Article 5a of this Regulation, and shall return a result. If the search shows that the travel document is not recognised by one or more Member States, Article 25(3) of Regulation (EC) No 810/2009 shall apply where a visa is issued.

3. For the purposes of the verifications provided for in Article 21(1), points (a), (c) and (d) of Article 21(3) and Article 21(4) of Regulation (EC) No 810/2009 and for the purposes of the objective referred to in point (k) of Article 2(1) of this Regulation, the VIS shall launch a query by using the ESP to compare the relevant data referred to in points (4), (5) and (6) of Article 9 of this Regulation with the data present in a record, file or alert registered in:

(a) the SIS;

(b) the EES;

(c) the European Travel Information and Authorisation System (ETIAS), including the ETIAS watchlist referred to in Article 34 of Regulation (EU) 2018/1240 (the ETIAS watchlist);

(d) Eurodac;

(e) the European Criminal Records Information System for third-country nationals (ECRIS-TCN);



- (f) the Europol data;
- (g) the Interpol Stolen and Lost Travel Document database (Interpol SLTD), and
- (h) the Interpol Travel Documents Associated with Notices database (Interpol TDAWN).

The comparison shall be made with both alphanumeric and biometric data, unless the information system or database queried contains only one of those data categories.

4. In particular, the VIS shall verify:

- (a) as regards the SIS, whether:
  - (i) the travel document used for the application corresponds to a travel document which has been lost, stolen, misappropriated or invalidated;
  - (ii) the applicant is subject to an alert for refusal of entry and stay;
  - (iii) the applicant is subject to an alert on return;
  - (iv) the applicant is subject to an alert on persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant, or wanted for arrest for extradition purposes;
  - (v) the applicant is subject to an alert on missing persons or vulnerable persons who need to be prevented from travelling;
  - (vi) the applicant is subject to an alert on persons sought to assist with a judicial procedure;
  - (vii) the applicant or the travel document is subject to an alert on persons or objects for discreet checks, inquiry checks or specific checks;
- (b) as regards the EES, whether:
  - (i) the applicant is currently reported as an overstayer or the applicant has been reported as an overstayer in the past in the EES;
  - (ii) the applicant is recorded as having been refused entry in the EES;
  - (iii) the intended stay of the applicant will exceed 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;
- (c) as regards the ETIAS, whether:
  - (i) the applicant is a person for whom an issued, refused, annulled or revoked travel authorisation is recorded in the ETIAS or the applicant's travel document corresponds to such issued, refused, annulled or revoked travel authorisation;
  - (ii) the data provided as part of the application correspond to data present in the ETIAS watchlist;
- (d) as regards Eurodac, whether the applicant is registered in that database;
- (e) as regards the ECRIS-TCN, whether the applicant corresponds to a person whose data have been recorded in that system during the previous 25 years as far as convictions for terrorist offences are concerned or during the previous 15 years as far as convictions for other serious criminal offences are concerned;
- (f) as regards Europol data, whether the data provided in the application correspond to data recorded in Europol data;
- (g) as regards Interpol databases, whether:
  - (i) the travel document used for the application corresponds to a travel document reported lost, stolen or invalidated in Interpol SLTD;
  - (ii) the travel document used for the application corresponds to a travel document recorded in a file in Interpol TDAWN.

5. SIS alerts in respect of missing persons or vulnerable persons, persons sought to assist with a judicial procedure and persons or objects for discreet checks, inquiry checks or specific checks shall be queried only for the purposes of the objective referred to in point (k) of Article 2(1).

6. As regards Interpol SLTD and Interpol TDAWN, any queries or verification shall be performed in such a way that no information shall be revealed to the owner of the Interpol alert. If the requirement provided for in this paragraph is not fulfilled, the VIS shall not query Interpol databases.

7. As regards Europol data, the automated processing shall receive the appropriate notification in accordance with Article 21(1b) of Regulation (EU) 2016/794.

8. A hit shall be triggered where all or some of the data from the application file used for the query correspond fully or partially to the data present in a record, alert or file of the information systems or databases referred to in paragraph 3. The manual referred to in Article 9h(2) shall define partial correspondence, including a degree of probability to limit the number of false hits.

9. Where the automatic comparison referred to in paragraph 3 reports a hit related to point (a)(i), (ii) and (iii), point (b), point (c)(i), point (d) and point (g)(i) of paragraph 4, the VIS shall add a reference in the application file to any hit and, where relevant, the Member States that entered or supplied the data having triggered the hit.

10. Where the automatic comparison referred to in paragraph 3 reports a hit related to point (a)(iv), point (c)(ii), points (e) and (f) and point (g)(ii) of paragraph 4, the VIS shall only indicate in the application file that further verification is needed.

In the event of hits pursuant to point (a)(iv), points (e) and (f) and point (g)(ii) of paragraph 4, the VIS shall send an automated notification regarding such hits to the VIS designated authority of the Member State processing the application. Such automated notification shall contain the data recorded in the application file in accordance with points (4), (5) and (6) of Article 9.

In the event of hits pursuant to point (c)(ii) of paragraph 4, the VIS shall send an automated notification regarding such hits to the ETIAS National Unit of the Member State that entered the data or, if the data was entered by Europol, to the ETIAS National Unit of the Member States processing the application. That automated notification shall contain the data recorded in the application file in accordance with point (4) of Article 9.

11. Where the automatic comparison referred to in paragraph 3 reports a hit related to point (a)(v), (vi) and (vii) of paragraph 4, the VIS shall neither record the hit in the application file nor indicate in the application file that further verification is needed.

12. The unique reference number of the data record having triggered a hit shall be kept in the application file for the purpose of the keeping of logs, reporting and statistics in accordance with Articles 34 and 45a.

13. The VIS shall compare the relevant data referred to in point (4)(a), (aa), (g), (h), (j), (k) and (l) of Article 9 to the specific risk indicators referred to in Article 9j.

#### *Article 9b*

### **Specific provisions for family members of Union citizens or of other third-country nationals enjoying the right of free movement under Union law**

1. As regards a third-country national who is a family member of a Union citizen to whom Directive 2004/38/EC applies or of a third-country national enjoying the right of free movement equivalent to that of Union citizens under an agreement between the Union and its Member States, on the one hand, and a third country, on the other, the automated queries pursuant to 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 that third-country national 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:

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

3. Where the automated processing pursuant to Article 9a(3) of this Regulation has reported a hit corresponding to an alert for refusal of entry and stay as referred to in Article 24 of Regulation (EU) 2018/1861, the visa authority shall verify the ground for the decision following which this alert was entered in the SIS. If that 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 in accordance with Article 26(2) of Regulation (EU) 2018/1861.
4. The specific risk indicators based on illegal immigration risks determined pursuant to Article 9j shall not apply.

#### *Article 9c*

#### **Manual verification and follow-up action with regard to hits by competent visa authorities**

1. Any hit pursuant to Article 9a(9) shall be manually verified by the competent visa authority of the Member State processing the visa application.
2. For the purposes of manual verification under paragraph 1 of this Article, the competent visa authority shall have access to the application file and any linked application files, as well as to the hits triggered during the automated processing pursuant to Article 9a(9).

The competent visa authority shall also have temporary access to data in the SIS, the EES, the ETIAS, Eurodac or Interpol SLTD that triggered the hit for the duration of the verifications referred to in this Article and the examination of the visa application and in the event of an appeal procedure. Such temporary access shall be in accordance with the legal instruments governing the SIS, the EES, the ETIAS, Eurodac and Interpol SLTD.

3. The competent visa authority shall verify whether the identity of the applicant recorded in the application file corresponds to the data in any of the information systems or databases queried.
4. Where the personal data in the application file correspond to the data stored in the relevant information system or database, the hit shall be taken into account in the examination of the visa application pursuant to Article 21 of Regulation (EC) No 810/2009.
5. Where the personal data in the application file do not correspond to the data stored in the relevant information system or database, the competent visa authority shall erase the false hit from the application file.
6. Where automatic comparison pursuant to Article 9a(13) of this Regulation reports a hit, the competent visa authority shall assess the security, illegal immigration or high epidemic risk and shall take it into account in the examination of a visa application pursuant to Article 21 of Regulation (EC) No 810/2009. The competent visa authority shall in no circumstances take a decision automatically on the basis of a hit based on specific risk indicators. The competent visa authority shall individually assess the security, illegal immigration and high epidemic risks in all cases.

#### *Article 9d*

#### **Manual verification of hits by VIS designated authorities**

1. Each Member State shall designate an authority (the “VIS designated authority”) for the purposes of the manual verification and follow-up action with regard to hits pursuant to points (a)(iv) to (vii), points (e) and (f) and point (g)(ii) of Article 9a(4). Member States may designate more than one authority as the VIS designated authority. Member States shall notify the Commission and eu-LISA of the VIS designated authority.

Where Member States choose to designate the SIRENE Bureau as the VIS designated authority, they shall allocate sufficient additional resources to enable the SIRENE Bureau to fulfil the tasks entrusted to the VIS designated authority under this Regulation.

2. The VIS designated authority shall be operational at least during regular working hours. It shall have temporary access to the data recorded in the application file and the data in the SIS, ECRIS-TCN, Europol data or Interpol TDawn that triggered the hit, for the duration of the verification referred to in this Article and in Article 9g.

3. The VIS designated authority shall verify, within two working days from the notification sent by the VIS, whether the identity of the applicant recorded in the application file corresponds to the data present in one of the information systems or databases queried.
4. Where the personal data in the application file do not correspond to the data stored in the relevant information system or database, the VIS designated authority shall erase the indication in the application file that further verification is needed.

#### Article 9e

##### **Manual verification and follow-up action with regard to hits in the ETIAS watchlist**

1. The ETIAS National Unit of the Member State which entered the data in the ETIAS watchlist or, if the data was entered by Europol, the ETIAS National Unit of the Member State processing the application shall manually verify and carry out follow-up action with regard to hits pursuant to point (c)(ii) of Article 9a(4).
2. The relevant ETIAS National Unit shall verify, within two working days from the notification sent by the VIS, whether the data recorded in the application file corresponds to the data in the ETIAS watchlist.
3. Where the data in the application file corresponds to the data in the ETIAS watchlist, the ETIAS National Unit shall provide a reasoned opinion to the central visa authority of the Member State processing the visa application on whether the applicant poses a risk to public security, which shall be taken into account in the examination of the visa application pursuant to Article 21 of Regulation (EC) No 810/2009.
4. Where the data was entered into the ETIAS watchlist by Europol, the ETIAS National Unit of the Member State processing the application shall, for the purpose of drafting its reasoned opinion, request without delay the opinion of Europol. For that purpose, the ETIAS National Unit shall send the data recorded in the application file in accordance with point (4) of Article 9 to Europol. Europol shall reply within 60 hours of the date of the request. Where Europol does not reply within that deadline, there shall be deemed to be no grounds for objecting to the issuing of the visa.
5. The ETIAS National Unit shall send the reasoned opinion to the central visa authority within seven calendar days from the notification sent by the VIS. Where the ETIAS National Unit sends no reasoned opinion within that deadline, there shall be deemed to be no grounds for objecting to the issuing of the visa.
6. The reasoned opinion shall be recorded in the application file in a manner that renders it accessible only to the central visa authority of the Member State processing the visa application.
7. Where the data in the application file do not correspond to the data in the ETIAS watchlist, the ETIAS National Unit shall inform the central visa authority of the Member State processing the visa application which shall erase the record of further verification being needed from the application file.

#### Article 9f

##### **Follow-up action with regard to certain hits by the SIRENE Bureau**

1. In the event of hits pursuant to point (a)(iii) to (vii) of Article 9a(4), and after manual verification, the competent visa authority or the VIS designated authority shall notify such hits to the SIRENE Bureau of the Member State processing the application.
2. In the event of hits pursuant to point (a)(iii) of Article 9a(4), the SIRENE Bureau of the Member State processing the application shall:
  - (a) where the return decision is accompanied by an entry ban, immediately inform the issuing Member State through the exchange of supplementary information, in order that the issuing Member State immediately delete the alert on return and enter an alert for refusal of entry and stay pursuant to point (b) of Article 24(1) of Regulation (EU) 2018/1861;
  - (b) where the return decision is not accompanied by an entry ban, immediately inform the issuing Member State through the exchange of supplementary information, in order that the issuing Member State delete the alert on return without delay.

3. In the event of hits pursuant to point (a)(iv) to (vii) of Article 9a(4) of this Regulation, the SIRENE Bureau of the Member State processing the application shall take any appropriate follow-up action in accordance with Regulation (EU) 2018/1862.

#### Article 9g

##### **Follow-up action with regard to certain hits by VIS designated authorities**

1. In the event of verified hits pursuant to point (e) or (f) or point (g)(ii) of Article 9a(4), the VIS designated authority shall, if necessary, take any appropriate follow-up action. For that purpose, it shall consult, where appropriate, the Interpol National Central Bureau of the Member State processing the application, Europol or the central authority of the convicting Member State designated in accordance with Article 3(1) of Council Framework Decision 2009/315/JHA \*.

2. The VIS designated authority shall provide a reasoned opinion on whether the applicant poses a threat to public security to the central visa authority of the Member State processing the visa application, which shall be taken into account in the examination of the visa application pursuant to Article 21 of Regulation (EC) No 810/2009.

3. In the event of verified hits pursuant to point (e) of Article 9a(4) of this Regulation, where the conviction was handed down prior to the start of operations of ECRIS-TCN in accordance with Article 35(4) of Regulation (EU) 2019/816, the VIS designated authority shall, in the reasoned opinion referred to in paragraph 2 of this Article, not take account of convictions for terrorist offences handed down more than 25 years before the date of the visa application or of convictions for other serious criminal offences handed down more than 15 years before the date of the visa application.

4. Where a hit manually verified by the VIS designated authority concerns the Europol data referred to in point (f) of Article 9a(4), the VIS designated authority shall request without delay the opinion of Europol in order to carry out its task as referred to in paragraph 2 of this Article. For that purpose, the VIS designated authority shall send the data recorded in the application file in accordance with points (4), (5) and (6) of Article 9 to Europol. Europol shall reply within 60 hours of the date of the request. Where Europol does not reply within that deadline, there shall be deemed to be no grounds for objecting to the issuing of the visa.

5. In the event of verified hits pursuant to point (a)(iv) of Article 9a(4) of this Regulation and after consulting the SIRENE bureau of the Member State issuing the alert, the VIS designated authority of the Member State processing the application shall provide a reasoned opinion on whether the applicant poses a threat to public security to the central visa authority processing the visa application, which shall be taken into account in the examination of the visa application pursuant to Article 21 of Regulation (EC) No 810/2009.

6. The reasoned opinion shall be recorded in the application file in a manner that renders it accessible only to the VIS designated authority referred to in Article 9d of the Member State processing the application and to the central visa authority of the same Member State.

7. The VIS designated authority shall send the reasoned opinion to the central visa authority within seven calendar days from the notification sent by the VIS. In the event of verified hits pursuant to point (e) of Article 9a(4), the deadline for sending the reasoned opinion shall be 10 calendar days. Where the VIS designated authority sends no such reasoned opinion within that deadline, there shall be deemed to be no grounds for objecting to the issuing of the visa.

#### Article 9h

##### **Implementation and manual**

1. For the purpose of implementing Articles 9a to 9g, eu-LISA shall, in cooperation with the Member States and Europol, establish appropriate channels for the notifications and exchange of information referred to in those Articles.

2. The Commission shall adopt a delegated act in accordance with Article 48a to lay down in a manual the procedures and rules necessary for queries, verifications and assessments.

*Article 9i***Responsibilities of Europol**

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

*Article 9j***Specific risk indicators**

1. The specific risk indicators shall be applied as an algorithm enabling profiling as defined in point (4) of Article 4 of Regulation (EU) 2016/679 through the comparison in accordance with Article 9a(13) of this Regulation of the data recorded in an application file of the VIS with specific risk indicators established by the ETIAS Central Unit under paragraph 4 of this Article pointing to security, illegal immigration or high epidemic risks. The ETIAS Central Unit shall enter the specific risk indicators in the VIS.

