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

►B REGULATION (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)

Amended by:

		Official Journal		
		No	page	date
►M1	Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018	L 236	1	19.9.2018
►M2	Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019	L 135	27	22.5.2019

Corrected by:

►C1	Corrigendum, OJ L 258, 15.10.2018, p. 5 (2017/2226)
►C2	Corrigendum, OJ L 117, 3.5.2019, p. 14 (2017/2226)

▼B

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

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

1. This Regulation establishes an 'Entry/Exit System' (EES) for:

(a) the recording and storage of the date, time and place of entry and exit of third–country nationals crossing the borders of the Member States at which the EES is operated;

(b) the calculation of the duration of the authorised stay of such third-country nationals;

(c) the generation of alerts to Member States when the authorised stay has expired; and

(d) the recording and storage of the date, time and place of refusal of entry of third-country nationals whose entry for a short stay has been refused, as well as the authority of the Member State which refused the entry and the reasons therefor.

2. For the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences, this Regulation also lays down the conditions under which Member States' designated authorities and Europol may obtain access to the EES for consultation.

▼M2

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

[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

Article 2

Scope

1. This Regulation applies to:

(a) third-country nationals admitted for a short stay to the territory of the Member States who are subject to border checks in accordance with Regulation (EU) 2016/399 when crossing the borders at which the EES is operated; and

(b) third-country nationals, on entry to and exit from the territory of the Member States, who:

(i) are members of the family of a Union citizen to whom Directive 2004/38/EC applies or of a national of a third country enjoying the right of free movement equivalent to that of Union citizens under an agreement between the Union and its Member States, on the one hand, and a third country, on the other; and

(ii) do not hold a residence card pursuant to Directive 2004/38/EC or a residence permit pursuant to Council Regulation (EC) No 1030/2002 ([1]).

2. This Regulation also applies to third-country nationals whose entry for a short stay to the territory of the Member States is refused in accordance with Article 14 of Regulation (EU) 2016/399.

3. This Regulation does not apply to:

(a) third–country nationals who are members of the family of a Union citizen to whom Directive 2004/38/EC applies and who hold a residence card pursuant to that Directive, whether or not they accompany or join that Union citizen;

(b) third-country nationals who are members of the family of a national of a third country, whether or not they accompany or join that national of a third country, where:

(i) that national of a third country enjoys 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; and

(ii) those third-country nationals hold a residence card pursuant to Directive 2004/38/EC or a residence permit pursuant to Regulation (EC) No 1030/2002;

(c) holders of residence permits referred to in point 16 of Article 2 of Regulation (EU) 2016/399 other than those covered by points (a) and (b) of this paragraph;

([1]) 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).

▼B

(d) third-country nationals exercising their right to mobility in accordance with Directive 2014/66/EU of the European Parliament and of the Council ([1]) or Directive (EU) 2016/801 of the European Parliament and of the Council ([2]);

(e) holders of long-stay visas;

(f) nationals of Andorra, Monaco and San Marino and ►C1 holders of a passport issued by the Vatican City State or the Holy See; ◄

(g) persons or categories of persons exempt from border checks or benefiting from specific rules in relation to border checks as referred to in point (g) of Article 6a(3) of Regulation (EU) 2016/399;

(h) persons or categories of persons referred to in points (h), (i), (j) and (k) of Article 6a(3) of Regulation (EU) 2016/399.

4. The provisions of this Regulation regarding the calculation of the duration of the authorised stay and the generation of alerts to Member States when the authorised stay has expired do not apply to third-country nationals who:

(a) are members of the family of a Union citizen to whom Directive 2004/38/EC applies or of a national of a third country enjoying the right of free movement equivalent to that of Union citizens under an agreement between the Union and its Member States, on the one hand, and a third country, on the other; and

(b) do not hold a residence card pursuant to Directive 2004/38/EC or a residence permit pursuant to Regulation (EC) No 1030/2002.

Article 3

Definitions

1. For the purposes of this Regulation, the following definitions apply:

(1) ‘external borders’ means external borders as defined in point 2 of Article 2 of Regulation (EU) 2016/399;

(2) ‘internal borders’ means internal borders as defined in point 1 of Article 2 of Regulation (EU) 2016/399;

(3) ‘border authority’ means the border guard assigned in accordance with national law to carry out border checks as defined in point 11 of Article 2 of Regulation (EU) 2016/399;

(4) ‘immigration authority’ means the competent authority responsible, in accordance with national law, for one or more of the following:

(a) checking within the territory of the Member States whether the conditions for entry to, or stay on, the territory of the Member States are fulfilled;

([1]) Directive 2014/66/EU of the European Parliament and of the Council of 15 May 2014 on the conditions of entry and residence of third-country nationals in the framework of an intra- corporate transfer (OJ L 157, 27.5.2014, p. 1).

([2]) Directive (EU) 2016/801 of the European Parliament and of the Council of 11 May 2016 on the conditions of entry and residence of third-country nationals for the purposes of research, studies, training, voluntary service, pupil exchange schemes or educational projects and au pairing (OJ L 132, 21.5.2016, p. 21).

▼B

(b) examining the conditions for, and taking decisions related to, the residence of third-country nationals on the territory of the Member States insofar as that authority does not constitute a 'determining authority' as defined in point (f) of Article 2 of Directive 2013/32/EU of the European Parliament and of the Council [1], and, where relevant, providing advice in accordance with Council Regulation (EC) No 377/2004 [2];

(c) the return of third-country nationals to a third country of origin or transit;

(5) 'visa authority' means the visa authority as defined in point 3 of Article 4 of Regulation (EC) No 767/2008;

(6) 'third-country national' means any person who is not a citizen of the Union within the meaning of Article 20(1) TFEU, with the exception of persons who enjoy the right of free movement equivalent to that of Union citizens under agreements between the Union and its Member States, on the one hand, and third countries, on the other;

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

(8) 'short stay' means stays on the territory of the Member States of a duration of no more than 90 days in any 180-day period as referred to in Article 6(1) of Regulation (EU) 2016/399;

(9) 'short-stay visa' means visa as defined in point (a) of point 2 of Article 2 of Regulation (EC) No 810/2009 of the European Parliament and of the Council [3];

(10) 'national short-stay visa' means an authorisation issued by a Member State which does not apply the Schengen *acquis* in full with a view to an intended stay on the territory of that Member State of a duration of no more than 90 days in any 180-day period;

(11) 'authorised stay' means the exact number of days during which a third-country national is permitted to legally stay on the territory of the Member States, counting from the date of the entry in accordance with the applicable provisions;

(12) 'Member State responsible' means the Member State which has entered data in the EES;

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

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

(15) 'alphanumeric data' means data represented by letters, digits, special characters, spaces and punctuation marks;

---

[1] 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).