2. The Commission shall adopt a delegated act in accordance with Article 48a to further define the risks related to security or illegal immigration or a high epidemic risk on the basis of:

- (a) statistics generated by the EES indicating abnormal rates of overstaying and refusals of entry for a specific group of visa holders;
- (b) statistics generated by the VIS in accordance with Article 45a indicating abnormal rates of refusals of visa applications due to a security, illegal immigration or high epidemic risk associated with a specific group of visa holders;
- (c) statistics generated by the VIS in accordance with Article 45a and the EES indicating correlations between information collected through the application form and overstaying by visa holders 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 a Member State;
- (e) information substantiated by factual and evidence-based elements provided by Member States concerning abnormal rates of overstaying and refusals of entry for a specific group of visa holders for a 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 and disease outbreaks reported by the World Health Organization.

3. The Commission shall adopt an implementing act to specify the risks, as defined in this Regulation and in the delegated act referred to in paragraph 2 of this Article, on which the specific risks indicators referred to in paragraph 4 of this Article are to be based. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 49(2).

The specific risks referred to in the first subparagraph of this paragraph shall be reviewed at least every six months and, where necessary, a new implementing act shall be adopted by the Commission in accordance with the examination procedure referred to in Article 49(2).

4. Based on the specific risks determined in accordance with paragraph 3, the ETIAS Central Unit shall establish a set of specific risk indicators 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) the Member States of destination;
- (d) the Member State of first entry;
- (e) purpose of travel;
- (f) current occupation (job group).

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

6. The specific risk indicators shall be defined, established, assessed *ex ante*, implemented, evaluated *ex post*, revised and deleted by the ETIAS Central Unit after consulting the VIS Screening Board.

#### Article 9k

### VIS Screening Board

1. A VIS Screening Board with an advisory function is hereby established within the European Border and Coast Guard Agency. It shall be composed of a representative of the central visa authority of each Member State, of the European Border and Coast Guard Agency and of Europol.

2. The ETIAS Central Unit shall consult the VIS Screening Board on the definition, establishment, *ex ante* assessment, implementation, *ex post* evaluation, revision and deletion of the specific risk indicators referred to in Article 9j.

3. The VIS Screening Board shall issue opinions, guidelines, recommendations and best practices for the purposes referred to in paragraph 2. When issuing recommendations, the VIS Screening Board shall take into consideration the recommendations issued by the VIS Fundamental Rights Guidance Board.

4. The VIS Screening Board shall meet whenever necessary, and at least twice a year. The costs and servicing of its meetings shall be borne by the European Border and Coast Guard Agency.

5. The VIS Screening Board may consult the VIS Fundamental Rights Guidance Board on specific issues related to fundamental rights, in particular with regard to privacy, the protection of personal data and non-discrimination.

6. The VIS Screening Board shall adopt rules of procedure at its first meeting by a simple majority of its members.

#### Article 9l

### VIS Fundamental Rights Guidance Board

1. An independent VIS Fundamental Rights Guidance Board with an advisory and appraisal function is hereby established. Without prejudice to their respective competences and independence, it shall be composed of the Fundamental Rights Officer of the European Border and Coast Guard Agency, a representative of the consultative forum on fundamental rights of the European Border and Coast Guard Agency, a representative of the European Data Protection Supervisor, a representative of the European Data Protection Board established by Regulation (EU) 2016/679 and a representative of the European Union Agency for Fundamental Rights.

2. The VIS Fundamental Rights Guidance Board shall perform regular appraisals and issue recommendations to the VIS Screening Board on the impact on fundamental rights of the processing of applications and of the implementation of Article 9j, in particular with regard to privacy, the protection of personal data and non-discrimination.

The VIS Fundamental Rights Guidance Board shall also support the VIS Screening Board in the execution of its tasks when consulted by the latter on specific issues related to fundamental rights, in particular with regard to privacy, the protection of personal data and non-discrimination.

The VIS Fundamental Rights Guidance Board shall have access to the audits referred to in point (e) of Article 7(2) of Regulation (EU) 2018/1240.

3. The VIS Fundamental Rights Guidance Board shall meet whenever necessary, and at least twice a year. The costs and servicing of its meetings shall be borne by the European Border and Coast Guard Agency. Its meetings shall take place in premises of the European Border and Coast Guard Agency. The secretariat of its meetings shall be provided by the European Border and Coast Guard Agency. The VIS Fundamental Rights Guidance Board shall adopt rules of procedure at its first meeting by a simple majority of its members.

4. One representative of the VIS Fundamental Rights Guidance Board shall be invited to attend the meetings of the VIS Screening Board in an advisory capacity. The members of the VIS Fundamental Rights Guidance Board shall have access to the information and files of the VIS Screening Board.

5. The VIS Fundamental Rights Guidance Board shall produce an annual report. The report shall be made publicly available.

---

\* Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States (OJ L 93, 7.4.2009, p. 23).";

(12) in Article 10(1), point (f) is replaced by the following:

"(f) the territory in which the visa holder is entitled to travel, in accordance with Articles 24 and 25 of Regulation (EC) No 810/2009;"

(13) Article 11 is deleted;

(14) Article 12(2) is amended as follows:

(a) in point (a) the following point is inserted:

"(iia) does not provide the justification for the purpose and conditions of the intended airport transit;"

(b) the following subparagraph is added:

"The numbering of refusal grounds in the VIS shall correspond to the numbering of refusal grounds in the standard refusal form set out in Annex VI to Regulation (EC) No 810/2009;"

(15) in Article 13, the following paragraph is added:

"4. When the application file is updated pursuant to paragraphs 1 and 2 of this Article, the VIS shall send a notification to the Member State that issued the visa, informing of the decision to annul or revoke that visa and the grounds for that decision. Such notification shall be generated automatically by the VIS Central system and transmitted via VISMail in accordance with Article 16;"

(16) Article 15 is amended as follows:

(a) paragraph 1 is replaced by the following:

"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. The competent visa authority's consultation of the VIS shall establish:

(a) whether the applicant has been subject to a decision to issue, refuse, annul, revoke or extend a visa; and

(b) whether the applicant has been subject to a decision to issue, refuse, withdraw, revoke, annul, extend or renew a long-stay visa or residence permit;"

(b) paragraph 2 is amended, as follows:

(i) point (c) is replaced by the following:

"(c) the type and number of the travel document, the date of expiry of the validity of the travel document, the country which issued the travel document and its date of issue;"



(ii) point (f) is replaced by the following:

“(ea) facial image;

(f) the number of the visa sticker, long-stay visa or residence permit and the date of issue of any previous visa, long-stay visa or residence permit;”;

(c) the following paragraph is inserted:

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

(d) paragraph 3 is replaced by the following:

“3. If the search with one or several of the data listed in paragraph 2 of this Article indicates that data on the applicant are recorded in the VIS, the competent visa authority shall be given access to the application files and the linked application files pursuant to Article 8(3) and (4) and Article 22a(4), solely for the purposes referred to in paragraph 1 of this Article.”;

(17) Article 16 is replaced by the following:

“Article 16

#### **Use of the VIS for consultation and requests for documents**

1. For the purposes of consultation between central visa authorities on applications in accordance with Article 22 of Regulation (EC) No 810/2009, 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 by VISMail 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 by VISMail that response to the Member State which created the application.

In the case of a negative response, the response shall specify whether the applicant poses a threat to public policy, internal security, public health or international relations.

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 in accordance with Article 22 of Regulation (EC) No 810/2009 shall be integrated into the VIS. The VIS shall provide the functionality for the centralised management of that list.

3. The transmission of information by VISMail shall also apply to:

- (a) the transmission of information on visas issued to nationals of specific third countries or to specific categories of such nationals (*ex post* notification) pursuant to Article 31 of Regulation (EC) No 810/2009;
- (b) the transmission of information on visas issued with limited territorial validity pursuant to Article 25(4) of Regulation (EC) No 810/2009;
- (c) the transmission of information on decisions to annul and revoke a visa and the grounds for that decision pursuant to Article 13(4);
- (d) the transmission of requests for data rectification or erasure pursuant to Article 24(2) and Article 25(2) respectively as well as contacts between Member States pursuant to Article 38(2);
- (e) 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 documents supporting the application and to the transmission of electronic copies of those documents.

- 3a. The list of Member States requiring that their central authorities be informed of visas issued by other Member States to nationals of specific third countries or to specific categories of such nationals pursuant to Article 31 of Regulation (EC) No 810/2009 shall be integrated into the VIS. The VIS shall provide for the centralised management of that list.
- 3b. The transmission of information pursuant to points (a), (b) and (c) of paragraph 3 shall be automatically generated by the VIS.
- 3c. The competent visa authorities shall respond to requests pursuant to point (e) of paragraph 3 within three working days.
- 4. The personal data transmitted pursuant to this Article shall be used solely for the consultation and information of central visa authorities and consular cooperation.”;

(18) Article 17 is deleted;

(19) the title of Chapter III is replaced by the following:

“ACCESS TO VISA DATA BY OTHER AUTHORITIES”;

(20) Article 17a is amended, as follows:

(a) in paragraph 3, point (e) is replaced by the following:

“(e) verify, where the identity of a visa holder is verified using fingerprints or a facial image, the identity of a visa holder with fingerprints or, where the facial image is recorded in the VIS with the indication that it was taken live upon submission of the application, with the facial image against the VIS, in accordance with Article 23(2) and (4) of Regulation (EU) 2017/2226 and Article 18(6) of this Regulation.”;

(b) the following paragraphs are inserted:

“3a. Interoperability shall enable the VIS to launch the process of erasure of the facial image referred to in point (d) of Article 16(1) of Regulation (EU) 2017/2226 from the individual file of the EES where a facial image is recorded in the VIS with the indication that it was taken live upon submission of the application.

3b. Interoperability shall enable the EES to automatically notify the VIS in accordance with Article 23(3) of this Regulation where the exit of a child below the age of 12 is entered in the entry/exit record in accordance with Article 16(3) of Regulation (EU) 2017/2226.”;

(21) Article 18 is amended as follows:

(a) in paragraph 4, point (b) is replaced by the following:

“(b) facial images”;

(b) in paragraph 5, point (b) is replaced by the following:

“(b) facial images”;

(c) paragraph 6 is amended as follows:

(i) in point (a) of the first subparagraph, point (ii) is replaced by the following:

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

(ii) the second subparagraph is replaced by the following:

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

(d) paragraph 7 is replaced by the following:

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

(22) Article 19 is amended as follows:

(a) in paragraph 1, the second subparagraph is replaced by the following:

“Where the identity of the holder of the long-stay visa or residence permit cannot be verified with fingerprints, the competent authorities may also carry out the verification with the facial image.”;

(b) in paragraph 2, point (b) is replaced by the following:

“(b) facial images;”;

(23) in Article 19a, paragraph 4 is replaced by the following:

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

(24) Article 20 is amended, as follows:

(a) paragraph 1 is replaced by the following:

“1. Solely for the purposes of the identification of any person who may have been registered previously in the VIS or who does not, or no longer, fulfils 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 the VIS to search with the fingerprints of that person.

Where the fingerprints of that person cannot be used or the search with the fingerprints fails, the search shall be carried out with the data referred to in point (4)(a), (aa), (b), (c) or (ca), or point (5) of Article 9. However, the facial image shall not be the only search criterion.”;

(b) in paragraph 2, points (c) and (d) are replaced by the following:

“(c) facial images;

(d) the data entered in respect of any visa issued, refused, annulled, revoked or extended referred to in Articles 10 to 14.”;

(25) Articles 21 and 22 are replaced by the following:

“Article 21

#### **Access to VIS 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 Articles 12 and 34 of Regulation (EU) No 604/2013, the competent asylum authorities shall have access to the VIS to search with the fingerprints of the applicant for international protection.

Where the fingerprints of the applicant for international protection cannot be used or the search with the fingerprints fails, the search shall be carried out with the data referred to in point (4)(a), (aa), (b), (c) or (ca), or point (5) of Article 9. However, the facial image shall not be the only search criterion.

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

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

- (b) the data taken from the application form referred to in point (4)(a) and (aa) of Article 9;
- (c) facial images;
- (d) the data entered in respect of any visa issued, annulled, revoked or extended referred to in Articles 10, 13 and 14;
- (e) the data referred to in point (4)(a) and (aa) of Article 9 of the linked application files relating to 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 34(6) of Regulation (EU) No 604/2013.

#### Article 22

##### ***Access to VIS 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 34 of Regulation (EU) No 604/2013 to search with the fingerprints of the applicant for international protection.

Where the fingerprints of the applicant for international protection cannot be used or the search with the fingerprints fails, the search shall be carried out with the data referred to in point (4)(a), (aa), (b), (c) or (ca), or point (5) of Article 9. However, the facial image shall not be the only search criterion.

2. If the search with the data listed in paragraph 1 of this Article indicates that data on the applicant for international protection is recorded in the VIS, the competent asylum authority shall have access to the VIS to consult the following data of the applicant and of any linked application files of the applicant pursuant to Article 8(3), and, as regards the data listed in point (f) of this paragraph, of the spouse and children, pursuant to Article 8(4), for the sole purpose referred to in paragraph 1 of this Article:

- (a) the application number;
- (b) the data taken from the application forms referred to in point (4) of Article 9;
- (c) facial images as referred to in point (5) of Article 9;
- (d) scans of the biographic data page of the travel document as referred to in point (7) of Article 9;
- (e) the data entered in respect of any visa issued, annulled, revoked or extended referred to in Articles 10, 13 and 14;
- (f) the data referred to in point (4) of Article 9 of the linked application files relating to 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 34(6) of Regulation (EU) No 604/2013.”;

(26) after Article 22, the following chapters are inserted:

“CHAPTER IIIa

##### **ENTRY AND USE OF DATA ON LONG-STAY VISAS AND RESIDENCE PERMITS**

#### Article 22a

##### **Procedures for entering data upon application for a long-stay visa or residence permit**

1. Upon application for a long-stay visa or residence permit, the authority competent for collecting or examining the application shall create without delay an application file, by entering the following data in the VIS as far as those data are required to be provided by the applicant in accordance with the relevant Union or national law:

- (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, place of birth;
- (e) type and number of the travel document;
- (f) the date of expiry of the validity of the travel document;
- (g) the country 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 names of the applicant's parental authority or legal guardian;
- (j) the facial image of the applicant, with an indication of whether the facial image was taken live upon submission of the application;
- (k) fingerprints of the applicant.

2. With regard to fingerprints as referred to in point (k) of paragraph 1, the fingerprints of children below the age of six shall not be entered in the VIS.

With regard to facial images and fingerprints as referred to in points (j) and (k) of paragraph 1, the data of minors shall be entered in the VIS only where all of the following conditions are met:

- (a) the staff taking the data of a minor have been trained specifically to take a minor's biometric data in a child-friendly and child-sensitive manner and in full respect of the best interests of the child and the safeguards laid down in the United Nations Convention on the Rights of the Child;
- (b) every minor is accompanied by an adult family member or legal guardian when the data is taken;
- (c) no force is used to take the data.

3. Upon creation of the application file, the VIS shall automatically launch the queries pursuant to Article 22b.

4. If the applicant has applied as part of a group or with a family member, the authority shall create an application file for each person in the group and link the files of the persons having applied together for long-stay visas or residence permits.

5. Where particular data are not required to be provided in accordance with Union or national law or cannot be provided, the specific data fields 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 law and the cases where they cannot be provided.

#### *Article 22b*

### **Queries of information systems and databases**

1. The application files shall be processed automatically by the VIS to identify hits in accordance with this Article. The VIS shall examine each application file individually.

2. For the purpose of assessing whether the person could pose a threat to the public policy, internal security or public health of the Member States pursuant to point (e) of Article 6(1) of Regulation (EU) 2016/399 and for the purposes of the objective referred to in point (f) of Article 2(2) of this Regulation, the VIS shall launch a query by using the ESP to compare the relevant data referred to in points (d) to (g) and points (i), (j) and (k) of Article 22a(1) of this Regulation with the data present in a record, file or alert registered in:

- (a) the SIS;
- (b) the EES;
- (c) the ETIAS, including the ETIAS watchlist;
- (d) the VIS;

- (e) the ECRIS-TCN;
- (f) the Europol data;
- (g) Interpol SLTD, and
- (h) Interpol TDAWN.

The comparison shall be made with both alphanumeric and biometric data, unless the information system or database queried contains only one of those data categories.

3. In particular, the VIS shall verify:

- (a) as regards the SIS, whether:
  - (i) the travel document used for the application corresponds to a travel document which has been lost, stolen, misappropriated or invalidated;
  - (ii) the applicant is subject to an alert for refusal of entry and stay;
  - (iii) the applicant is subject to an alert on return;
  - (iv) the applicant is subject to an alert on persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant, or wanted for arrest for extradition purposes;
  - (v) the applicant is subject to an alert on missing persons or vulnerable persons who need to be prevented from travelling;
  - (vi) the applicant is subject to an alert on persons sought to assist with a judicial procedure;
  - (vii) the applicant or the travel document is subject to an alert on persons or objects for discreet checks, inquiry checks or specific checks;
- (b) as regards the EES, whether the applicant is recorded as having been refused entry in the EES on the basis of a reason corresponding to point (B), (D), (H) or (I) of Part B of Annex V to Regulation (EU) 2016/399;
- (c) as regards the ETIAS, whether:
  - (i) the applicant is a person for whom refused, annulled or revoked travel authorisation is recorded in the ETIAS on the basis of a reason corresponding to point (a), (b), (d) or (e) of Article 37(1) or to Article 37(2) of Regulation (EU) 2018/1240, or the applicant's travel document corresponds to such refused, annulled or revoked travel authorisation;
  - (ii) the data provided as part of the application correspond to data present in the ETIAS watchlist;
- (d) as regards the VIS, whether the applicant corresponds to a person:
  - (i) for whom a refused, annulled or revoked visa is recorded in the VIS on the basis of a reason corresponding to point (a)(i), (v) or (vi) or point (b) of Article 12(2);
  - (ii) for whom a refused, withdrawn, revoked or annulled long-stay visa or residence permit is recorded in the VIS on the basis of a reason corresponding to point (a) of Article 22d(1); or
  - (iii) whose travel document corresponds to a refused, withdrawn, revoked or annulled visa, long-stay visa or residence permit referred to in point (i) or (ii);
- (e) as regards the ECRIS-TCN, whether the applicant corresponds to a person whose data have been recorded in that system during the previous 25 years as far as convictions for terrorist offences are concerned or during the previous 15 years as far as convictions for other serious criminal offences are concerned;
- (f) as regards Europol data, whether the data provided in the application correspond to data recorded in Europol data;
- (g) as regards Interpol databases, whether:
  - (i) the travel document used for the application corresponds to a travel document reported lost, stolen or invalidated in Interpol SLTD;
  - (ii) the travel document used for the application corresponds to a travel document recorded in a file in Interpol TDAWN.

4. SIS alerts in respect of missing persons or vulnerable persons, persons sought to assist with a judicial procedure and persons or objects for discreet checks, inquiry checks or specific checks shall be queried only for the purposes of the objective referred to in point (f) of Article 2(2).

5. As regards Interpol SLTD and Interpol TDawn, any queries or verification shall be performed in such a way that no information shall be revealed to the owner of the Interpol alert.

If the requirement provided for in this paragraph is not fulfilled, the VIS shall not query Interpol databases.

6. As regards Europol data, the automated processing shall receive the appropriate notification in accordance with Article 21(1b) of Regulation (EU) 2016/794.

7. A hit shall be triggered where all or some of the data from the application file used for the query correspond fully or partially to the data present in a record, alert or file of the information systems or databases referred to in paragraph 2. The manual referred to in paragraph 18 shall define partial correspondence, including a degree of probability to limit the number of false hits.

8. Where the automatic comparison referred to in paragraph 2 reports a hit related to point (a)(i), (ii) and (iii), point (b), point (c)(i), point (d) and point (g)(i) of paragraph 3, the VIS shall add a reference in the application file to any hit and, where relevant, the Member States that entered or supplied the data having triggered the hit.

9. Where the automatic comparison referred to in paragraph 2 reports a hit related to point (a)(iv), point (c)(ii), points (e) and (f) and point (g)(ii) of paragraph 3, the VIS shall only indicate in the application file that further verification is needed.

In the event of hits pursuant to point (a)(iv), points (e) and (f) and point (g)(ii) of paragraph 3, the VIS shall send an automated notification regarding such hits to the VIS designated authority of the Member State processing the application. Such automated notification shall contain the data recorded in the application file in accordance with points (d) to (g), and (i), (j) and (k) of Article 22a(1).

In the event of hits pursuant to point (c)(ii) of paragraph 3, the VIS shall send an automated notification regarding such hits to the ETIAS National Unit of the Member State that entered the data or, if the data was entered by Europol, to the ETIAS National Unit of the Member States processing the application. That automated notification shall contain the data recorded in the application file in accordance with points (d) to (g) and (i) of Article 22a(1).

10. Where the automatic comparison referred to in paragraph 2 reports a hit related to point (a)(v), (vi) and (vii) of paragraph 3, the VIS shall neither record the hit in the application file nor indicate in the application file that further verification is needed.

11. The unique reference number of the data record having triggered a hit shall be kept in the application file for the purpose of the keeping of logs, reporting and statistics in accordance with Articles 34 and 45a.

12. Any hit pursuant to paragraph 6 shall be manually verified by the competent visa or immigration authority of the Member State processing the application for a long-stay visa or residence permit.

For the purposes of manual verification under the first subparagraph of this paragraph, the competent authority shall have access to the application file and any linked application files, as well as to the hits triggered during the automated processing pursuant to paragraph 6.

The competent authority shall also have temporary access to data in the VIS, the SIS, the EES, the ETIAS, or Interpol SLTD that triggered the hit for the duration of the verifications referred to in this Article and the examination of the application for a long-stay visa or residence permit and in the event of an appeal procedure.

The competent authority shall verify whether the identity of the applicant recorded in the application file corresponds to the data in any of the information systems and databases queried.

Where the personal data in the application file correspond to the data stored in the relevant information system or database, the hit shall be taken into account when assessing whether the applicant for a long-stay visa or a residence permit could pose a threat to the public policy, internal security or public health of the Member States processing the application.

Where the hit concerns a person in respect of whom an alert for refusal of entry and stay or an alert on return has been entered into the SIS by another Member State, the prior consultation pursuant to Article 27 of Regulation (EU) 2018/1861 or Article 9 of Regulation (EU) 2018/1860 shall apply.

Where the personal data in the application file do not correspond to the data stored in the relevant information system or database, the competent authority shall erase the false hit from the application file.

13. For the manual verification of hits pursuant to points (a)(iv) to (vii), points (e) and (f) and point (g)(ii) of paragraph 3 of this Article by VIS designated authorities, Article 9d shall apply accordingly.

14. For the manual verification and follow-up action with regard to hits in the ETIAS watchlist pursuant to point (c)(ii) of paragraph 3 of this Article by ETIAS National Units, Article 9e shall apply accordingly. The reference to the central visa authority shall be understood as referring to the visa or immigration authority competent for long-stay visas or residence permits.

15. For follow-up action with regard to hits in the SIS pursuant to point (a)(iv) to (vii) of paragraph 3 of this Article by the SIRENE Bureaux, Article 9f shall apply accordingly.

16. For follow-up action with regard to hits pursuant to point (e) or (f) or point (g)(ii) of paragraph 3 of this Article by the VIS designated authorities, Article 9g shall apply accordingly. The reference to the central visa authority shall be understood as referring to the visa or immigration authority competent for long-stay visas or residence permits.

17. For the purpose of implementing this Article, eu-LISA shall, in cooperation with the Member States and Europol, establish appropriate channels for the notifications and exchange of information referred to in this Article.

18. The Commission shall adopt a delegated act in accordance with Article 48a to lay down in a manual the procedures and rules necessary for queries, verifications and assessments.

#### *Article 22c*

#### **Data to be added for a long-stay visa or residence permit issued**

Where a competent authority decides to issue a long-stay visa or residence permit, it shall add the following data to the application file where the data is collected in accordance with the relevant Union and national law:

- (a) status information indicating that a long-stay visa or residence permit has been issued;
- (b) the authority that took the decision;
- (c) place and date of the decision to issue the long-stay visa or residence permit;
- (d) the type of document issued (long-stay visa or residence permit);
- (e) the number of the issued long-stay visa or residence permit;
- (f) the commencement and the expiry dates of the validity of the long-stay visa or residence permit;
- (g) data listed in Article 22a(1), if available and not entered in the application file upon application for a long-stay visa or residence permit.

#### *Article 22d*

#### **Data to be added in certain cases of a long-stay visa or residence permit refused**

1. Where a competent authority decides 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 public health or the applicant has presented documents which were fraudulently acquired, or falsified, or tampered with, it shall add the following data to the application file where the data is collected in accordance with the relevant Union and national law:

- (a) status 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, internal security or public health, or because the applicant presented documents which were fraudulently acquired, or falsified, or tampered with;



- (b) the authority that took the decision;
- (c) place and date of the decision.

2. Where a final decision to refuse a long-stay visa or a residence permit has been taken on the basis of reasons other than those referred to in paragraph 1, the application file shall be deleted without delay from the VIS.

#### *Article 22e*

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

Where a competent authority decides to withdraw, revoke or annul a long-stay visa or residence permit, it shall add the following data to the application file where the data is collected in accordance with the relevant Union and national law:

- (a) status information indicating that the long-stay visa or residence permit has been withdrawn, revoked or annulled;
- (b) the authority that took the decision;
- (c) place and date of the decision;
- (d) where applicable, the grounds for withdrawal, revocation or annulment of the long-stay visa or residence permit, in accordance with Article 22d.

#### *Article 22f*

##### **Data to be added for a long-stay visa extended or residence permit renewed**

1. Where a competent authority decides to extend a long-stay visa, it shall add the following data to the application file, where the data is collected in accordance with the relevant Union and national law:

- (a) status information indicating that the long-stay visa has been extended;
- (b) the authority that took the decision;
- (c) place and date of the decision;
- (d) the number of the visa sticker;
- (e) the commencement and the expiry dates of the validity of the long-stay visa.

2. Where a competent authority decides to renew a residence permit, Article 22c applies.

#### *Article 22g*

##### **Access to VIS 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 holder of the long-stay visa or residence permit, or the authenticity and the validity of the long-stay visa or residence permit 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, the competent authorities for carrying out checks at external border crossing points in accordance with that Regulation shall have access to search the VIS 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 long-stay visa or residence permit.

2. If the search with the data listed in paragraph 1 of this Article indicates that data on the holder of the long-stay visa or residence permit are recorded in the VIS, the competent border control authority shall have access to the VIS to consult the following data of the application file and of linked application files pursuant to Article 22a(4), solely for the purposes referred to in paragraph 1 of this Article:

- (a) the status information of the long-stay visa or residence permit indicating if it has been issued, withdrawn, revoked, annulled, extended or renewed;
- (b) the data referred to in points (d), (e), and (f) of Article 22c;

- (c) where applicable, the data referred to in points (d) and (e) of Article 22f(1);
- (d) facial images as referred to in point (j) of Article 22a(1).

3. For the purposes referred to in paragraph 1, the competent authorities for carrying out checks at external border crossing points shall also have access to the VIS to verify the fingerprints or the facial image of the holder of the long-stay visa or residence permit against the fingerprints or the facial image taken live recorded in the VIS.

4. Where verification of the holder of the long-stay visa or residence permit fails or where there are doubts as to the identity of the holder or the authenticity of the long-stay visa or residence permit or the travel document, the duly authorised staff of the competent authorities for carrying out checks at external border crossing points shall have access to VIS data in accordance with Article 22i(1) and (2).

#### Article 22h

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

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

Where the identity of the holder of the long-stay visa or residence permit cannot be verified with fingerprints, the competent authorities may also carry out the verification with the facial image.

2. If the search with the data listed in paragraph 1 of this Article indicates that data on the holder of the long-stay visa or residence permit are recorded in the VIS, the competent authority shall have access to the VIS to consult the following data of the application file and of linked application files pursuant to Article 22a(4), solely for the purposes referred to in paragraph 1 of this Article:

- (a) the status information of the long-stay visa or residence permit indicating if it has been issued, withdrawn, revoked, annulled, extended or renewed;
- (b) the data referred to in points (d), (e) and (f) of Article 22c;
- (c) where applicable, the data referred to in points (d) and (e) of Article 22f(1);
- (d) facial images as referred to in point (j) of Article 22a(1).

3. Where verification of the holder of the long-stay visa or residence permit fails or where there are doubts as to the identity of the holder or the authenticity of the long-stay visa or residence permit or the travel document, the duly authorised staff of the competent authorities shall have access to VIS data in accordance with Article 22i(1) and (2).

#### Article 22i

##### Access to VIS data for identification

1. For the sole purpose of the identification of any person who may have been registered previously in the VIS or who does not or no longer fulfils the conditions for the entry to, stay or residence on the territory of the Member States, the authorities competent for carrying out checks at external border crossing points in accordance with Regulation (EU) 2016/399 or within the territory of the Member States as to whether the conditions for entry to, stay or residence on the territory of the Member States are fulfilled, shall have access to the VIS to search with the fingerprints of that person.

Where the fingerprints of that person cannot be used or the search with the fingerprints fails, the search shall be carried out with the data referred to in points (d) to (g) or point (j) of Article 22a(1). However, the facial image shall not be the only search criterion.

2. If the search with the data listed in paragraph 1 of this Article indicates that data on the applicant are recorded in the VIS, the competent authority shall have access to the VIS to consult the following data of the application file and of linked application files pursuant to Article 22a(4), solely for the purposes referred to in paragraph 1 of this Article:

- (a) the application number, the status information and the authority with which the application was lodged;
- (b) the data referred to in points (d) to (g) and (i) of Article 22a(1);
- (c) facial images as referred to in point (j) of Article 22a(1);
- (d) the data entered in respect of any long-stay visa or residence permit issued, refused, withdrawn, revoked, annulled, extended or renewed referred to in Articles 22c to 22f.

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

#### *Article 22j*

#### **Access to VIS 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 Articles 12 and 34 of Regulation (EU) No 604/2013, the competent asylum authorities shall have access to the VIS to search with the fingerprints of the applicant for international protection.

Where the fingerprints of the applicant for international protection cannot be used or the search with the fingerprints fails, the search shall be carried out with the data referred to in points (d) to (g) or point (j) of Article 22a(1). However, the facial image shall not be the only search criterion.

2. If the search with the data listed in paragraph 1 of this Article indicates that a long-stay visa or residence permit is recorded in the VIS, the competent asylum authority shall have access to the VIS to consult the following data of the application file and, as regards the data listed in point (e) of this paragraph, of linked application files relating to the spouse and children pursuant to Article 22a(4), solely for the purpose referred to in paragraph 1 of this Article:

- (a) the application number and the authority that issued, revoked, annulled, extended or renewed the long-stay visa or residence permit;
- (b) the data referred to in points (d) to (g) and (i) of Article 22a(1);
- (c) the data entered in respect of any long-stay visa or residence permit issued, withdrawn, revoked, annulled, extended or renewed referred to in Articles 22c, 22e and 22f;
- (d) facial images as referred to in point (j) of Article 22a(1);
- (e) the data referred to in points (d) to (g) of Article 22a(1) of the linked application files relating to 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 34(6) of Regulation (EU) No 604/2013.

#### *Article 22k*

#### **Access to VIS 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 to the VIS in accordance with Article 34 of Regulation (EU) No 604/2013 to search with the fingerprints of the applicant for international protection.

Where the fingerprints of the applicant for international protection cannot be used or the search with the fingerprints fails, the search shall be carried out with the data referred to in points (d) to (g) or point (j) of Article 22a(1). However, the facial image shall not be the only search criterion.

2. If the search with the data listed in paragraph 1 of this Article indicates that data on the applicant for international protection is recorded in the VIS, the competent asylum authority shall have access to the VIS to consult the following data of the application file and, as regards the data listed in point (f) of this paragraph, of the linked application files relating to the spouse and children pursuant to Article 22a(4), solely for the purpose referred to in paragraph 1 of this Article:

- (a) the application number;
- (b) the data referred to in points (d) to (g) and (i) of Article 22a(1);
- (c) facial images as referred to in point (j) of Article 22a(1);
- (d) scans of the biographic data page of the travel document as referred to in point (h) of Article 22a(1);
- (e) the data entered in respect of any long-stay visa or residence permit issued, withdrawn, revoked, annulled, extended or renewed referred to in Articles 22c, 22e and 22f;
- (f) the data referred to in points (d) to (g) of Article 22a(1) of the linked application files relating to 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 34(6) of Regulation (EU) No 604/2013.

#### CHAPTER IIIB

### PROCEDURE AND CONDITIONS FOR ACCESS TO THE VIS FOR LAW ENFORCEMENT PURPOSES

#### Article 22l

##### ***Member States' designated authorities***

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

The data accessed by those authorities shall only be processed for the purposes of the specific case for which the data have been consulted.