[2] Council Regulation (EC) No 377/2004 of 19 February 2004 on the creation of an immigration liaison officers network (OJ L 64, 2.3.2004, p. 1).

[3] 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).

▼B

(16) ‘fingerprint data’ means the data relating to the four fingerprints of the index, middle finger, ring finger and little finger from the right hand where present, and otherwise from the left hand;

(17) ‘facial image’ means digital images of the face;

(18) ‘biometric data’ means fingerprint data and facial image;

(19) ‘overstayer’ means a third-country national who does not fulfil or no longer fulfils the conditions relating to the duration of his or her authorised short stay on the territory of the Member States;

(20) ‘eu-LISA’ means the European Agency for the operational management of large-scale information systems in the area of freedom, security and justice established by Regulation (EU) No 1077/2011;

(21) ‘supervisory authorities’ means the supervisory authority established in accordance with Article 51(1) of Regulation (EU) 2016/679 and the supervisory authority established in accordance with Article 41(1) of Directive (EU) 2016/680;

▼M2

(22) ‘EES data’ means all data stored in the EES Central System and in the CIR in accordance with Articles 15 to 20;

(22a) ‘identity data’ means the data referred to in point (a) of Article 16(1) as well as the relevant data referred to in Articles 17(1) and 18(1);

▼B

(23) ‘law enforcement’ means the prevention, detection or investigation of terrorist offences or other serious criminal offences;

(24) ‘terrorist offence’ means an offence under national law which corresponds or is equivalent to one of the offences referred to in Directive (EU) 2017/541;

(25) ‘serious criminal offence’ means an offence which corresponds or is equivalent to one of the offences referred to in Article 2(2) of 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;

(26) ‘designated authority’ means an authority designated by a Member State pursuant to Article 29 as responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences;

(27) ‘self-service system’ means a self-service system as defined in point 23 of Article 2 of Regulation (EU) 2016/399;

(28) ‘e-gate’ means an e-gate as defined in point 24 of Article 2 of Regulation (EU) 2016/399;

(29) ‘Failure To Enrol Rate’ (FTER) means the proportion of registrations with insufficient quality of the biometric enrolment;

(30) ‘False Positive Identification Rate’ (FPIR) means the proportion of returned matches during a biometric search which do not belong to the checked traveller;

▼B

(31) ‘False Negative Identification Rate’ (FNIR) means the proportion of missed matches during a biometric search even though the traveller’s biometric data were registered;

▼M2

(32) ‘ESP’ means the European search portal established by Article 6(1) of Regulation (EU) 2019/817;

(33) ‘CIR’ means the common identity repository established by Article 17(1) of Regulation (EU) 2019/817.

▼B

2. The terms defined in Article 4 of Regulation (EU) 2016/679 shall have the same meaning in this Regulation in so far as personal data are processed by the authorities of Member States for the purposes laid down in Article 6(1) of this Regulation.

3. The terms defined in Article 3 of Directive (EU) 2016/680 shall have the same meaning in this Regulation in so far as personal data are processed by the authorities of the Member States for the purposes laid down in Article 6(2) of this Regulation.

Article 4

Borders at which the EES is operated and use of the EES at those borders

1. The EES shall be operated at the external borders.

2. The Member States which apply the Schengen *acquis* in full shall introduce the EES at their internal borders with Member States which do not yet apply the Schengen *acquis* in full but operate the EES.

3. The Member States which apply the Schengen *acquis* in full and the Member States which do not yet apply the Schengen *acquis* in full but operate the EES shall introduce the EES at their internal borders with the Member States which do not yet apply the Schengen *acquis* in full and do not operate the EES.

4. Member States which do not yet apply the Schengen *acquis* in full but operate the EES shall introduce the EES at their internal borders as defined under points (b) and (c) of Article 2(1) of Regulation (EU) 2016/399.

5. By way of derogation from the third and fourth subparagraphs of Article 23(2) and from Article 27, a Member State which does not yet apply the Schengen *acquis* in full but operates the EES shall introduce the EES without biometric functionalities at its internal land borders with a Member State which does not yet apply the Schengen *acquis* in full but operates the EES. Where, at those internal borders, a third-country national has not yet been registered in the EES, that third-country national’s individual file shall be created without recording biometric data. Biometric data shall be added at the next border crossing point where the EES is operated with biometric functionalities.

▼B

Article 5

Set-up of the EES

eu-LISA shall develop the EES and ensure its operational management, including the functionalities for processing biometric data as referred to in point (d) of Article 16(1) and points (b) and (c) of Article 17(1), as well as the adequate security of the EES.

Article 6

Objectives of the EES

1. By recording and storing data in the EES and by providing Member States with access to such data, the objectives of the EES shall be to:

(a) enhance the efficiency of border checks by calculating and monitoring the duration of the authorised stay on the entry and exit of third-country nationals admitted for a short stay;

(b) assist in the identification of third-country nationals who do not or no longer fulfil the conditions for entry to, or for short stay on, the territory of the Member States;

(c) allow the identification and detection of overstayers and enable the competent national authorities of the Member States to take appropriate measures;

(d) allow refusals of entry in the EES to be checked electronically;

(e) enable automation of border checks on third-country nationals;

(f) enable visa authorities to have access to information on the lawful use of previous visas;

(g) inform third-country nationals of the duration of their authorised stay;

(h) gather statistics on the entries and exits, refusals of entry and overstays of third-country nationals in order to improve the assessment of the risk of overstays and support evidence-based Union migration policy making;

(i) combat identity fraud and the misuse of travel documents;

▼M2

(j) ensure the correct identification of persons.