2. Each Member State shall keep a list of its designated authorities and shall communicate that list to the Commission and eu-LISA. Each Member State may at any time amend or replace the list which it communicated and shall inform the Commission and eu-LISA accordingly.

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 for access to VIS data laid down in Article 22o 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 from the designated authorities and shall not receive instructions from them 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 communicate to the Commission and eu-LISA its central access point and may at any time amend or replace its communication.

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 VIS data through the central access point.

6. Only duly empowered staff of the central access point shall be authorised to access VIS data in accordance with Articles 22n and 22o.

*Article 22m***Europol**

1. Europol shall designate one of its operating units as 'Europol designated authority' and shall authorise it to request access to VIS data 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.

The data accessed by Europol shall only be processed for the purposes of the specific case for which the data have been consulted.

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 for access to VIS data laid down in Article 22r 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 as regards the outcome of the verification.

*Article 22n***Procedure for access to VIS data for law enforcement purposes**

1. The operating units referred to in Article 22l(5) shall submit a reasoned electronic or written request to the central access points referred to in paragraph 3 of that Article for access to VIS data. Upon receipt of a request for access the central access point shall verify whether the conditions referred to in Article 22o are fulfilled. If the conditions are fulfilled, the central access point shall process the request. The VIS data accessed shall be transmitted to the operating units referred to in Article 22l(5) in such a way as not to 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 other serious criminal offence, the central access point shall process the request immediately and shall only verify *ex post* whether all the conditions of Article 22o 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 seven working days after the processing of the request.

3. Where an *ex post* verification reveals that the access to VIS data was not justified, all the authorities that accessed such data shall without delay erase the data accessed from the VIS and shall inform the central access point of the erasure.

*Article 22o***Conditions for access to VIS data by designated authorities of Member States**

1. Without prejudice to Article 22 of Regulation (EU) 2019/817 designated authorities shall have access to the VIS for the purposes of consultation where all of the following conditions are met:

- (a) consultation is necessary and proportionate for the purposes of the prevention, detection or investigation of a terrorist offence or other serious criminal offence;
- (b) consultation is necessary and proportionate in a specific case;
- (c) reasonable grounds exist to consider that consultation of 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) a query of the CIR was launched in accordance with Article 22 of Regulation (EU) 2019/817 and the reply received as referred to in paragraph 2 of that Article indicates that data is stored in the VIS.

2. The fulfilment of the condition provided for in point (d) of paragraph 1 shall not be required where 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, or the data category with which the search is conducted is not stored in the CIR.

3. Consultation of the VIS shall be limited to searching with any of the following data in the application file:

- (a) surname(s) (family name(s)), first name(s) (given name(s)), date of birth, nationality or nationalities and/or sex;
- (b) type and number of travel document or documents, the country which issued the travel document and date of expiry of the validity of the travel document;
- (c) visa sticker number or number of the long-stay visa or residence permit and the date of expiry of the validity of the visa, long-stay visa or residence permit, as applicable;
- (d) fingerprints, including latent fingerprints;
- (e) facial image.

4. The facial image referred to in point (e) of paragraph 3 shall not be the only search criterion.

5. Consultation of the VIS shall, in the event of a hit, give access to the data listed in paragraph 3 of this Article as well as to any other data taken from the application file, including data entered in respect of any document issued, refused, annulled, revoked, withdrawn, renewed or extended. Access to the data referred to in point (4)(l) 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.

6. By way of derogation from paragraphs 3 and 5 the data referred to in points (d) and (e) of paragraph 3 of children below the age of 14 shall only be used to search the VIS and, in the case of a hit, shall only be accessed where:

- (a) necessary for the purposes of the prevention, detection or investigation of a serious criminal offence of which those children are the victim of and to protect missing children;
- (b) necessary in a specific case; and
- (c) the use of the data is in the best interest of the child.

#### *Article 22p*

#### **Access to VIS data for identification of persons in specific circumstances**

1. By way of derogation from Article 22o(1), designated authorities shall not be required to fulfil the conditions laid down in that paragraph to access the VIS for the purposes of the identification of persons who have gone missing, were abducted or were identified as victims of trafficking in human beings, and in respect of whom there are reasonable grounds to consider that consultation of VIS data will support their identification 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.

2. Where the fingerprints of the persons referred to in paragraph 1 cannot be used or the search with the fingerprints fails, the search shall be carried out with the data referred to in point (4)(a) to (ca) of Article 9 or points (d) to (g) of Article 22a(1).

3. Consultation of the VIS shall, in the event of a hit, give access to any of the data in Article 9 and Article 22a, as well as to the data in linked application files in accordance with Article 8(3) and (4) or Article 22a(4).

#### *Article 22q*

#### **Use of VIS data for the purpose of entering in the SIS alerts on missing persons or vulnerable persons who need to be prevented from travelling and access to those data**

1. VIS data may be used for the purpose of entering in the SIS an alert on missing persons or vulnerable persons who need to be prevented from travelling in accordance with Article 32 of Regulation (EU) 2018/1862. In those cases, the central access point referred to in Article 22l(3) shall ensure the transmission of data through secured means.

2. In the case of a hit against a SIS alert through the use of VIS data as referred to in paragraph 1, child protection authorities and national judicial authorities may request an authority with access to the VIS to grant them access to those data for the purposes of their tasks. Such national judicial authorities shall include those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to charging a person, and their coordinating authorities, as referred to in Article 44(3) of Regulation (EU) 2018/1862. The conditions provided for in Union and national law shall apply. Member States shall ensure that the data are transmitted in a secure manner.

#### *Article 22r*

#### **Procedure and conditions for access to VIS data by Europol**

1. Europol shall have access to the VIS for the purposes of consultation where all of the following conditions are met:

- (a) consultation is necessary and proportionate for the purpose of supporting and strengthening action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences falling under Europol's mandate;
- (b) consultation is necessary and proportionate in a specific case;
- (c) reasonable grounds exist to consider that consultation of 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) a query of the CIR was launched in accordance with Article 22 of Regulation (EU) 2019/817 and the reply received as referred to in paragraph 2 of that Article indicates that data is stored in the VIS.

2. Fulfilment of the condition provided for in point (d) of paragraph 1 shall not be required where 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, or the data category with which the search is conducted is not stored in the CIR.

3. Consultation of the VIS shall be limited to searching with any of the following data in the application file:

- (a) surname(s) (family name(s)), first name(s) (given name(s)), date of birth, nationality or nationalities and/or sex;
- (b) type and number of travel document or documents, the country which issued the travel document and date of expiry of the validity of the travel document;
- (c) visa sticker number or number of the long-stay visa or residence permit and the date of expiry of the validity of the visa, long-stay visa or residence permit, as applicable;
- (d) fingerprints, including latent fingerprints;
- (e) facial image.

4. The facial image referred to in point (e) of paragraph 3 shall not be the only search criterion.

5. Consultation of the VIS shall, in the event of a hit, give access to the data listed in paragraph 3 of this Article as well as to any other data taken from the application file, including data entered in respect of any document issued, refused, annulled, revoked, withdrawn, renewed or extended. Access to the data referred to in point (4)(l) 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.

6. By way of derogation from paragraphs 3 and 5 the data referred to in points (d) and (e) of paragraph 3 of children below the age of 14 shall only be used to search the VIS and, in the case of a hit, shall only be accessed where:

- (a) necessary for the purposes of the prevention, detection or investigation of a serious criminal offence of which those children are the victim of and to protect missing children;
- (b) necessary in a specific case; and
- (c) the use of the data is in the best interest of the child.

7. Europol's designated authority may submit a reasoned electronic request for the consultation of all VIS data or a specific set of VIS data to the Europol central access point. Upon receipt of a request for access the Europol central access point shall verify whether the conditions referred to in paragraphs 1 and 2 are fulfilled. If all conditions are fulfilled, the duly authorised staff of the central access point shall process the request. The VIS data accessed shall be transmitted to the Europol designated authority in such a way as not to compromise the security of the data.

8. The processing of data obtained by Europol by consulting VIS data shall be subject to the authorisation of the Member State of origin of the data. That authorisation shall be obtained via the Europol national unit of that Member State.

#### Article 22s

#### **Keeping of logs of requests to consult VIS data for the purposes of the prevention, detection and investigation of terrorist offences or other serious criminal offences**

1. eu-LISA shall keep logs of all data processing operations within the VIS involving access by the central access points referred to in Article 22l(3) for the purposes of Chapter IIIb. Those logs shall show the date and time of each operation, the data used for launching the search, the data transmitted by the VIS and the name of the authorised staff of the central access points entering and retrieving the data.

2. In addition, each Member State and Europol shall keep logs of all data processing operations within the VIS resulting from requests to consult VIS data or from access to VIS data for the purposes of Chapter IIIb.

3. The logs referred to in paragraph 2 shall show:

- (a) the exact purpose of the request for consultation of or access to VIS data, including the terrorist offence or other serious criminal offence concerned and, for Europol, the exact purpose of the request for consultation;
- (b) the decision taken with regard to the admissibility of the request;
- (c) the national file reference;
- (d) the date and exact time of the request for access made by the central access point to the VIS;
- (e) where applicable, the use of the urgency procedure referred to in Article 22n(2) and the outcome of the *ex post* verification;
- (f) which of the data or set of data referred to in Article 22o(3) have been used for consultation; and
- (g) in accordance with national rules or with Regulation (EU) 2016/794, the identifying mark of the official who carried out the search and of the official who ordered the search or transmission of data.

4. The logs referred to in paragraphs 1 and 2 of this Article shall be used only to check the admissibility of the request, monitor the lawfulness of data processing and to ensure data integrity and security. The logs shall be protected by appropriate measures against unauthorised access. They shall be deleted one year after the retention period referred to in Article 23 has expired, if they are not required for monitoring procedures which have already begun. The European Data Protection Supervisor and the competent supervisory authorities shall have access to the logs at their request for the purpose of fulfilling their duties. The authority responsible for checking the admissibility of the request shall also have access to the logs for that purpose. Other than for such purposes, personal data shall be erased in all national and Europol files after a period of one month, unless those data are required for the purposes of the specific ongoing criminal investigation for which they were requested by a Member State or by Europol. Only logs containing non-personal data may be used for the monitoring and evaluation referred to in Article 50.

#### Article 22t

#### **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 such access is:



- (a) within the scope of the powers of those designated authorities;
- (b) subject to the same conditions as referred to in Article 22o(1);
- (c) 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 to consult the VIS.

2. A Member State in respect of which this Regulation has not yet been put into effect shall make its data on visas 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 22o(1).”;

(27) Article 23 is replaced by the following:

“Article 23

### **Retention period for data storage**

1. Each application file shall be stored in the VIS for a maximum of five years, without prejudice to the erasure referred to in Articles 24 and 25 and to the keeping of the logs 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, a long-stay visa or a residence permit has been extended or renewed;
- (c) on the date of the creation of the application file in the VIS, if the application has been withdrawn and closed;
- (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, withdrawn, revoked or annulled, as applicable.

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

3. By way of derogation from paragraph 1, fingerprints and facial images pertaining to children below the age of 12 shall be erased upon the visa, long-stay visa or residence permit having expired and, in the event of a visa, the child having exited the external borders.

For the purposes of that erasure, the EES shall automatically notify the VIS when the exit of the child is entered in the entry/exit record in accordance with Article 16(3) of Regulation (EU) 2017/2226.”;

(28) Article 24 is replaced by the following:

“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 rectifying or erasing 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. That message shall be transmitted by VISMail in accordance with the procedure in Article 16(3).

Where the inaccurate data refers to links created pursuant to Article 8(3) or (4) or Article 22a(4) or where a link is missing, the Member State responsible shall check the data concerned and provide an answer within three working days, and shall rectify the link if necessary. If no answer is provided within that timeframe, the requesting Member State shall rectify the link and notify, by VISMail, the Member State responsible of the rectification made.

3. The Member State responsible shall, as soon as possible, check the data concerned and, if necessary, rectify or erase them immediately.”;

(29) Article 25 is amended as follows:

(a) the title is replaced by the following:

“Advance erasure of data”;

(b) paragraphs 1 and 2 are replaced by the following:

“1. Where, before expiry of the period referred to in Article 23(1), an applicant has acquired the nationality of a Member State, the application files and the links created pursuant to Article 8(3) and (4) or Article 22a(4) relating to the applicant shall be erased without delay from the VIS by the Member State which created the respective application files and links.

2. Each Member State shall inform the Member States responsible without delay if an applicant has acquired its nationality. That message shall be transmitted by the VISMail in accordance with the procedure in Article 16(3).”;

(30) Article 26 is replaced by the following:

“Article 26

### **Operational management**

1. eu-LISA shall be responsible for the technical and operational management of the VIS and its components as set out in Article 2a. It 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 those components.

2. eu-LISA shall be responsible for the following tasks relating to the communication infrastructure between the VIS Central System and the NUIs:

(a) supervision;

(b) security;

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

(d) tasks relating to implementation of the budget;

(e) acquisition and renewal;

(f) contractual matters.

3. 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. It shall include, in particular, the maintenance work and technical developments necessary to ensure that the VIS functions at a satisfactory level of operational quality, in particular as regards the response time for consultation of the VIS by visa authorities, the authorities competent to decide on an application for a long-stay visa or residence permit and border authorities. Such response times shall be as short as possible.

8a. eu-LISA may use anonymised real personal data in the VIS for testing purposes in the following circumstances:

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

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

In the cases referred to in point (b) of the first subparagraph, the security measures, access control and logging activities at the testing environment shall be equal to those for the VIS. 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 Council Regulation (EEC, Euratom, ECSC) No 259/68 \*, eu-LISA 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.

10. Where eu-LISA cooperates with external contractors in any VIS-related tasks, it shall closely monitor the activities of the contractor to ensure compliance with this Regulation, in particular on security, confidentiality and data protection.

\* OJ L 56, 4.3.1968, p. 1.”;

- (31) Article 27 is deleted;
- (32) the following article is inserted:

*“Article 27a*

#### **Interoperability with other EU information systems and Europol data**

Interoperability between the VIS and the SIS, the EES, the ETIAS, Eurodac, the ECRIS-TCN and Europol data shall be established to enable the automated processing of the queries of other systems pursuant to Articles 9a to 9g and Article 22b. Interoperability shall rely on the ESP.”;

- (33) Article 28 is amended as follows:
- (a) paragraphs 1 and 2 are replaced by the following:
    - “1. The VIS shall be connected to the national system of each Member State via the NUI in the Member State concerned.
    - 2. Each Member State shall designate a national authority which shall provide the access of the competent authorities referred to in Article 6(1) and (2) to the VIS, and connect that national authority to the NUI.”;
  - (b) paragraph 4 is amended, as follows:
    - (i) point (a) is replaced by the following:
      - “(a) the development of the national system and its adaptation to the VIS.”;
    - (ii) point (d) is replaced by the following:
      - “(d) bearing the costs incurred by the national system and the costs of its connection to the NUI, including the investment and operational costs of the communication infrastructure between the NUI and the national system.”;
- (34) Article 29 is replaced by the following:

*“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. eu-LISA shall ensure that the VIS is operated in accordance with this Regulation and its implementing rules referred to in Article 45. In particular, eu-LISA shall:
- (a) take the necessary measures to ensure the security of the VIS Central System and the communication infrastructure between the VIS Central System and the NUIs, 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 eu-LISA in accordance with this Regulation.
- 2a. eu-LISA shall develop and maintain a mechanism and procedures for carrying out quality checks on the data in the VIS and shall provide regular reports to the Member States. eu-LISA shall provide a regular report to the European Parliament, the Council and the Commission covering the issues encountered.

The Commission shall adopt implementing acts to lay down and develop the mechanism and the procedures for carrying out quality checks and appropriate requirements for data quality compliance. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 49(2).

3. eu-LISA shall inform the European Parliament, the Council and the Commission of the measures which it takes pursuant to paragraph 2.

4. In relation to the processing of personal data in the VIS, each Member State shall designate the authority which is to be considered as controller in accordance with point (7) of Article 4 of Regulation (EU) 2016/679 and which shall have central responsibility for the processing of data by that Member State. Each Member State shall notify the Commission of the designation.