▼B

2. By granting access to designated authorities in accordance with the conditions set out in this Regulation, the objectives of the EES shall be to:

▼B

(a) contribute to the prevention, detection and investigation of terrorist offences or of other serious criminal offences;

(b) enable the generation of information for investigations related to terrorist offences or other serious criminal offences, including the identification of perpetrators, suspects and victims of those offences who have crossed the external borders.

3. The EES shall, where relevant, support Member States in operating their national facilitation programmes established in accordance with Article 8d of Regulation (EU) 2016/399, in order to facilitate border crossing for third-country nationals, by:

(a) enabling the national competent authorities referred to in Article 8d of Regulation (EU) 2016/399 to have access to information on previous short stays or refusals of entry for the purposes of the examination of applications for access to national facilitation programmes and the adoption of decisions referred to in Article 25 of this Regulation;

(b) notifying the border authorities that access is granted to a national facilitation programme.

Article 7

Technical architecture of the EES

1. The EES shall be composed of:

(a) a Central System (EES Central System);

▼M2

(aa) the CIR central infrastructure as referred to in point (a) of Article 17(2) of Regulation (EU) 2019/817;

▼B

(b) a National Uniform Interface (NUI) in each Member State based on common technical specifications and identical for all Member States, enabling the connection of the EES Central System to the national border infrastructures in Member States in a secure manner;

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

(d) a Communication Infrastructure, which shall be secure and encrypted, between the EES Central System and the NUIs;

(e) the web service referred to in Article 13;

▼M2

(f) a secure communication infrastructure between the EES Central System and the central infrastructures of the ESP and the CIR.

1a. The CIR shall contain the data referred to in points (a) to (d) of Article 16(1), points (a), (b) and (c) of Article 17(1) and Article 18(1) and (2). The remaining EES data shall be stored in the EES Central System.

▼B

2. The EES Central System shall be hosted by eu-LISA in its technical sites. It shall provide the functionalities laid down in this Regulation in accordance with the conditions of availability, quality and speed pursuant to Article 37(3).

▼B

3. Without prejudice to Commission Decision 2008/602/EC ([1]), certain hardware and software components of the Communication Infrastructure of the EES shall be shared with the communication infrastructure of the VIS referred to in Article 1(2) of Decision 2004/512/EC. Logical separation of VIS data and EES data shall be ensured.

Article 8

Interoperability with the VIS

1. eu-LISA shall establish a Secure Communication Channel between the EES Central System and the VIS Central System to enable interoperability between the EES and the VIS. Direct consultation between the EES and the VIS shall only be possible where provided for by both this Regulation and Regulation (EC) No 767/2008. The retrieval of visa-related data from the VIS, their importation into the EES and the updating of data from the VIS in the EES shall be an automated process once the operation in question is launched by the authority concerned.

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

(a) retrieve the visa-related data directly from the VIS and import them into the EES in order to create or update the entry/exit record or the refusal of entry record of a visa holder in the EES in accordance with Articles 14, 16 and 18 of this Regulation and Article 18a of Regulation (EC) No 767/2008;

(b) retrieve the visa-related data directly from the VIS and import them into the EES in order to update the entry/exit record in the event that a visa is annulled, revoked or extended in accordance with Article 19 of this Regulation and Articles 13, 14 and 18a of Regulation (EC) No 767/2008;

(c) verify, pursuant to Article 23 of this Regulation and Article 18(2) of Regulation (EC) No 767/2008, the authenticity and validity of the relevant visa or whether the conditions for entry to the territory of the Member States in accordance with Article 6 of Regulation (EU) 2016/399 are fulfilled;

(d) verify at the borders at which the EES is operated whether a visa-exempt third-country national has been previously registered in the VIS in accordance with Article 23 of this Regulation and Article 19a of Regulation (EC) No 767/2008; and

(e) where the identity of a visa holder is verified using fingerprints, verify at the borders at which the EES is operated the identity of a visa holder by comparing the fingerprints of the visa holder with the fingerprints recorded in the VIS in accordance with Article 23 of this Regulation and Article 18(6) of Regulation (EC) No 767/2008.

([1]) Commission Decision 2008/602/EC of 17 June 2008 laying down the physical architecture and requirements of the national interfaces and of the communication infrastructure between the central VIS and the national interfaces for the development phase (OJ L 194, 23.7.2008, p. 3).

▼B

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

(a) examine visa applications and adopt decisions relating to those applications in accordance with Article 24 of this Regulation and Article 15(4) of Regulation (EC) No 767/2008;

(b) examine, for the Member States which do not yet apply the Schengen *acquis* in full but operate the EES, applications for national short-stay visas and adopt decisions relating to those applications;

(c) update the visa-related data in the entry/exit record in the event that a visa is annulled, revoked or extended in accordance with Article 19 of this Regulation and Articles 13 and 14 of Regulation (EC) No 767/2008.

4. For the operation of the EES web service referred to in Article 13, the separate read-only database referred to in Article 13(5) shall be updated on a daily basis by the VIS via a one-way extraction of the minimum necessary subset of VIS data.

Article 9

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

1. Access to the EES for entering, amending, erasing and consulting the data referred to in Article 14 and Articles 16 to 20 shall be reserved exclusively for the duly authorised staff of the national authorities of each Member State which are competent for the purposes laid down in Articles 23 to 35. That access shall be limited to the extent necessary for the performance of the tasks of those national authorities in accordance with those purposes and shall be proportionate to the objectives pursued.

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

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

▼M2

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

▼B

Article 10

General principles

1. Each competent authority authorised to access the EES shall ensure that the use of the EES is necessary, appropriate and proportionate.

2. Each competent authority shall ensure that the use of the EES, including the capturing of biometric data, is in accordance with the safeguards laid down in the 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. In particular, when capturing a child's data, the best interests of the child shall be a primary consideration.

Article 11

Automated calculator and obligation to inform third-country nationals on the remaining authorised stay

1. The EES shall include an automated calculator that indicates the maximum duration of authorised stay for third-country nationals registered in the EES.

The automated calculator shall not apply to third-country nationals:

(a) who are members of the family of a Union citizen to whom Directive 2004/38/EC applies or of a national of a third country enjoying the right of free movement equivalent to that of Union citizens under an agreement between the Union and its Member States, on the one hand, and a third country, on the other; and

(b) who do not hold a residence card pursuant to Directive 2004/38/EC or a residence permit pursuant to Regulation (EC) No 1030/2002.

2. The automated calculator shall inform the competent authorities:

(a) on entry, of the maximum duration of authorised stay of third-country nationals and whether the number of authorised entries of a short-stay visa issued for one or two entries has been exhausted;

(b) during checks or verifications carried out within the territory of the Member States, of the remaining authorised stay or duration of overstay of the third-country nationals;

(c) on exit, of any overstay of third-country nationals;

(d) when examining and deciding on short-stay visa applications, of the maximum remaining duration of authorised stay based on intended entry dates.

▼B

3. The border authorities shall inform the third-country national of the maximum duration of authorised stay, which shall take into account the number of entries and the length of stay authorised by the visa in accordance with Article 8(9) of Regulation (EU) 2016/399. That information shall be provided either by the border guard at the moment of the border checks or by means of equipment installed at the border crossing point enabling the third-country national to consult the web service as referred to in Article 13(1) and (2) of this Regulation.

4. For third-country nationals subject to a visa requirement staying on the basis of a short-stay visa or a national short-stay visa in a Member State which does not yet apply the Schengen *acquis* in full but operates the EES, the automated calculator shall not indicate the authorised stay based on the short-stay visa or the national short-stay visa.

In the case referred to in the first subparagraph, the automated calculator shall only verify:

(a) compliance with the overall limit of 90 days in any 180-day period; and

(b) for short-stay visas, compliance with the period of validity of such visas.

5. For the purpose of verifying whether third-country nationals holding a short-stay visa issued for one or two entries have already used the number of entries authorised by their short-stay visa, the automated calculator shall only take into account entries into the territory of Member States which apply the Schengen *acquis* in full. That verification shall not be carried out, however, at the entry into the territory of Member States which do not yet apply the Schengen *acquis* in full but operate the EES.

6. The automated calculator shall also apply to short stays based on a short-stay visa with limited territorial validity issued pursuant to point (b) of Article 25(1) of Regulation (EC) No 810/2009. In that case, the automated calculator shall take into account the authorised stay as defined by such a visa, irrespective of whether the cumulative stay of the third-country national concerned exceeds 90 days in any 180-day period.

Article 12

Information mechanism

1. The EES shall include a mechanism that shall automatically identify which entry/exit records do not have exit data immediately following the date of expiry of an authorised stay and automatically identify records for which the maximum duration of authorised stay was exceeded.

▼B

2. For third-country nationals who cross a border on the basis of a valid Facilitated Transit Document issued in accordance with Council Regulation (EC) No 693/2003 ([1]) (FTD), the EES shall include a mechanism which shall automatically identify which entry/exit records do not have exit data immediately following the time of expiry of authorised stay and automatically identify records ►C1 for which the maximum duration of authorised stay was exceeded. ◄

3. A list generated by the EES containing the data referred to in Articles 16 and 17 of all persons identified as overstayers shall be available to the competent national authorities designated in accordance with Article 9(2) in order to enable those authorities to adopt appropriate measures.

Article 13

Web service

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

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

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

3. In order to fulfil their obligation under point (b) of Article 26(1) of the Convention implementing the Schengen Agreement, carriers shall use the web service to verify whether third-country nationals holding a short-stay visa issued for one or two entries have already used the number of entries authorised by their visa. 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

([1]) Council Regulation (EC) No 693/2003 of 14 April 2003 establishing a specific Facilitated Transit Document (FTD), a Facilitated Rail Transit Document (FRTD) and amending the Common Consular Instructions and the Common Manual (OJ L 99, 17.4.2003, p. 8).

▼B

OK/NOT OK answer. Carriers may store the information sent and the answer received in accordance with the applicable law. Carriers shall establish an authentication scheme to ensure that only authorised staff may access the web service. It shall not be possible to regard the OK/NOT OK answer as a decision to authorise or refuse entry in accordance with Regulation (EU) 2016/399.

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

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

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

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

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

CHAPTER II

ENTRY AND USE OF DATA BY COMPETENT AUTHORITIES

Article 14

Procedures for entering data in the EES

1. Border authorities shall verify, in accordance with Article 23, whether a previous individual file has been created in the EES for the third-country national as well as his or her identity. Where a third-country national uses a self-service system for the pre-enrolment of data or for the carrying out of border checks, the verification shall be carried out through the self-service system.

▼B

2. Where a previous individual file has been created for the third-country national, the border authority shall, where necessary:

(a) update that individual file, namely the data referred to in Articles 16, 17 and 18, as applicable, and

(b) enter an entry record for each entry and an exit record for each exit in accordance with Articles 16 and 17 or, where applicable, a refusal of entry record in accordance with Article 18.

The records referred to in point (b) of the first subparagraph of this paragraph shall be linked to the individual file of the third-country national concerned.

Where applicable, the data referred to in Article 19(1), (2), (4) and (5) shall be added to the entry/exit record of the third-country national concerned. The travel documents and identities used legitimately by a third-country national shall be added to the third-country national's individual file.

Where a previous individual file is recorded and the third-country national presents a valid travel document which differs from the one that was previously recorded, the data referred to in point (d) of Article 16(1) and point (b) of Article 17(1) shall also be updated in accordance with Article 15.

3. Where it is necessary to enter or update the entry/exit record data of a visa holder, the border authorities may retrieve from the VIS and import into the EES the data provided for in points (c) to (f) of Article 16(2) of this Regulation in accordance with Article 8 of this Regulation and Article 18a of Regulation (EC) No 767/2008.

4. In the absence of a previous registration of a third-country national in the EES, the border authority shall create an individual file of that third-country national by entering the data referred to in Articles 16(1) and (6), 17(1) and 18(1) as applicable.

5. Where a third-country national uses a self-service system for the pre-enrolment of data, Article 8a of Regulation (EU) 2016/399 shall apply. In that case, the third-country national may pre-enrol the individual file data or, if applicable, the data in the entry/exit record that need to be updated. The data shall be confirmed by the border authorities when the decision to authorise or to refuse entry has been taken in accordance with Regulation (EU) 2016/399. The data listed in points (c) to (f) of Article 16(2) of this Regulation may be retrieved from the VIS and imported into the EES.