#### *Article 29a*

#### **Specific rules for entering data**

1. The data referred to in Article 6(4), Articles 9 to 14, Article 22a and Articles 22c to 22f shall be entered in the VIS only following a quality check performed by the responsible national authorities and shall be processed by the VIS following a quality check performed by the VIS in accordance with paragraph 2 of this Article.

2. Quality checks on the data referred to in Articles 9 to 14, Article 22a and Articles 22c to 22f shall be performed by the VIS in accordance with this paragraph.

The quality checks shall be initiated when creating or updating application files in the VIS. Where the quality checks fail to meet the established quality standards, the responsible authority or authorities shall be automatically notified by the VIS. The automated queries pursuant to Article 9a(3) and Article 22b(2) shall be triggered by the VIS only following a positive quality check.

Quality checks on facial images and fingerprints shall be performed when creating or updating application files in the VIS, to ascertain the fulfilment of minimum data quality standards allowing for biometric matching.

Quality checks on the data referred to Article 6(4) shall be performed when storing information about the national competent authorities in the VIS.

3. Quality standards shall be established for the storage of the data referred to in paragraphs 1 and 2 of this Article.

The Commission shall adopt implementing acts to lay down the specification of those quality standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 49(2).";

(35) Article 31 is replaced by the following:

#### *"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 with the exception of transfers to Interpol for the purpose of carrying out the queries referred to in point (g) of Article 9a(4) and in point (g) of Article 22b(3) of this Regulation. Transfers of personal data to Interpol are subject to the provisions of Chapter V of Regulation (EU) 2018/1725 and Chapter V of Regulation (EU) 2016/679.

2. By way of derogation from paragraph 1 of this Article, the data referred to in points (4)(a), (b), (ca), (k) and (m) and points (6) and (7) of Article 9 or in points (d) to (i) and (k) of Article 22a(1) of this Regulation may be accessed by the competent authorities and transferred or made available to a third country or to an international organisation listed in the Annex, provided that it is necessary in individual cases in order to prove the identity of third-country nationals for the purposes of return in accordance with Directive 2008/115/EC, or, as regards transfers to an international organisation listed in the Annex to this Regulation, for the purposes of resettlement in accordance with European or national resettlement schemes, and provided that one of the following conditions is satisfied:

- (a) the Commission has adopted a decision on the adequate level of protection of personal data in that third country or international organisation in accordance with Article 45(3) of Regulation (EU) 2016/679;
- (b) appropriate safeguards have been provided as referred to in Article 46 of Regulation (EU) 2016/679, such as through a readmission agreement which is in force between the Union or a Member State and the third country in question;
- (c) point (d) of Article 49(1) of Regulation (EU) 2016/679 applies.

Moreover, the data referred to in the first subparagraph shall be transferred only where all of the following conditions are satisfied:

- (a) the transfer of the data is carried out in accordance with the relevant provisions of Union law, in particular provisions on data protection, readmission agreements, and the national law of the Member State transferring the data;
- (b) the Member State which entered the data in the VIS has given its approval;
- (c) the third country or international organisation has agreed to process the data only for the purposes for which they were provided.

Subject to the first and second subparagraphs of this paragraph, where a return decision adopted pursuant to Directive 2008/115/EC has been issued in relation to a third-country national, the data referred to in the first subparagraph shall be transferred only where the enforcement of such a return decision is not suspended and provided that no appeal has been lodged which may lead to the suspension of its enforcement.

3. Transfers of personal data to third countries or to international organisations pursuant to paragraph 2 shall not prejudice the rights of applicants for and beneficiaries of international protection, in particular as regards non-refoulement.

4. Personal data obtained from the VIS by a Member State or by Europol 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.

5. By way of derogation from paragraph 4 of this Article, the data referred to in point (4)(a) to (ca) of Article 9 and in points (d) to (g) of Article 22a(1) may be transferred by the designated authority to a third country in individual cases, only where all of the following conditions are met:

- (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 a terrorist offence or other serious criminal offence;
- (c) the designated authority has access to such data in accordance with the procedure and the conditions set out in Articles 22n and 22o;
- (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;
- (f) the reciprocal provision of any information in visa information systems held by the requesting country to the Member States operating the VIS is ensured.

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 referred to in 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.”;

(36) Article 32 is amended, as follows:

(a) paragraph 2 is amended as follows:

(i) the following point is inserted:

“(ea) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment.”;

(ii) the following points are inserted:

“(ja) ensure that, in the event of an interruption, installed systems can be restored to normal operation;

(jb) ensure reliability by making sure that any faults in the functioning of the systems are properly reported and that the necessary technical measures are put in place to ensure that personal data can be restored in the event of corruption due to a malfunctioning of the systems.”;

(b) paragraph 3 is replaced by the following:

“3. eu-LISA shall take the necessary measures in order to achieve the objectives set out in paragraph 2 as regards the operation of the VIS, including the adoption of a security plan.”;

(37) the following Article is inserted:

*“Article 32a*

### **Security incidents**

1. Any event that has or may have an impact on the security of the VIS and may cause damage to or loss of VIS data shall be considered to be a security incident, in particular where unauthorised access to data may have occurred or where the availability, integrity and confidentiality of data has or may have been compromised.

2. Security incidents shall be managed so as to ensure a quick, effective and proper response.

3. Without prejudice to the notification and communication of a personal data breach pursuant to Article 33 of Regulation (EU) 2016/679, Article 30 of Directive (EU) 2016/680, or both, Member States shall notify the Commission, eu-LISA and the European Data Protection Supervisor of security incidents. In the event of a security incident in relation to the VIS Central System, eu-LISA shall notify the Commission and the European Data Protection Supervisor. Europol and the European Border and Coast Guard Agency shall notify the Commission and the European Data Protection Supervisor in the case of a VIS-related security incident.

4. Information regarding a security incident that has or may have an impact on the operation of the VIS or on the availability, integrity and confidentiality of the VIS data shall be provided to the Commission and, if affected, to Member States, to Europol and to the European Border and Coast Guard Agency. Such incidents shall also be reported in compliance with the incident management plan to be provided by eu-LISA.

5. Member States, the European Border and Coast Guard Agency, eu-LISA and Europol shall cooperate in the event of a security incident.

6. The Commission shall inform the European Parliament and the Council without delay of serious incidents and the measures taken to address them. This information shall be classified, where appropriate, as EU RESTRICTED/RESTREINT UE in accordance with applicable security rules.”;

(38) Articles 33 and 34 are replaced by the following:

*“Article 33*

### **Liability**

1. Without prejudice to the liability of and the right to compensation from the controller or processor under Regulation (EU) 2016/679, Directive (EU) 2016/680 and Regulation (EU) 2018/1725:

(a) any person or Member State that has suffered material or non-material damage as a result of an unlawful personal data processing operation or any other act incompatible with this Regulation by a Member State shall be entitled to receive compensation from that Member State;

(b) any person or Member State that has suffered material or non-material damage as a result of an act of a Union institution, body, office or agency incompatible with this Regulation shall be entitled to receive compensation from that Union institution, body, office or agency.

The Member State or Union institution, body, office or agency shall be exempt from its liability under the first subparagraph, in whole or in part, if it proves that it is not responsible for the event which gave rise to the damage.

2. If any failure of a Member State to comply with its obligations under this Regulation causes damage to the VIS, that Member State shall be held liable for such damage, unless and insofar as eu-LISA or another Member State participating in the VIS failed to take reasonable measures to prevent the damage from occurring or to minimise its impact.

3. Claims for compensation against a Member State for the damage referred to in paragraphs 1 and 2 shall be governed by the national law of that Member State. Claims for compensation against a Union institution, body, office or agency for the damage referred to in paragraphs 1 and 2 shall be subject to the conditions provided for in the Treaties.”;

#### *Article 34*

#### **Keeping of logs**

1. Each Member State, the European Border and Coast Guard Agency and eu-LISA shall keep logs of all their data processing operations within the VIS. Those logs shall show:

- (a) the purpose of access;
- (b) the date and time;
- (c) the type of data entered;
- (d) the type of data used for search; and
- (e) 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 data in or retrieve data from the VIS.

2. For the queries and consultations referred to in Articles 9a to 9g and 22b, a log for each data processing operation carried out within the VIS and, respectively, the EES, the ETIAS, the SIS, the ECRIS-TCN and Eurodac shall be kept in accordance with this Article and, respectively, Article 28a of Regulation (EU) No 603/2013, Article 46(2) of Regulation (EU) 2017/2226, Article 69 of Regulation (EU) 2018/1240, Article 18a of Regulation (EU) 2018/1861, Article 18a of Regulation (EU) 2018/1862 and Article 31a of Regulation (EU) 2019/816.

3. For the operations listed in Article 45c of this Regulation a log of each data processing operation carried out within the VIS and the EES shall be kept in accordance with that Article and Article 46 of Regulation (EU) 2017/2226. For the operations listed in Article 17a of this Regulation, a log of each data processing operation carried out in the VIS and the EES shall be kept in accordance with this Article and Article 46 of Regulation (EU) 2017/2226.

4. Logs kept pursuant to this Article shall 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 has expired, if they are not required for monitoring procedures which have already begun.”;

(39) Article 36 is replaced by the following:

“Article 36

#### **Penalties**

Without prejudice to Regulation (EU) 2016/679 and Directive (EU) 2016/680, Member States shall lay down the rules on penalties applicable to infringements of this Regulation, including for processing of personal data carried out in breach of this Regulation, and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.”;

(40) in Chapter VI, the following Article is inserted:

“Article 36a

#### **Data protection**

1. Regulation (EU) 2018/1725 shall apply to the processing of personal data by the European Border and Coast Guard Agency and eu-LISA under this Regulation.

2. Regulation (EU) 2016/679 shall apply to the processing of personal data by the visa, border, asylum and immigration authorities when performing tasks under this Regulation.

3. Directive (EU) 2016/680 shall apply to the processing of personal data stored in the VIS, including access to those data, for the purposes referred to in Chapter IIIb of this Regulation by Member States' designated authorities under that Chapter.

4. Regulation (EU) 2016/794 shall apply to the processing of personal data by Europol pursuant to this Regulation.”;

(41) Article 37 is amended as follows:

(a) paragraph 1 is amended as follows:

(i) the introductory sentence is replaced by the following:

“1. Without prejudice to the right to information referred to in Articles 15 and 16 of Regulation (EU) 2018/1725, Articles 13 and 14 of Regulation (EU) 2016/679 and Article 13 of Directive (EU) 2016/680, applicants and the persons referred to in point (4)(f) of Article 9 of this Regulation shall be informed of the following by the Member State responsible:”;

(ii) point (a) is replaced by the following:

“(a) the identity of the controller referred to in Article 29(4), including the controller's contact details;”;

(iii) point (c) is replaced by the following:

“(c) the categories of recipients of the data, including the authorities referred to in Article 22l and Europol;

(ca) the fact that the VIS may be accessed by the Member States and Europol for law enforcement purposes;”;

(iv) the following point is inserted:

“(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 of this Regulation and to Member States in accordance with Council Decision (EU) 2017/1908 \*;

\* 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 (OJ L 269, 19.10.2017, p. 39).”;

(v) point (f) is replaced by the following:

“(f) the existence of the right to request access to data relating to them, the right to request that inaccurate data relating to them be rectified, that incomplete personal data relating to them be completed, that unlawfully processed personal data concerning them be erased or that the processing thereof be restricted, as well as the right to receive information on the procedures for exercising those rights, including the contact details of the supervisory authorities, or of the European Data Protection Supervisor if applicable, which shall hear complaints concerning the protection of personal data;”;

(b) paragraph 2 is replaced by the following:

“2. The information referred to in paragraph 1 of this Article shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language in writing to the applicant when the data, the facial image and the fingerprint data as referred to in Article 9 and Article 22a are collected. Children shall be informed in an age-appropriate manner, including by using visual tools to explain the fingerprinting procedure.”;

(c) in paragraph 3, the second subparagraph is replaced by the following:

“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.”;



(42) Articles 38 to 43 are replaced by the following:

*“Article 38*

**Right of access to, rectification, completion, erasure of personal data and restriction of processing**

1. In order to exercise their rights under Articles 15 to 18 of Regulation (EU) 2016/679, any person shall have the right to obtain communication of the data relating to him or her recorded in the VIS and of the Member State which entered them in the VIS. The Member State that receives the request shall examine and reply to it as soon as possible, and at the latest within one month of receipt of the request.

2. Any person may request that data relating to him or her which are inaccurate be rectified and that data recorded unlawfully be erased.

Where the request is addressed to the Member State responsible and where it is found that VIS data are factually inaccurate or have been recorded unlawfully, the Member State responsible shall, in accordance with Article 24(3), rectify or erase those data in the VIS without delay and at the latest within one month of receipt of the request. The Member State responsible shall confirm in writing to the person concerned without delay that it has taken action to rectify or erase data relating to him or her.

Where the request is addressed to a Member State other than the Member State responsible, the authorities of the Member State to which the request was addressed shall contact the authorities of the Member State responsible within a period of seven days. The Member State responsible shall proceed in accordance with the second subparagraph of this paragraph. The Member State which contacted the authority of the Member State responsible shall inform the person concerned that his or her request was forwarded, to which Member State and about the further procedure.

3. Where the Member State responsible does not agree with the claim that data recorded in the VIS are factually inaccurate or have been recorded unlawfully, it shall without delay adopt an administrative decision explaining in writing to the person concerned why it does not intend to rectify or erase data relating to him or her.

4. The administrative decision referred to in paragraph 3 shall also provide the person concerned with information explaining the possibility to challenge that decision and, where relevant, information on how to bring an action or a complaint before the competent authorities or courts and information on any assistance available to the person, including from the competent supervisory authorities.

5. Any request made pursuant to paragraph 1 or 2 shall contain the necessary information to identify the person concerned. That information shall be used exclusively to enable the exercise of the rights referred to in paragraph 1 or 2.

6. The Member State responsible shall keep a record in the form of a written document that a request as referred to in paragraph 1 or 2 was made and how it was addressed. It shall make that document available to the competent supervisory authorities without delay and not later than seven days following the decision to rectify or erase the data referred to in the second subparagraph of paragraph 2 or following the administrative decision referred to in paragraph 3.

7. By way of derogation from paragraphs 1 to 6 of this Article, and only as regards data contained in the reasoned opinions that are recorded in the VIS in accordance with Article 9e(6), Article 9g(6) and Article 22b(14) and (16) as a result of the queries pursuant to Articles 9a and 22b, a Member State shall take a decision not to provide information to the person concerned, in whole or in part, in accordance with national or Union 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 person 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 the cases referred to in the first subparagraph, the Member State shall inform the person concerned 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 person concerned 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 person concerned is based. That information shall be made available to the supervisory authorities.

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

#### *Article 39*

### **Cooperation to ensure the rights on data protection**

1. The competent authorities of the Member States shall cooperate actively to enforce the rights laid down in Article 38.
2. In each Member State, the supervisory authority referred to in Article 51(1) of Regulation (EU) 2016/679 shall, upon request, assist and advise the data subject in exercising his or her right to rectification, completion or erasure of personal data relating to him or her or to restriction of the processing of such data, in accordance with Regulation (EU) 2016/679.

In order to achieve the aims referred to in the first subparagraph, the supervisory authority of the Member State responsible and the supervisory authority of the Member State to which the request has been made shall cooperate with each other.

#### *Article 40*

### **Remedies**

1. Without prejudice to Articles 77 and 79 of Regulation (EU) 2016/679, any person shall have the right to bring an action or a complaint before the competent authorities or courts of the Member State which refused the right of access to, rectification, completion or erasure of data relating to him or her provided for in Article 38 and Article 39(2) of this Regulation. The right to bring such an action or complaint shall also apply where requests for access to, rectification, completion or erasure were not responded to within the deadlines provided for in Article 38 or were never dealt with by the data controller.
2. The assistance of the supervisory authority referred to in Article 51(1) of Regulation (EU) 2016/679 shall remain available throughout the proceedings.