6. Where a third-country national uses a self-service system for the carrying out of the border checks, Article 8b of Regulation (EU) 2016/399 shall apply. In that case, the verification referred to in paragraph 1 of this Article shall be carried out through the self-service system.

7. Where a third-country national uses an e-gate for crossing the external borders or the internal borders where controls have not yet been lifted, Article 8b of Regulation (EU) 2016/399 shall apply. In that case, the corresponding registration of the entry/exit record and the linking of that record to the individual file concerned shall be carried out through the e-gate.

▼B

8. Without prejudice to Article 20 of this Regulation and Article 12(3) of Regulation (EU) 2016/399, where the short stay of a third-country national who is present on the territory of a Member State starts directly after a stay based on a residence permit or a long-stay visa and no previous individual file has been created, that third-country national may request the competent authorities referred to in Article 9(2) of this Regulation to create an individual file and an entry/exit record by entering the data referred to in Articles 16(1), (2) and (6) and 17(1) of this Regulation. Instead of the data referred to in point (a) of Article 16(2) of this Regulation, those competent authorities shall insert the date of the start of the short stay and, instead of the data referred to in point (b) of Article 16(2) of this Regulation, they shall insert the name of the authority that inserted those data.

Article 15

Facial image of third-country nationals

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.

2. By way of derogation from paragraph 1, in exceptional cases where the quality and resolution specifications set for the enrolment of the live facial image in the EES cannot be met, the facial image may be extracted electronically from the chip of the electronic Machine Readable Travel Document (eMRTD). In such cases, the facial image shall only be inserted into the individual file after electronic verification that the facial image recorded in the chip of the eMRTD corresponds to the live facial image of the third-country national concerned.

3. Each Member State shall transmit once a year a report on the application of paragraph 2 to the Commission. That report shall include the number of third-country nationals concerned, as well as an explanation of the exceptional cases faced.

4. The facial image of third-country nationals shall have sufficient image resolution and quality to be used in automated biometric matching.

5. Within a period of two years following the start of operations of the EES, the Commission shall produce a report on the quality standards of facial images stored in the VIS and on whether they are such that they enable biometric matching with a view to using facial images stored in the VIS at borders and within the territory of the Member States for the verification of the identity of third-country nationals subject to a visa requirement, without storing such facial images in the EES. The Commission shall transmit that report to the European Parliament and to the Council. That report shall be accompanied, where considered appropriate by the Commission, by legislative proposals, including proposals to amend this Regulation, Regulation (EC) No 767/2008, or both, as regards the use of the facial images of third-country nationals stored in the VIS for the purposes referred to in this paragraph.

▼B

Article 16

Personal data of third-country nationals subject to a visa requirement

1. At the borders at which the EES is operated, the border authority shall create the individual file of a third-country national subject to a visa requirement by entering the following data:

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

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

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

(d) the facial image as referred to in Article 15.

2. On each entry of a third-country national subject to a visa requirement at a border at which the EES is operated, the following data shall be entered in an entry/exit record:

(a) the date and time of the entry;

(b) the border crossing point of the entry and the authority that authorised the entry;

(c) where applicable, the status of that third-country national indicating that he or she is a third-country national who:

(i) is a member of the family of a Union citizen to whom Directive 2004/38/EC applies or of a national of a third country enjoying the right of free movement equivalent to that of Union citizens under an agreement between the Union and its Member States, on the one hand, and a third country, on the other; and

(ii) does not hold a residence card pursuant to Directive 2004/38/EC or a residence permit pursuant to Regulation (EC) No 1030/2002;

▼C1

(d) where applicable, the short-stay visa sticker number, including the three letter code of the issuing Member State, the type of short-stay visa, the end date of the maximum duration of the stay as authorised by the short-stay visa, which shall be updated at each entry, and the date of expiry of the validity of the short-stay visa;

▼B

(e) on the first entry on the basis of a short-stay visa, the number of entries and the duration of stay authorised by the short-stay visa as indicated on the short-stay visa sticker;

(f) where applicable, the information indicating that the short-stay visa has been issued with limited territorial validity pursuant to point (b) of Article 25(1) of Regulation (EC) No 810/2009;

(g) for the Member States which do not yet apply the Schengen *acquis* in full but operate the EES, a notification, where applicable, indicating that the third-country national used a national short-stay visa for the entry.

▼B

The entry/exit record referred to in the first subparagraph shall be linked to the individual file of that third-country national using the individual reference number created by the EES upon creation of that individual file.

3. On each exit of a third-country national subject to a visa requirement at a border at which the EES is operated, the following data shall be entered in the entry/exit record:

(a) the date and time of the exit;

(b) the border crossing point of the exit.

Where that third-country national uses a visa other than the visa recorded in the last entry record, the data of the entry/exit record listed in points (d) to (g) of paragraph 2 shall be updated accordingly.

The entry/exit record referred to in the first subparagraph shall be linked to the individual file of that third-country national.

4. Where there is no exit data immediately following the date of expiry of the authorised stay, the entry/exit record shall be identified with a flag by the EES and the data of the third-country national subject to a visa requirement, who has been identified as an overstayer, shall be entered into the list referred to in Article 12.

5. In order to enter or update the entry/exit record of a third-country national subject to a visa requirement, the data provided for in points (c) to (f) of paragraph 2 of this Article may be retrieved from the VIS and imported into the EES by the border authority in accordance with Article 18a of Regulation (EC) No 767/2008.

6. Where a third-country national benefits from the national facilitation programme of a Member State in accordance with Article 8d of Regulation (EU) 2016/399, the Member State concerned shall insert a notification in the individual file of that third-country national specifying the national facilitation programme of the Member State concerned.

7. The specific provisions set out in Annex II shall apply to third-country nationals who cross the border on the basis of a valid FTD.

Article 17

Personal data of visa-exempt third-country nationals

1. The border authority shall create the individual file of visa-exempt third-country nationals by entering the following:

▼B

(a) the data provided for in points (a), (b) and (c) of Article 16(1);

(b) the facial image as referred to in Article 15;

(c) fingerprint data from the right hand, where present, and otherwise the corresponding fingerprint data from the left hand; fingerprint data shall have sufficient resolution and quality to be used in automated biometric matching;

(d) where relevant, the data provided for in Article 16(6).