#### *Article 41*

### **Supervision by the supervisory authorities**

1. Each Member State shall ensure that the supervisory authority referred to in Article 51(1) of Regulation (EU) 2016/679 independently monitors the lawfulness of the processing of personal data pursuant to this Regulation by the Member State concerned.
2. The supervisory authority referred to in Article 41(1) of Directive (EU) 2016/680 shall monitor the lawfulness of the processing of personal data by the Member States in accordance with Chapter IIIB, including the access to personal data by the Member States and their transmission to and from the VIS.
3. The supervisory authority referred to in Article 51(1) of Regulation (EU) 2016/679 shall ensure that an audit of the data processing operations by the responsible national authorities is carried out in accordance with relevant international auditing standards at least every four years. The results of the audit may be taken into account in the evaluations conducted under the mechanism established by Council Regulation (EU) No 1053/2013 \*. The supervisory authority referred to in Article 51(1) of Regulation (EU) 2016/679 shall publish annually the number of requests for rectification, completion or erasure, or restriction of processing of data, the action subsequently taken and the number of rectifications, completions, erasures and restrictions of processing made in response to requests by the persons concerned.

4. Member States shall ensure that their supervisory authorities have sufficient resources to fulfil the tasks entrusted to them under this Regulation and have access to advice from persons with sufficient knowledge of biometric data.

5. Member States shall supply any information requested by the supervisory authorities and shall, in particular, provide them with information on the activities carried out in accordance with their responsibilities under this Regulation. Member States shall grant the supervisory authorities access to their logs and allow them access at all times to all their VIS-related premises.

#### Article 42

### **Supervision by the European Data Protection Supervisor**

1. The European Data Protection Supervisor shall be responsible for monitoring the personal data processing activities of eu-LISA, Europol and the European Border and Coast Guard Agency under this Regulation and for ensuring that such activities are carried out in accordance with this Regulation and Regulation (EU) 2018/1725 or, as regards Europol, with Regulation (EU) 2016/794.

2. The European Data Protection Supervisor shall ensure that an audit of eu-LISA's personal data processing activities is carried out in accordance with relevant international auditing standards at least every four years. A report of that audit shall be sent to the European Parliament, the Council, eu-LISA, the Commission and the supervisory authorities. eu-LISA shall be given an opportunity to make comments before the reports are adopted.

3. eu-LISA shall supply information requested by the European Data Protection Supervisor, give the European Data Protection Supervisor access to all documents and to its logs as referred to in Articles 22s, 34 and 45c and allow the European Data Protection Supervisor access to all its premises at any time.

#### Article 43

### **Cooperation between supervisory authorities and the European Data Protection Supervisor**

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

2. The European Data Protection Supervisor and the supervisory authorities shall exchange relevant information, assist each other in carrying out audits and inspections, examine any difficulties concerning the interpretation or application of this Regulation, assess problems in the exercise of independent supervision or in the exercise of the rights of the data subject, draw up harmonised proposals for joint solutions to any problems and promote awareness of data protection rights, as necessary.

3. For the purposes of paragraph 2, the supervisory authorities and the European Data Protection Supervisor shall meet at least twice a year within the framework of the European Data Protection Board. The European Data Protection Board shall organise and bear the costs of those meetings. 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 undertaken pursuant to this Article shall be sent by the European Data Protection Board to the European Parliament, to the Council, to the Commission, to Europol, to the European Border and Coast Guard Agency and to eu-LISA every two years. That report shall include a chapter on each Member State prepared by the supervisory authority of that Member State.

\* Council Regulation (EU) No 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen acquis and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen (OJ L 295, 6.11.2013, p. 27).";

(43) Article 44 is deleted;

(44) Article 45 is replaced by the following:

*“Article 45*

#### **Implementation by the Commission**

1. The Commission shall adopt implementing acts to lay down the measures necessary for the development of the VIS Central System, the NUIs in each Member State and the communication infrastructure between the VIS Central System and the NUIs concerning the following:

- (a) the design of the physical architecture of the VIS Central System including its communication network;
- (b) technical aspects which have a bearing on the protection of personal data;
- (c) technical aspects which have serious financial implications for the budgets of the Member States or which have serious technical implications for the national systems;
- (d) the development of security requirements, including biometric aspects.

2. The Commission shall adopt implementing acts to lay down measures necessary for the technical implementation of the functionalities of the VIS Central System, in particular:

- (a) for entering the data and linking applications in accordance with Article 8, Articles 10 to 14, Article 22a and Articles 22c to 22f;
- (b) for accessing the data in accordance with Article 15, Articles 18 to 22, Articles 22g to 22k, Articles 22n to 22r and Articles 45e and 45f;
- (c) for rectification, erasure and advance erasure of data in accordance with Articles 23, 24 and 25;
- (d) for keeping and accessing the logs in accordance with Article 34;
- (e) for the consultation mechanism and the procedures referred to in Article 16;
- (f) for accessing the data for the purposes of reporting and statistics in accordance with Article 45a.

3. The Commission shall adopt implementing acts to lay down the technical specifications for the quality, resolution and use of fingerprints and of the facial image for biometric verification and identification in the VIS.

4. The implementing acts referred to in paragraphs 1, 2 and 3 of this Article shall be adopted in accordance with the examination procedure referred to in Article 49(2).

*Article 45a*

#### **Use of VIS data for reporting and statistics**

1. The duly authorised staff of the competent authorities of Member States, the Commission, eu-LISA, the European Asylum Support Office and the European Border and Coast Guard Agency, including the ETIAS Central Unit in accordance with Article 9j, shall have access to the VIS to consult the following data, solely for the purposes of reporting and statistics without allowing for individual identification and in accordance with the safeguards related to non-discrimination referred to in Article 7(2):

- (a) status information;
- (b) the authority with which the application has been lodged, including its location;
- (c) sex, age and nationality or nationalities of the applicant;
- (d) country and city of residence of the applicant, only as regards visas;
- (e) current occupation (job group) of the applicant, only as regards visas;
- (f) the Member States of first entry and destination, only as regards visas;
- (g) date and place of the application and the decision concerning the application (issued, withdrawn, refused, annulled, revoked, renewed or extended);
- (h) the type of document applied for or issued, i.e. whether airport transit visa, uniform or limited territorial validity visa, long-stay visa or residence permit;

- (i) the type of the travel document and the country which issued the travel document, only as regards visas;
- (j) the decision concerning the application and, in the case of refusal, withdrawal, annulment or revocation, the grounds indicated for that decision;
- (k) hits resulting from queries of EU information systems, Europol data or Interpol databases pursuant to Article 9a or 22b, differentiated by system or database, or hits against the specific risk indicators pursuant to Article 9j, and hits where, after manual verification pursuant to Article 9c, 9d, 9e or 22b the applicant's personal data was confirmed as corresponding to the data present in one of the information systems or databases queried;
- (l) decisions to refuse a visa, long-stay visa or residence permit which are correlated to a manually verified and confirmed hit in one of the information systems or databases queried or to a hit against the specific risk indicators;
- (m) the competent authority, including its location, which decided on the application and the date of the decision, only as regards visas;
- (n) the cases in which the same applicant applied for a visa from more than one visa authority, indicating those visa authorities, their location and the dates of the decisions;
- (o) the main purposes of the journey, only as regards visas;
- (p) visa applications processed in representation pursuant to Article 8 of Regulation (EC) No 810/2009;
- (q) the data entered in respect of any document withdrawn, annulled, revoked, renewed or extended, as applicable;
- (r) the expiry date of the long-stay visa or residence permit;
- (s) the number of persons exempt from the requirement to give fingerprints pursuant to Article 13(7) of Regulation (EC) No 810/2009;
- (t) the cases in which the data referred to in point (6) of Article 9 could not be provided, in accordance with Article 8(5);
- (u) 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 Article 8(5);
- (v) the cases in which a person who could not provide the data referred to in point (6) of Article 9 was refused a visa, in accordance with Article 8(5);
- (w) links to the previous application file on that applicant as well as links of the application files of the persons travelling together, only as regards visas.

The duly authorised staff of the European Border and Coast Guard Agency shall have access to the VIS to consult the data referred to in the first subparagraph of this paragraph for the purpose of carrying out risk analyses and vulnerability assessments as referred to in Articles 29 and 32 of Regulation (EU) 2019/1896.

2. For the purposes of paragraph 1 of this Article, 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 Regulation (EU) 2019/817. In accordance with Article 39(1) of that Regulation, cross-system statistical data and analytical reporting shall allow the authorities listed in paragraph 1 of this Article to obtain customisable reports and statistics, to support the implementation of the specific risk indicators referred to in Article 9j of this Regulation, to improve the assessment of the security, illegal immigration and high epidemic risks, to enhance the efficiency of border checks and to help the visa authorities to process visa applications.

3. The procedures put in place by 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, eu-LISA shall compile statistics based on the VIS data on visas showing, for each location where a visa application was lodged and for each Member State, in particular:

- (a) the number of airport transit (A) visas applied for; the number of A visas issued, disaggregated by single airport transit and multiple airport transits; the number of A visas refused;

- (b) the number of short-stay (C) visas applied for (and disaggregated by the main purposes of the journey); the number of C visas issued, disaggregated by issued for single entry, two entries or multiple entry and the latter divided by length of validity (six months or below, one year, two years, three years, four years, five years); the number of visas with limited territorial validity issued (LTV); the number of C visas refused.

The daily statistics shall be stored in the central repository for reporting and statistics in accordance with Article 39 of Regulation (EU) 2019/817.

5. Every quarter, 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, withdrawn, revoked, annulled and extended;
- (b) total of residence permits applied for, issued, refused, withdrawn, revoked, annulled and renewed.

6. At the end of each year, statistical data shall be compiled in an annual report for that year. The statistics shall contain a breakdown of data for each location and each Member State. The report shall be published and transmitted to the European Parliament, to the Council, to the Commission, to the European Border and Coast Guard Agency, to the European Data Protection Supervisor and to the supervisory authorities.

7. At the request of the Commission, 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

#### Notifications

1. Member States shall notify the Commission of the authority which is to be considered as controller as referred to in Article 29(4).
2. Member States shall notify the Commission and eu-LISA of the competent authorities referred to in Article 6(3) which have access to the VIS to enter, amend, erase or consult data in the VIS and of the VIS designated authority as referred to in Article 9d(1) and Article 22b(14).

Three months after the date of the start of operations of the VIS pursuant to Article 11 of Regulation (EU) 2021/1134 of the European Parliament and of the Council \* eu-LISA shall publish a consolidated list of the authorities notified pursuant to the first subparagraph of this paragraph in the *Official Journal of the European Union*.

Member States shall notify the Commission and eu-LISA of any changes to the authorities notified without delay. In the event of such changes, eu-LISA shall publish once a year an updated consolidated list in the *Official Journal of the European Union*. eu-LISA shall maintain a continuously updated public website containing that information.

3. Member States shall notify the Commission and eu-LISA of their designated authorities and of their central access points as referred to in Article 22l and shall notify any changes in that regard without delay.
4. The Commission shall publish the information referred to in paragraphs 1 and 3 in the *Official Journal of the European Union*. In the event of changes to the information, the Commission shall publish once a year an updated consolidated version of it. The Commission shall maintain a continuously updated public website containing that information.

#### Article 45c

#### Access to data for verification by carriers

1. In order to fulfil their obligation under point (b) of Article 26(1) of the Schengen Convention, air carriers, sea carriers and international carriers transporting groups overland by coach shall send a query to the VIS in order to verify whether third country nationals who are subject to a visa requirement or who are required to hold a long-stay visa or a residence permit are in possession of a valid visa, long-stay visa or residence permit, as applicable.

2. Secure access to the carrier gateway referred to in point (h) of Article 2a, including the possibility to use mobile technical solutions, shall allow carriers to proceed with the query referred to in paragraph 1 of this Article prior to the boarding of a passenger.

For this purpose, as regards visas, the carrier shall provide the data referred to in point (4)(a), (b) and (c) of Article 9 and as regards long-stay visas and residence permits, the carrier shall provide the data referred to in points (d), (e) and (f) of Article 22a(1), as contained in the travel document. The carrier shall also indicate the Member State of entry or, in the case of airport transit, the Member State of transit.

By way of derogation from the second subparagraph of this paragraph, in the case of airport transit, the carrier shall not be obliged to send a query to the VIS, except where the third-country national is required to hold an airport transit visa in accordance with Article 3 of Regulation (EC) No 810/2009.

3. The VIS shall provide the carriers with an OK/NOT OK answer, indicating whether the person has a valid visa, long-stay visa or residence permit, as applicable.

If a visa with limited territorial validity has been issued in accordance with Article 25 of Regulation (EC) No 810/2009, the answer provided by the VIS shall take into account the Member States for which the visa is valid as well as the Member State of entry indicated by the carrier.

Carriers may store the information sent and the answer received in accordance with the applicable law. The OK/NOT OK answer shall not be regarded as a decision to authorise or refuse entry in accordance with Regulation (EU) 2016/399.

The Commission shall adopt implementing acts to lay down detailed rules concerning the conditions for the operation of the carrier gateway and the data protection and security rules applicable. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 49(2).

4. Where third-country nationals are refused boarding as a result of a consultation of the VIS, carriers shall inform them that this refusal is due to information stored in the VIS and shall provide them with information on their rights with regard to access to and rectification or erasure of personal data recorded in the VIS.

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 this Article to the duly authorised members of the carriers' staff. When setting up the authentication scheme, information security risk management and the principles of data protection by design and by default shall be taken into account.

The Commission shall adopt implementing acts to lay down the authentication scheme for carriers. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 49(2).

6. The carrier gateway 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 VIS data. eu-LISA shall be responsible for the security of the carrier gateway, for the security of the personal data it contains and for the process of extracting the personal data into the separate read-only database.

7. By way of derogation from paragraph 1 of this Article, for carriers transporting groups overland by coach, the verification pursuant to that paragraph shall be optional for the first 18 months following the date of the start of operations of the VIS pursuant to Article 11 of Regulation (EU) 2021/1134.

8. For the purpose of implementing paragraph 1 or for the purpose of resolving any potential dispute arising from its application, 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 consultation, the data transmitted by the carrier gateway and the name of the carrier in question.

eu-LISA shall store the logs for a period of two years. eu-LISA shall ensure that logs are protected by appropriate measures against unauthorised access.

*Article 45d***Fall-back procedures in the case of technical impossibility to access data by carriers**

1. Where it is technically impossible to proceed with the query referred to in Article 45c(1), because of a failure of any part of the VIS, the carriers shall be exempt from the obligation to verify the possession of a valid visa, long-stay visa or residence permit by using the carrier gateway. Where such a failure is detected by eu-LISA, the ETIAS Central Unit shall notify the carriers and the Member States. It shall also notify the carriers and the Member States when the failure is remedied. Where such a failure is detected by the carriers, they may notify the ETIAS Central Unit. The ETIAS Central Unit shall inform the Member States without delay about the notification of the carriers.
2. Where for other reasons than a failure of any part of VIS it is technically impossible for a carrier to proceed with the query referred to in Article 45c(1) for a prolonged period of time, the carrier shall notify the ETIAS Central Unit. The ETIAS Central Unit shall inform the Member States without delay about the notification of that carrier.
3. The Commission shall adopt an implementing act to lay down the details of the fall-back procedures in the case of technical impossibility to access data by carriers. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 49(2).

*Article 45e***Access to VIS data by European Border and Coast Guard teams**

1. To exercise the tasks and powers pursuant to Article 82(1) and (10) of Regulation (EU) 2019/1896 of the European Parliament and of the Council \*\* 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 VIS data.
2. To ensure the access referred to in paragraph 1 of this Article, 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 45f are fulfilled.

*Article 45f***Conditions and procedure for access to VIS data by European Border and Coast Guard teams**

1. In view of the access referred to in Article 45e(1), a European Border and Coast Guard team may submit a request for the consultation of all VIS data or a specific set of VIS data to the European Border and Coast Guard central access point referred to in Article 45e(2). The request shall refer to the operational plan on border checks, border surveillance 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 of this Article are fulfilled. If all conditions for access are fulfilled, the duly authorised staff of the central access point shall process the request. 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 European Border and Coast Guard team to consult the VIS in order to fulfil the operational aims specified in the operational plan on border checks, border surveillance and return; and
  - (b) consultation of the VIS is necessary for performing the specific tasks entrusted to the team by the host Member State.
3. In accordance with Article 82(4) of Regulation (EU) 2019/1896, members of the European Border and Coast Guard teams, as well as teams of staff involved in return-related tasks shall act in response to information obtained from the VIS only 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 European Border and Coast Guard teams to act on its behalf.