2. For visa-exempt third-country nationals, points (a), (b) and (c) of Article 16(2), points (a) and (b) of Article 16(3) and Article 16(4) shall apply *mutatis mutandis*.

3. Children under the age of 12 shall be exempt from the requirement to give fingerprints.

4. Persons for whom fingerprinting is physically impossible shall be exempt from the requirement to give fingerprints.

However, where the physical impossibility is of a temporary nature, that fact shall be recorded in the EES and the person shall be required to give the fingerprints on exit or at the subsequent entry. This information shall be deleted from the EES once the fingerprints have been given. The border authorities shall be entitled to request further clarification on the grounds for the temporary impossibility to give fingerprints. Member States shall ensure that appropriate procedures guaranteeing the dignity of the person are in place in the event of difficulties encountered in the capturing of fingerprints.

5. Where the person concerned is exempt from the requirement to give fingerprints pursuant to paragraphs 3 or 4, the specific data field shall be marked as ‘not applicable’.

Article 18

Personal data of third-country nationals who have been refused entry

1. Where a decision has been taken by the border authority, in accordance with Article 14 of and Annex V to Regulation (EU) 2016/399, to refuse the entry of a third-country national for a short stay on the territory of the Member States and where no previous file is recorded in the EES for that third-country national, the border authority shall create an individual file in which it shall enter:

(a) for third-country nationals subject to a visa requirement, the alpha-numeric data required pursuant to Article 16(1) of this Regulation and, where relevant, the data referred to in Article 16(6) of this Regulation;

▼B

(b) for visa-exempt third-country nationals, the alphanumeric data required pursuant to Article 17(1) of this Regulation.

2. Where the third-country national is refused entry on the basis of a reason corresponding to point B, D or H of Part B of Annex V to Regulation (EU) 2016/399 and where no previous file with biometric data is recorded in the EES for that third-country national, the border authority shall create an individual file in which it shall enter the alphanumeric data required pursuant to Article 16(1) or Article 17(1) of this Regulation, as appropriate, as well as the following data:

(a) for third-country nationals subject to a visa requirement, the facial image referred to in point (d) of Article 16(1) of this Regulation;

(b) for visa-exempt third-country nationals, the biometric data required pursuant to points (b) and (c) of Article 17(1) of this Regulation;

(c) for third-country nationals subject to a visa requirement who are not registered in the VIS, the facial image referred to in point (d) of Article 16(1) of this Regulation and the fingerprint data as referred to point (c) of Article 17(1) of this Regulation.

3. By way of derogation from paragraph 2 of this Article, where the reason corresponding to point H of Part B of Annex V to Regulation (EU) 2016/399 applies and the biometric data of the third-country national are recorded in the SIS alert that results in the refusal of entry, the biometric data of the third-country national shall not be entered in the EES.

4. Where the third-country national is refused entry on the basis of a reason corresponding to point I of Part B of Annex V to Regulation (EU) 2016/399 and where no previous file with biometric data is recorded in the EES for that third-country national, the biometric data shall only be entered in the EES where the entry is refused because the third-country national is considered to be a threat to internal security, including, where appropriate, elements of public policy.

5. Where a third-country national is refused entry on the basis of a reason corresponding to point J of Part B of Annex V to Regulation (EU) 2016/399, the border authority shall create the individual file of that third-country national without adding biometric data. If the third-country national possesses an eMRTD, the facial image shall be extracted from that eMRTD.

6. Where a decision has been taken by the border authority, in accordance with Article 14 of and Annex V to Regulation (EU) 2016/399, to refuse the entry of a third-country national for a short stay to the territory of the Member States, the following data shall be entered in a separate refusal of entry record:

(a) the date and time of refusal of entry;

(b) the border crossing point;

(c) the authority that refused the entry;

(d) the point or points corresponding to the reasons for refusing entry in accordance with Part B of Annex V to Regulation (EU) 2016/399.

▼B

In addition, for third-country nationals subject to a visa requirement, the data provided for in points (d) to (g) of Article 16(2) of this Regulation shall be entered in the refusal of entry record.

In order to create or update the refusal of entry record of third-country nationals subject to a visa requirement, the data provided for in points (d), (e) and (f) of Article 16(2) of this Regulation may be retrieved from the VIS and imported into the EES by the competent border authority in accordance with Article 18a of Regulation (EC) No 767/2008.

7. The refusal of entry record provided for in paragraph 6 shall be linked to the individual file of the third-country national concerned.

Article 19

Data to be added where an authorisation for short stay is revoked, annulled or extended

1. Where a decision has been taken to revoke or annul an authorisation for short stay or a visa or to extend the duration of an authorised stay or visa, the competent authority that has taken such a decision shall add the following data to the latest relevant entry/exit record:

(a) the status information indicating that the authorisation for short stay or the visa has been revoked or annulled or that the duration of the authorised stay or the visa has been extended;

(b) the identity of the authority that revoked or annulled the authorisation for short stay or the visa or extended the duration of the authorised stay or the visa;

(c) the place and date of the decision to revoke or annul the authorisation for short stay or the visa or to extend the duration of the authorised stay or the visa;

(d) where applicable, the new visa sticker number, including the three letter code of the issuing country;

(e) where applicable, the period of the extension of the duration of authorised stay;

(f) where applicable, the new expiry date of the authorised stay or the visa.

2. Where the duration of authorised stay has been extended in accordance with Article 20(2) of the Convention implementing the Schengen Agreement, the competent authority that extended the authorised stay shall add the data regarding the period of extension of the authorised stay to the latest relevant entry/exit record and, where applicable, an indication that the authorised stay was extended in accordance with point (b) of Article 20(2) of the Convention implementing the Schengen Agreement.

3. Where a decision has been taken to annul, revoke or extend a visa, the visa authority which has taken the decision shall immediately retrieve the data provided for in paragraph 1 of this Article from the VIS and import them directly into the EES in accordance with Articles 13 and 14 of Regulation (EC) No 767/2008.

▼B

4. The entry/exit record shall indicate the grounds for revocation or annulment of the short stay, which shall be:

(a) a return decision adopted pursuant to Directive 2008/115/EC of the European Parliament and of the Council ([1]);

(b) any other decision taken by the competent authorities of the Member State, in accordance with national law, resulting in the return, removal or voluntary departure of a third-country national who does not fulfil or no longer fulfils the conditions for the entry into or for the stay on the territory of the Member States.

5. The entry/exit record shall indicate the grounds for extending the duration of an authorised stay.

6. When a person has departed or has been removed from the territory of the Member States pursuant to a decision as referred to in paragraph 4 of this Article, the competent authority shall enter the data in accordance with Article 14(2) in the related entry/exit record of that specific entry.

Article 20

Data to be added in case of rebuttal of the presumption that a third-country national does not fulfil the conditions of duration of authorised stay

Without prejudice to Article 22, where no individual file has been created in the EES for a third-country national present on the territory of a Member State or where there is no last relevant entry/exit record for such a third-country national, the competent authorities may presume that the third-country national does not fulfil or no longer fulfils the conditions relating to duration of authorised stay within the territory of the Member States.

In the case referred to in the first paragraph of this Article, Article 12 of Regulation (EU) 2016/399 shall apply and, if the presumption is rebutted in accordance with Article 12(3) of that Regulation, the competent authorities shall:

(a) create an individual file for that third-country national in the EES, if necessary;

(b) update the latest entry/exit record by entering the missing data in accordance with Articles 16 and 17 of this Regulation; or

(c) erase an existing file where Article 35 of this Regulation provides for such erasure.

Article 21

Fall-back procedures where it is technically impossible to enter data or in the event of failure of the EES

▼M2

1. Where it is technically impossible to enter data in the EES Central System or the CIR or in the event of a failure of the EES Central System or the CIR, the data referred to in Articles 16 to 20 shall be temporarily stored in the NUI. Where that is not possible, the data shall be temporarily stored locally in an electronic format. In both cases, the

([1]) 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).

▼M2

data shall be entered in the EES Central System or the CIR as soon as the technical impossibility or failure has been remedied. The Member States shall take the appropriate measures and deploy the required infrastructure, equipment and resources to ensure that such temporary local storage may be carried out at any time and for any of their border crossing points.

2. Without prejudice to the obligation to carry out border checks under Regulation (EU) 2016/399, the border authority, in the exceptional situation where it is technically impossible to enter data in either the EES Central System and the CIR or in the NUI and it is technically impossible to temporarily store the data locally in an electronic format, shall manually store the data referred to in Articles 16 to 20 of this Regulation, with the exception of biometric data, and shall affix an entry or exit stamp in the travel document of the third-country national. That data shall be entered in the EES Central System and the CIR as soon as technically possible.

▼B

Member States shall inform the Commission of the stamping of travel documents in the event of the exceptional situations referred to in the first subparagraph of this paragraph. The Commission shall adopt implementing acts concerning the detailed rules on the information to be provided to the Commission. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 68(2).

3. The EES shall indicate that data referred to in Articles 16 to 20 were entered as a result of a fall-back procedure and that the individual file created pursuant to paragraph 2 of this Article is missing biometric data. The biometric data shall be entered in the EES at the next border crossing.

Article 22

Transitional period and transitional measures

1. For a period of 180 days after the EES has started operations, in order to verify, on entry and exit, that third-country nationals admitted for a short stay have not exceeded the maximum duration of authorised stay and, where relevant, to verify on entry that third-country nationals have not exceeded the number of entries authorised by the short-stay visa issued for one or two entries, the competent border authorities shall take into account the stays in the territory of the Member States during the 180 days preceding the entry or the exit by checking the stamps in the travel documents in addition to the entry/exit data recorded in the EES.

2. Where a third-country national has entered the territory of the Member States before the EES has started operations and exits it after the EES has started operations, an individual file shall be created on exit and the date of entry as stamped in the passport shall be entered in the entry/exit record in accordance with Article 16(2). This rule shall not be limited to the 180 days after the EES has started operations as referred to in paragraph 1 of this Article. In case of a discrepancy between the entry stamp and the EES data, the stamp shall prevail.

▼B

Article 23

Use of data for verification at the borders at which the EES is operated

1. Border authorities shall have access to the EES for verifying the identity and previous registration of the third-country national, for updating the EES data where necessary and for consulting the data to the extent required for the carrying out of border checks.

2. While performing the tasks referred to in paragraph 1 of this Article, the border authorities shall have access to search with the data referred to in points (a), (b) and (c) of Article 16(1) and point (a) of Article 17(1).

In addition, for the purposes of consulting the VIS for verification in accordance with Article 18 of Regulation (EC) No 767/2008, for third-country nationals who are subject to a visa requirement, the border authorities shall launch a search in the VIS directly from the EES using the same alphanumeric data or, where applicable, ►C1 consult the VIS in accordance with Article 18(3) of Regulation (EC) No 767/2008. ◄

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 compare the live facial image of the third-country national with the facial image referred to in point (d) of Article 16(1) and point (b) of Article 17(1) of this Regulation or the border authorities shall, in the case of visa-exempt third-country nationals, proceed to a verification of fingerprints against the EES and, in the case of third-country nationals subject to a visa requirement, 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 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 that Regulation.

If the verification of the facial image fails, the verification shall be carried out using fingerprints and vice versa.

▼M2

2a. For the purpose of the verifications in accordance with paragraph 1 of this Article, the border authority shall launch a query by using the ESP to compare the data on the third-country national with the relevant data in the EES and the VIS.

▼B

3. If the search with the data set out in paragraph 2 indicates that data on the third-country national are recorded in the EES, the border authority shall be given access to consult the data of the individual file of that third-country national and the entry/exit record or records or refusal of entry record or records linked to it.

▼M2

4. Where the search with the alphanumeric data set out in paragraph 2 of this Article indicates that data on the third-country national are not recorded in the EES, where a verification of the third-country national pursuant to paragraph 2 of this Article fails or where there are doubts as

▼M2

to the identity of the third-country national, the border authorities shall have access to data for identification in accordance with Article 27 in order to create or update an individual file in accordance with Article 14.

▼B

In addition to the identification referred to in first subparagraph of this paragraph, the following provisions shall apply:

(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 against the VIS shall be carried out in accordance with Article 18(5) of Regulation (EC) No 767/2008. For this purpose, the border authority may launch a search from the EES to the VIS as provided for in Article 18(6) 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.