4. In the 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 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 European Border and Coast Guard teams shall have access to VIS data for verification at external border crossing points in accordance with Article 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 Article 19 or 22h of this Regulation respectively;
  - (c) when identifying any person that does not or no longer fulfils 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 Articles 20 and 22i of this Regulation.
6. Where access and searches pursuant to paragraph 5 reveal the existence of data recorded in the 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 eu-LISA in accordance with Article 34.
8. Every instance of access and every search made by the European Border and Coast Guard teams shall be logged in accordance with Article 34 and every use made of data accessed by the European Border and Coast Guard teams shall be registered.
9. For the purposes of Article 45e and of this Article, no parts of the 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 the VIS to which the European Border and Coast Guard Agency has access be transferred to such a system. No part of the 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.

\* Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System (OJ L 248, 13.7.2021, p. 11).

\*\* Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624 (OJ L 295, 14.11.2019, p. 1).";

(45) Articles 46, 47 and 48 are deleted;

(46) the following Article is inserted:

*"Article 48a*

### **Exercise of delegation**

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The power to adopt delegated acts referred to in Article 9, Article 9h(2), Article 9j(2) and Article 22b(18) shall be conferred on the Commission for a period of five years from 2 August 2021. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

3. The delegation of power referred to in Article 9, Article 9h(2), Article 9j(2) and Article 22b(18) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Article 9, Article 9h(2), Article 9j(2) or Article 22b(18) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.”;

(47) Articles 49 and 50 are replaced by the following:

“Article 49

#### **Committee procedure**

1. The Commission shall be assisted by the committee established by Article 68(1) of Regulation (EU) 2017/2226. 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.

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. eu-LISA 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, eu-LISA shall have access to the necessary information relating to the data processing operations performed in the VIS.

3. Every two years eu-LISA shall submit to the European Parliament, the Council and the Commission a report on the technical functioning of the VIS, including the security and costs thereof. The report shall also contain, once the technology is in use, an evaluation of the use of facial images to identify persons, including an assessment of any difficulties encountered.

4. While respecting the provisions of national law on the publication of sensitive information, each Member State and Europol shall prepare annual reports on the effectiveness of access to VIS data for law enforcement purposes containing information and statistics on:

(a) the exact purpose of the consultation including the type of terrorist offence or other serious criminal offence;

(b) reasonable grounds given for the substantiated suspicion that the suspect, perpetrator or victim is covered by this Regulation;

- (c) the number of requests to access the VIS for law enforcement purposes and to access the data on children below 14 years of age;
- (d) the number and type of cases in which the urgency procedures referred to in Article 22n(2) were used, including those cases where the urgency was not accepted by the *ex post* verification carried out by the central access point;
- (e) 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.

A technical solution shall be made available to Member States in order to facilitate the collection of those data pursuant to Chapter IIIb for the purpose of generating statistics referred to in this paragraph. The Commission shall, by means of implementing acts, adopt the specifications of the technical solution. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 49(2).

5. Three years after the date of the start of operations of the VIS pursuant to Article 11 of Regulation (EU) 2021/1134 and every four years thereafter, the Commission shall produce an overall evaluation of the VIS. The overall evaluation shall include an examination of results achieved against objectives and costs sustained and an assessment of the continuing validity of the underlying rationale, and its impact on fundamental rights, 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. It shall also include a detailed analysis of the data provided in the annual reports foreseen by paragraph 4 of this Article, with a view to assessing the effectiveness of access to VIS data for law enforcement purposes, as well as an assessment of whether the querying of ECRIS-TCN by the VIS has contributed to supporting the objective of assessing whether the applicant could pose a threat to public policy or public security. The Commission shall transmit the evaluation to the European Parliament and the Council.

6. Member States shall provide eu-LISA and the Commission with the information necessary to draft the reports referred to in paragraphs 3, 4 and 5.

7. eu-LISA shall provide the Commission with the information necessary to produce the overall evaluation referred to in paragraph 5.

\* Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).".

## Article 2

### Amendments to Regulation (EC) No 810/2009

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

(1) Article 10 is amended as follows:

(a) paragraph 1 is replaced by the following:

"1. When lodging an application, applicants shall, where required in accordance with Article 13, appear in person to provide their fingerprints or facial image. Without prejudice to the first sentence of this paragraph and to Article 45, applicants may lodge their applications electronically, where available.";

(b) paragraph 3 is amended as follows:

(i) point (c) is replaced by the following:

"(c) allow his or her facial image to be taken live in accordance with Article 13 or, where the exemptions referred to in Article 13(7a) apply, present a photograph in accordance with the standards set out in Regulation (EC) No 1683/95;"

(ii) the following subparagraph is added:

“Without prejudice to point (c) of this paragraph, Member States may require the applicant to present a photograph in accordance with the standards set out in Regulation (EC) No 1683/95 at every application.”;

(2) Article 13 is amended as follows:

(a) paragraphs 1 to 4 are replaced by the following:

“1. Member States shall collect biometric identifiers of the applicant comprising a facial image and 10 fingerprints of the applicant 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) a facial image taken live at the time of the application;

(b) 10 fingerprints taken flat and collected digitally.

2a. The facial images and fingerprints referred to in paragraph 2 of this Article shall be collected for the sole purpose of recording them in the VIS in accordance with points (5) and (6) of Article 9 of the VIS Regulation and the national systems for visa processing.

3. Where fingerprints and a live facial image 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, those data shall be copied to the subsequent application.

However, where there is reasonable doubt regarding the identity of the applicant, the consulate shall collect the fingerprints and facial image of that applicant 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 be collected.

4. The facial image of third-country nationals referred to in paragraph 2 shall have sufficient image resolution and be of sufficient quality to be used in automated biometric matching. The technical requirements for this facial image of the applicant referred to in paragraph 2 shall be in accordance with the international standards as set out in the International Civil Aviation Organization (ICAO) document 9303, 8th edition.”;

(b) the following paragraph is inserted:

“6a. When collecting biometric identifiers of minors all of the following conditions shall be met:

(a) the staff taking the biometric identifiers of a minor have been trained specifically to take a minor’s biometric data in a child-friendly and child-sensitive manner and in full respect of the best interests of the child and the safeguards laid down in the United Nations Convention on the Rights of the Child;

(b) every minor is accompanied by an adult family member or legal guardian when the biometric identifiers are taken;

(c) no force is used to take the biometric identifiers.”;

(c) paragraph 7 is amended as follows:

(i) point (a) is replaced by the following:

“(a) children below the age of six and persons over the age of 75.”;

(ii) the following point is added:

“(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 an application would put them in serious danger.”;

(d) the following paragraphs are inserted:

“7a. Applicants as referred to in points (c), (d) and (e) of paragraph 7 may also be exempt from having their facial images taken live upon submission of the application.

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 application file in the VIS pursuant to Article 9 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.”;

(e) paragraph 8 is deleted;

(3) Article 21 is amended as follows:

(a) the following paragraphs are inserted:

“3a. For the purpose of assessing the entry conditions provided for in paragraph 3 of this Article, the consulate or the central authorities shall take into account, where applicable, the result of the verifications of hits pursuant to Article 9c of the VIS Regulation or the reasoned opinion provided in accordance with Articles 9e and 9g of that Regulation by the VIS designated authority as defined in point (3b) of Article 4 of the VIS Regulation or the ETIAS National Unit as referred to in Article 8 of Regulation (EU) 2018/1240 of the European Parliament and of the Council \*.

By way of derogation from Article 4(1), in the case of applications where a reasoned opinion was provided by the VIS designated authority or the ETIAS National Unit, the central authorities shall either be empowered to decide on the application themselves or shall, after assessing the reasoned opinion, inform the consulate processing the application that they object to the issuance of the visa.

3b. For the purpose of assessing the entry conditions provided for in paragraph 3 of this Article, the consulate or the central authorities shall, where a red link exists in accordance with Article 32 of Regulation (EU) 2019/817 of the European Parliament and of the Council \*\*, assess and take into account the differences in the linked identities.

3c. Hits against the specific risk indicators referred to in Article 9j of the VIS Regulation pursuant to Article 9a(13) of that Regulation shall be taken into account in the examination of an application. The consulate and the central authorities shall in no circumstances take a decision automatically on the basis of a hit based on specific risk indicators. The consulate or the central authorities shall individually assess the security, illegal immigration and high epidemic risks in all cases.

\* Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018, p. 1).

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

(b) paragraph 4 is replaced by the following:

“4. The consulate or the central authorities shall verify, using the information obtained from the EES, in accordance with Article 24 of Regulation (EU) 2017/2226 of the European Parliament and of the Council \*, 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.

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

(c) the following paragraph is inserted:

“8a. Consulates shall pay particular attention to the correct verification of the identity of minors and the link with the person exercising parental authority or legal guardianship in order to prevent child trafficking.”;

(4) in point (a) of Article 25(1), the following point is added:

“(iv) to issue a visa for reasons of urgency, although the verifications of hits in accordance with Articles 9a to 9g of the VIS Regulation have not been completed.”;

(5) in Article 35, the following paragraph is inserted:

“5a. A third-country national for whom the verifications of hits in accordance with Articles 9a to 9g of the VIS Regulation have not been completed shall, in principle, not be issued a visa at the external border.

However, a visa with limited territorial validity for the territory of the issuing Member State may be issued at the external border for such persons in exceptional cases, in accordance with point (a) of Article 25(1).”;

(6) in Article 36, paragraph 3 is replaced by the following:

“3. This Article shall apply without prejudice to Article 35(3) to (5a).”;

(7) in Article 39, paragraphs 2 and 3 are replaced by the following:

“2. Consular and central authorities’ staff shall, in the performance of their duties, fully respect human dignity and the fundamental rights and principles recognised by the Charter of Fundamental Rights of the European Union. Any measures taken shall be proportionate to the objectives pursued by such measures.

3. While performing their tasks, consular and central authorities’ staff shall not discriminate against persons on grounds of sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation. They shall pay particular attention to children, the elderly and persons with a disability. The best interests of the child shall be a primary consideration.”;

(8) Article 46 is deleted;

(9) Article 57 is amended as follows:

(a) paragraph 1 is replaced by the following:

“1. Two years after all the provisions of this Regulation have become applicable, the Commission shall produce an overall evaluation of its application. The overall evaluation shall include an examination of the results achieved against the objectives pursued and of the implementation of this Regulation.”;

(b) paragraphs 3 and 4 are deleted;

(10) in point C(b) of Annex X, the second indent is replaced by the following:

“— respect the human dignity and integrity of applicants, do not discriminate against persons on grounds of sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation,

— respect the provisions regarding the taking of biometrics identifiers laid down in Article 13, and”;

(11) Annex XII is deleted.

*Article 3***Amendments to Regulation (EU) 2016/399**

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

(1) in Article 8, paragraph 3 is amended as follows:

(a) the following point is inserted:

“(bb) if the third-country national holds a long-stay visa or a residence permit, the thorough checks on entry shall 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 VIS in accordance with Article 22g of Regulation (EC) No 767/2008.

In circumstances where verification of the identity of the holder of the long-stay visa or residence permit or of the authenticity and validity of the long-stay visa or residence permit, fails or where there are doubts as to the identity of the holder, the authenticity of the long-stay visa or residence permit or the travel document, the duly authorised staff of those competent authorities shall proceed to a verification of the document chip;”;

(b) points (c) to (f) are deleted;

(2) in Annex VII, point 6, is replaced by the following:

“6. Minors

- 6.1. Border guards shall pay particular attention to minors, whether travelling accompanied or unaccompanied. Minors crossing an external border shall be subject to the same checks on entry and exit as adults, as provided for in this Regulation.
- 6.2. In the case of accompanied minors, the border guard shall check that the persons accompanying minors have parental care or legal guardianship over them, especially where minors are accompanied by only one adult and there are serious grounds for suspecting that they may have been unlawfully removed from the custody of the persons legally exercising parental care or legal guardianship over them. In the latter case, the border guard shall carry out a further investigation in order to detect any inconsistencies or contradictions in the information given.
- 6.3. In the case of minors travelling unaccompanied, border guards shall ensure, by means of thorough checks on travel documents and supporting documents, that the minors do not leave the territory against the wishes of the persons having parental care or legal guardianship over them.
- 6.4. Member States shall nominate national contact points for consultation on minors and inform the Commission thereof. A list of those national contact points shall be made available to the Member States by the Commission.
- 6.5. Where there is doubt as to any of the circumstances set out in points 6.1, 6.2 and 6.3, border guards shall make use of the list of national contact points for consultation on minors.
- 6.6. Member States shall ensure that border guards verifying biometrics of children or using them to identify a child are specifically trained to do so in a child-friendly and child-sensitive manner and in full respect of the best interests of the child and the safeguards laid down in the United Nations Convention on the Rights of the Child. When accompanied by a parent or a legal guardian that person shall accompany the child when the biometrics are verified or used for identification. No force shall be used. Member States shall ensure, where necessary, that the infrastructure at border crossing points is adapted for the use of biometrics of children.”.

## Article 4

**Amendments to Regulation (EU) 2017/2226**

Regulation (EU) 2017/2226 is amended as follows:

(1) Article 8 is amended as follows:

(a) in paragraph 2, point (e) is replaced by the following:

“(e) where the identity of a visa holder is verified using fingerprints or facial image, verify at the borders at which the EES is operated the identity of a visa holder by comparing the fingerprints or facial image of the visa holder with the fingerprints or the facial image taken live that are recorded in the VIS, in accordance with Article 23(2) and (4) of this Regulation and Article 18(6) of Regulation (EC) No 767/2008. Only facial images recorded in the VIS with an indication that the facial image was taken live upon submission of the visa application shall be used for that comparison.”;

(b) the following paragraphs are inserted:

“3a. Interoperability shall enable the erasure of the facial image referred to in point (d) of Article 16(1) from the individual file where a facial image is recorded in the VIS with an indication that it was taken live upon submission of the visa application.

3b. Interoperability shall enable the EES to automatically notify the VIS in accordance with Article 23(3) of Regulation (EC) No 767/2008 where the exit of a child below the age of 12 is entered in the entry/exit record in accordance with Article 16(3) of this Regulation.”;

(c) the following paragraph is added:

“5. From the date of the start of operations of the VIS pursuant to Article 11 of Regulation (EU) 2021/1134 of the European Parliament and of the Council \* the EES shall be connected to the ESP to enable the automated processing pursuant to Articles 9a and 22b of Regulation (EC) No 767/2008.

\* Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System (OJ L 248, 13.7.2021, p. 11).”;

(2) in Article 9(2), the following subparagraph is added:

“The EES shall provide the functionality for the centralised management of that list. The detailed rules on managing that 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).”;

(3) in Article 13, paragraph 3 is replaced by the following:

“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 third-country national holding a short-stay visa issued for one or two entries has already used the number of authorised entries or whether the holder of a short-stay visa has reached the maximum duration of the authorised stay.

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.

Where third-country nationals are refused boarding due to the answer of the web service, carriers shall inform them that this refusal is due to information stored in the EES and shall provide them with information on their rights with regard to access to and rectification or erasure of personal data recorded in the EES.”;



(4) Article 15 is amended as follows:

(a) paragraph 1 is replaced by the following:

“1. Where it is necessary to create an individual file or to update the facial image referred to in point (d) of Article 16(1) and point (b) of Article 17(1), the facial image shall be taken live. This shall not apply to third-country nationals subject to a visa requirement where a facial image is recorded in the VIS with an indication that it was taken live upon submission of the application.”;

(b) paragraph 5 is deleted;

(5) Article 16 is amended as follows:

(a) in paragraph 1, point (d) is replaced by the following:

“(d) the facial image as referred to in Article 15, unless a facial image is recorded in the VIS with an indication that it was taken live upon submission of the application.”;

(b) the following paragraph is inserted:

“1a. Where, for a third-country national whose individual file contains a facial image as referred to in point (d) of paragraph 1, a facial image is subsequently recorded in the VIS with an indication that it was taken live upon submission of the application, the EES shall erase the facial image from the individual file.”;

(6) in Article 18(2), the following subparagraph is added:

“By way of derogation from Article 15(1) and point (d) of Article 16(1) of this Regulation, where the third-country national is refused entry on the basis of a reason corresponding to point (B) or (D) of Part B of Annex V to Regulation (EU) 2016/399 and where there are doubts regarding the authenticity of the facial image recorded in the VIS, the facial image referred to in point (a) of this paragraph shall be taken live and entered in the individual file irrespective of any facial image recorded in the VIS.”;

(7) Article 23 is amended as follows:

(a) in paragraph 2, the third subparagraph is replaced by the following:

“If the search in the EES with the data set out in the first subparagraph of this paragraph indicates that data on the third-country national are recorded in the EES, the border authorities shall:

(a) for third-country nationals who are not subject to a visa requirement, compare the live facial image with the facial image referred to in point (b) of Article 17(1) or proceed to a verification of fingerprints against the EES, and

(b) for third-country nationals subject to a visa requirement:

(i) compare the live facial image with the facial image recorded in the EES referred to in point (d) of Article 16(1) of this Regulation or with the facial image taken live recorded in the VIS in accordance with point (5) of Article 9 of Regulation (EC) No 767/2008, or

(ii) proceed to a verification of fingerprints directly against the VIS in accordance with Article 18 of Regulation (EC) No 767/2008.

For the verification of fingerprints or the facial image taken live against the VIS for visa holders, the border authorities may launch the search in the VIS directly from the EES as provided in Article 18(6) of Regulation (EC) No 767/2008.”;

(b) in the second subparagraph of paragraph 4, point (a) is replaced by the following:

“(a) for third-country nationals who are subject to a visa requirement, if the search in the VIS with the data referred to in Article 18(1) of Regulation (EC) No 767/2008 indicates that data on the third-country national are recorded in the VIS, a verification of fingerprints or the facial image taken live against the VIS shall be carried out in accordance with Article 18(6) of that Regulation. For that purpose, the border authority may launch a search from the EES to the VIS as provided for in Article 18(7) of Regulation (EC) No 767/2008. Where a verification of a third-country national pursuant to paragraph 2 of this Article failed, the border authorities shall access the VIS data for identification in accordance with Article 20 of Regulation (EC) No 767/2008.”;

(8) in Article 24 the following paragraph is added:

“5. The competent visa authorities and the authorities competent to decide on an application for a long-stay visa or residence permit shall have access to the relevant data in the EES for the purpose of manually verifying the hits resulting from the queries in the EES in accordance with Articles 9c and 22b of Regulation (EC) No 767/2008 as well as for the purpose of examining and deciding on those applications.”;

(9) in Article 35, paragraph 4 is replaced by the following:

“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 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).”.

#### Article 5

### Amendments to Regulation (EU) 2018/1240

Regulation (EU) 2018/1240 is amended as follows:

(1) in Article 4, the following point is inserted:

“(da) support the objectives of the VIS of facilitating the visa application procedure and contribute to the prevention of threats to the internal security of the Member States, by allowing queries in ETIAS, including the ETIAS watchlist referred to in Article 34;”;

(2) Article 7 is amended as follows:

(a) paragraph 2 is amended as follows:

(i) the following point is inserted:

“(ca) defining, establishing, assessing *ex ante*, implementing, evaluating *ex post*, revising and deleting the specific risk indicators referred to in Article 9j of Regulation (EC) No 767/2008 after consulting the VIS Screening Board;”;

(ii) point (e) is replaced by the following:

“(e) carrying out regular audits of the processing of applications and of the implementation of Article 33 of this Regulation and Article 9j of Regulation (EC) No 767/2008, including by regularly assessing their impact on fundamental rights, in particular with regard to privacy and personal data protection;”;

(iii) point (h) is replaced by the following:

“(h) notifying carriers in cases of a failure of the ETIAS Information System as referred to in Article 46(1) of this Regulation or of the VIS as referred to in Article 45d(1) of Regulation (EC) No 767/2008;”;

(b) in paragraph 3, the following point is inserted:

“(aa) information on the functioning of the specific risk indicators for the VIS.”;

(3) in Article 8(2) the following point is added:

“(h) manually verifying the hits in the ETIAS watchlist referred to in Article 34 of this Regulation triggered by the automated queries carried out by the VIS pursuant to Articles 9a and 22b of Regulation (EC) No 767/2008 and following up those hits, in accordance with Article 9e of that Regulation.”;

- (4) the following article is inserted:

*“Article 11a*

**Interoperability with the VIS**

From the date of the start of operations of the VIS pursuant to Article 11 of Regulation (EU) 2021/1134 of the European Parliament and of the Council \* the ETIAS Central System and the CIR shall be connected to the ESP to enable the automated processing pursuant to Articles 9a and 22b of Regulation (EC) No 767/2008.

\* Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System (OJ L 248, 13.7.2021, p. 11).”;

- (5) in Article 13, the following paragraph is inserted:

“4b. Access by visa authorities and the authorities competent to decide on an application for a long-stay visa or residence permit to the ETIAS Central System in accordance with Articles 9a and 22b of Regulation (EC) No 767/2008 shall be limited to verifying whether the applicant for a visa, long-stay visa or residence permit or his or her travel document corresponds to an issued, refused, revoked or annulled travel authorisation in the ETIAS Central System and the reasons for the issuing, refusal, revocation or annulment.”;

- (6) the following chapter is inserted:

“CHAPTER IXa

**USE OF ETIAS BY VISA AUTHORITIES AND AUTHORITIES COMPETENT TO DECIDE ON AN APPLICATION FOR A LONG-STAY VISA OR RESIDENCE PERMIT**

*Article 49a*

**Access to data by visa authorities and authorities competent to decide on an application for a long-stay visa or residence permit**

For the purpose of carrying out the verifications laid down in Articles 9c and 22b of Regulation (EC) No 767/2008, the competent visa authorities and authorities competent to decide on an application for a long-stay visa or residence permit shall have the right to access relevant data in the ETIAS Central System and the CIR.”;

- (7) in Article 69(1), the following point is added:

“(h) the hits triggered by the automated queries carried out by the VIS pursuant to Articles 9a and 22b of Regulation (EC) No 767/2008, the data processed by the competent visa authorities and authorities competent to decide on an application for a long-stay visa or residence permit for the purpose of manually verifying the hits in accordance with Articles 9c and 22b of that Regulation, and the data processed by the ETIAS National Units in accordance with Article 9e of that Regulation.”;

- (8) in Article 75(1), the following point is added:

“(d) the specific risk indicators referred to in Article 9j of Regulation (EC) No 767/2008.”.

*Article 6*

**Amendments to Regulation (EU) 2018/1860**

In Regulation (EU) 2018/1860, Article 19 is replaced by the following:

*“Article 19*

**Applicability of the provisions of Regulation (EU) 2018/1861**

Insofar as not established in this Regulation, the entry, processing and updating of alerts, the provisions on responsibilities of the Member States and eu-LISA, the conditions concerning access and the review period for alerts, data processing, data protection, liability and monitoring and statistics, as laid down in Articles 6 to 19, Article 20(3) and (4), Articles 21, 23, 32 and 33, Article 34(5), Article 36a and Articles 38 to 60 of Regulation (EU) 2018/1861, shall apply to data entered and processed in SIS in accordance with this Regulation.”.

*Article 7***Amendments to Regulation (EU) 2018/1861**

Regulation (EU) 2018/1861 is amended as follows:

- (1) the following article is inserted:

*“Article 18a*

**Keeping of logs for the purposes of interoperability with VIS**

Logs of each data processing operation carried out within SIS and VIS pursuant to Article 36c of this Regulation shall be kept in accordance with Article 18 of this Regulation and Article 34 of Regulation (EC) No 767/2008.”;

- (2) the following article is inserted:

*“Article 36a*

**Interoperability with VIS**

From the date of the start of operations of the VIS pursuant to Article 11 of Regulation (EU) 2021/1134 of the European Parliament and of the Council \* the Central SIS shall be connected to the ESP to enable the automated processing pursuant to Articles 9a and 22b of Regulation (EC) No 767/2008.

\* Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System (OJ L 248, 13.7.2021, p. 11).”.

*Article 8***Amendments to Regulation (EU) 2019/817**

Regulation (EU) 2019/817 is amended as follows:

- (1) in Article 4, point 20 is replaced by the following:

“(20) ‘designated authorities’ means the Member State designated authorities as defined in point (26) of Article 3(1) of Regulation (EU) 2017/2226, point (3a) of Article 4 of Regulation (EC) No 767/2008, and point (21) of Article 3(1) of Regulation (EU) 2018/1240;”;

- (2) in Article 13(1), point (b) is replaced by the following:

“(b) the data referred to in points (5) and (6) of Article 9 and points (k) and (j) of Article 22a(1) of Regulation (EC) No 767/2008, provided, as regards the facial image, that it was recorded in VIS with an indication that it was taken live upon submission of the application;”;

- (3) in Article 18(1), point (b) is replaced by the following:

“(b) the data referred to in points (4)(a) to (ca) and points (5) and (6) of Article 9 and in points (d) to (g), (j) and (k) of Article 22a(1) of Regulation (EC) No 767/2008;”;

- (4) in Article 26(1), point (b) is replaced by the following:

“(b) the visa authorities and the authorities competent to decide on an application for a long-stay visa or residence permit as referred to in Article 6(1) of Regulation (EC) No 767/2008 when creating or updating an application file in VIS in accordance with that Regulation;

(ba) the VIS designated authorities referred to in Articles 9d and 22b of Regulation (EC) No 767/2008 when manually verifying hits triggered by automated queries from VIS to ECRIS-TCN in accordance with that Regulation;”;

- (5) in Article 27(3), point (b) is replaced by the following:

“(b) surname (family name); first name(s) (given name(s)); date of birth; place of birth; sex, and nationality or nationalities as referred to in points (4)(a) and (aa) of Article 9 and in point (d) of Article 22a(1) of Regulation (EC) No 767/2008;”;

(6) in Article 29(1), point (b) is replaced by the following:

- “(b) the visa authorities and the authorities competent to decide on an application for a long-stay visa or residence permit as referred to in Article 6(1) of Regulation (EC) No 767/2008 for matches that occurred when creating or updating an application file in VIS in accordance with that Regulation, with the exception of the cases referred to in point (ba) of this paragraph;
- (ba) the VIS designated authorities referred to in Articles 9d and 22b of Regulation (EC) No 767/2008 only for yellow links created between data in VIS and ECRIS-TCN when creating or updating an application file in VIS in accordance with that Regulation;”;

(7) in Article 39, paragraph 2 is replaced by the following:

“2. eu-LISA shall establish, implement and host in its technical sites the CRRS containing the data and statistics referred to in Article 63 of Regulation (EU) 2017/2226, Article 45a of Regulation (EC) No 767/2008, Article 84 of Regulation (EU) 2018/1240, Article 60 of Regulation (EU) 2018/1861 and Article 16 of Regulation (EU) 2018/1860, logically separated by EU information system. Access to the CRRS shall be granted by means of controlled, secured access and specific user profiles, solely for the purpose of reporting and statistics, to the authorities referred to in Article 63 of Regulation (EU) 2017/2226, Article 45a of Regulation (EC) No 767/2008, Article 84 of Regulation (EU) 2018/1240 and Article 60 of Regulation (EU) 2018/1861.”;

(8) in Article 72, the following paragraph is inserted:

“1a. Without prejudice to paragraph 1 of this Article, for the purposes of the automated processing pursuant to Articles 9a and 22b of Regulation (EC) No 767/2008, the ESP shall start operations, limited to those purposes, from the date of the start of operations of the VIS pursuant to Article 11 of Regulation (EU) 2021/1134 of the European Parliament and of the Council \*.

\* Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System (OJ L 248, 13.7.2021, p. 11).”.

#### *Article 9*

### **Amendments to Regulation (EU) 2019/1896**

In Article 10(1) of Regulation (EU) 2019/1896, the following point is inserted:

“(afa) fulfil the tasks and obligations entrusted to the Agency under Regulation (EC) No 767/2008;”.

#### *Article 10*

### **Repeal**

Decisions 2004/512/EC and 2008/633/JHA are repealed. References to those Decisions shall be construed as references to Regulation (EC) No 767/2008 and shall be read in accordance with the correlation tables in Annexes I and II to this Regulation, respectively.

#### *Article 11*

### **Start of operations**

1. No later than 31 December 2023, the Commission shall adopt a decision by means of an implementing act setting the date on which VIS operations start pursuant to this Regulation. The Commission shall adopt that decision once the following conditions are met:

- (a) the measures referred to in Article 5a(3), Article 6(5), the third paragraph of Article 9, Article 9h(2), Article 9j(2) and (3), Article 22b(18), the second subparagraph of Article 29(2a), the second subparagraph of Article 29a(3), Article 45, the fourth subparagraph of Article 45c(3), the second subparagraph of Article 45c(5), Article 45d(3), and third subparagraph of Article 50(4) of Regulation (EC) No 767/2008 have been adopted;

- (b) eu-LISA has notified the Commission of the successful completion of all testing activities;
- (c) Member States have notified the Commission that they have made the necessary technical and legal arrangements to process data pursuant to this Regulation and have notified to the Commission and eu-LISA the information referred to in Article 45b of Regulation (EC) No 767/2008;

2. The Commission shall closely monitor the process of gradual fulfilment of the conditions set out in paragraph 1 and shall inform the European Parliament and the Council about the outcome of the testing activities referred to in point (b) of that paragraph.

3. By 3 August 2022 and every year thereafter until the decision of the Commission referred to in paragraph 1 has been taken, the Commission shall submit a report to the European Parliament and to the Council on the state of play of preparations for the full implementation of this Regulation. That report shall contain detailed information on the costs incurred and information as to any risks which may impact the overall costs of the VIS to be borne by the general budget of the Union.

In the event of delays in the full implementation of this Regulation, the Commission shall inform the European Parliament and the Council as soon as possible about the reasons for the delays and their impact in terms of time and costs.

4. The decision referred to in paragraph 1 shall be published in the *Official Journal of the European Union*.

## Article 12

### Entry into force and application

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

This Regulation shall apply from the date set by the Commission in accordance with Article 11, with the exception of:

- (a) the following provisions which shall apply from 2 August 2021:

- (i) point (6) of Article 1 of this Regulation as regards Article 5a(3) and Article 6(5) of Regulation (EC) No 767/2008;
- (ii) point (10)(c) of Article 1 of this Regulation as regards the third paragraph of Article 9 of Regulation (EC) No 767/2008;
- (iii) point (11) of Article 1 of this Regulation as regards Article 9h(2) and Article 9j(2) and (3) of Regulation (EC) No 767/2008;
- (iv) point (26) of Article 1 of this Regulation as regards Article 22b(18) of Regulation (EC) No 767/2008;
- (v) point (34) of Article 1 of this Regulation as regards the second subparagraph of Article 29(2a) and the second subparagraph of Article 29a(3) of Regulation (EC) No 767/2008;
- (vi) point (44) of Article 1 of this Regulation as regards Article 45, the fourth subparagraph of Article 45c(3), the second subparagraph of Article 45c(5) and Article 45d(3) of Regulation (EC) No 767/2008;
- (vii) point (46) of Article 1;
- (viii) point (47) of Article 1 of this Regulation as regards Article 49 and the third subparagraph of Article 50(4) of Regulation (EC) No 767/2008; and
- (ix) point (2) of Article 4 of this Regulation as regards Article 9(2) of Regulation (EU) 2017/2226;

- (b) points (40) to (43) of Article 1, which shall apply from 3 August 2022;

- (c) point (44) of Article 1 of this Regulation as regards Articles 45e and 45f of Regulation (EC) No 767/2008, which shall apply from 3 August 2023.

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

Done at Strasbourg, 7 July 2021.

*For the European Parliament*  
*The President*  
D. M. SASSOLI

*For the Council*  
*The President*  
A. LOGAR

---

## ANNEX I

**CORRELATION TABLE FOR DECISION 2004/512/EC**

Council Decision 2004/512/EC	Regulation (EC) No 767/2008
Article 1(1)	Article 1
Article 1(2)	Article 2a
Article 2	-
Article 3 and 4	Article 45
Article 5	Article 49
Article 6	-



## ANNEX II

**CORRELATION TABLE FOR DECISION 2008/633/JHA**

Council Decision 2008/633/JHA	Regulation (EC) No 767/2008
Article 1	Article 1
Article 2	Article 4
Article 3	Articles 22l and 22m, Article 45b
Article 4	Article 22n
Article 5	Article 22o
Article 6	Article 22t
Article 7	Article 22m Article 22r
Article 8	Article 28(5), Article 31(4) and (5), and Chapter VI
Article 9	Article 32
Article 10	Article 33
Article 11	Article 35
Article 12	Article 36
Article 13	Article 30
Article 14	Article 38
Article 15	-
Article 16	Article 22s
Article 17	Article 50



ISSN 1977-0677 (electronic edition)  
ISSN 1725-2555 (paper edition)



Publications Office  
of the European Union  
L-2985 Luxembourg  
LUXEMBOURG

EN