(b) for third-country nationals who are not subject to a visa requirement and for whom no data are found in the EES further to the identification run in accordance with Article 27 of this Regulation, the VIS shall be consulted in accordance with Article 19a of Regulation (EC) No 767/2008. The border authority may launch a search from the EES to the VIS as provided for in Article 19a of Regulation (EC) No 767/2008.

5. For third-country nationals whose data are already recorded in the EES but whose individual file was created in the EES by a Member State which does not yet apply the Schengen *acquis* in full but operates the EES and whose data were entered in the EES on the basis of a national short-stay visa, the border authorities shall consult the VIS in accordance with point (a) of the second subparagraph of paragraph 4 when, for the first time after the creation of the individual file, the third-country national intends to cross the border of a Member State which applies the Schengen *acquis* in full and operates the EES.

CHAPTER III

USE OF THE EES BY OTHER AUTHORITIES

Article 24

Use of the EES for examining and deciding on visas

1. Visa authorities shall consult the EES for examining visa applications and adopting decisions relating to those applications, including decisions to annul, revoke or extend the period of validity of an issued visa, in accordance with Regulation (EC) No 810/2009.

In addition, visa authorities of a Member State which does not yet apply the Schengen *acquis* in full but operates the EES shall consult the EES when examining national short-stay visa applications and adopting decisions relating to those applications, including decisions to annul, revoke or extend the period of validity of an issued national short-stay visa.

▼B

2. Visa authorities shall be given access to search the EES directly from the VIS with one or several of the following data:

(a) the data referred to in points (a), (b) and (c) of Article 16(1);

(b) the short-stay visa sticker number, including the three letter code of the issuing Member State referred to in point (d) of Article 16(2);

(c) the fingerprint data or the fingerprint data combined with the facial image.

3. If the search with the data set out in paragraph 2 indicates that data on the third-country national are recorded in the EES, visa authorities shall be given access to consult the data of the individual file of that third-country national and the entry/exit records, as well as any refusal of entry records linked to that individual file. Visa authorities shall be given access to consult the automated calculator in order to check the maximum remaining duration of an authorised stay. Visa authorities shall also be given access to consult the EES and the automated calculator when examining and taking decisions on new visa applications, so as to automatically establish the maximum duration of authorised stay.

4. Visa authorities of a Member State which does not yet apply the Schengen *acquis* in full but operates the EES shall be given access to search the EES with one or several of the data set out in paragraph 2. If the search indicates that data on the third-country national are recorded in the EES, they shall be given access to consult the data of the individual file of that third-country national and the entry/exit records, as well as any refusal of entry records linked to that individual file. Visa authorities of a Member State which does not yet apply the Schengen *acquis* in full but operates the EES shall be given access to consult the automated calculator in order to establish the maximum remaining duration of an authorised stay. Visa authorities shall also be given access to consult the EES and the automated calculator when examining and taking decisions on new visa applications, so as to establish the maximum duration of authorised stay.

Article 25

Use of the EES for examining applications for access to national facilitation programmes

1. The competent authorities referred to in Article 8d of Regulation (EU) 2016/399 shall consult the EES for the purposes of the examination of applications for access to national facilitation programmes referred to in that Article and the adoption of decisions relating to those applications, including decisions to refuse, revoke or extend the period of validity of access to the national facilitation programmes in accordance with that Article.

2. The competent authorities shall be given access to search with one or several of the following:

(a) the data referred to in points (a), (b) and (c) of Article 16(1) or the data referred to in point (a) of Article 17(1);

(b) the fingerprint data or the fingerprint data combined with the facial image.

▼B

3. If the search with the data set out in paragraph 2 indicates that data on the third-country national are recorded in the EES, the competent authority shall be given access to consult the data of the individual file of that third-country national and the entry/exit records, as well as any refusal of entry records linked to that individual file.

Article 26

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

1. For the purpose of verifying the identity of the third-country national, or checking or verifying whether the conditions for entry to, or stay on, the territory of the Member States are fulfilled, or both, the immigration authorities of the Member States shall have access to search with the data referred to in points (a), (b) and (c) of Article 16(1) and point (a) of Article 17(1).

If the search indicates that data on the third-country national are recorded in the EES, the immigration authorities may:

(a) compare the live facial image of the third-country national with the facial image referred to in point (d) of Article 16(1) and point (b) of Article 17(1) of this Regulation; or

(b) verify the fingerprints of visa-exempt third-country nationals in the EES and of third-country nationals subject to a visa requirement in the VIS in accordance with Article 19 of Regulation (EC) No 767/2008.

2. If the search with the data set out in paragraph 1 indicates that data on the third-country national are recorded in the EES, the immigration authorities shall be given access to consult the automated calculator, the data of the individual file of that third-country national, the entry/exit record or records and any refusal of entry record linked to that individual file.

3. Where the search with the data set out in paragraph 1 of this Article indicates that data on the third-country national are not recorded in the EES, where verification of the third-country national fails or where there are doubts as to the identity of the third-country national, the immigration authorities shall have access to data for identification in accordance with Article 27.

Article 27

Access to data for identification

1. The border authorities or immigration authorities shall have access to search with the fingerprint data or the fingerprint data combined with the facial image, for the sole purpose of identifying any third-country national who may have been registered previously in the EES under a different identity or who does not fulfil or no longer fulfils the conditions for entry to, or for stay on, the territory of the Member States.

▼B

Where the search with the fingerprint data or with the fingerprint data combined with the facial image indicates that data on that third-country national are not recorded in the EES, access to data for identification shall be carried out in the VIS in accordance with Article 20 of Regulation (EC) No 767/2008. At borders at which the EES is operated, prior to any identification against the VIS, the competent authorities shall first access the VIS in accordance with Articles 18 or 19a of Regulation (EC) No 767/2008.

Where the fingerprints of that third-country national cannot be used or the search with the fingerprint data or with the fingerprint data combined with the facial image has failed, the search shall be carried out with all or some of the data referred to in points (a), (b) and (c) of Article 16(1) and point (a) of Article 17(1).

2. If the search with the data set out in paragraph 1 indicates that data on the third-country national are recorded in the EES, the competent authority shall be given access to consult the data of the individual file and the entry/exit records and refusal of entry records linked to it.

Article 28

Keeping of data retrieved from the EES

Data retrieved from the EES pursuant to this Chapter may be kept in national files only where necessary in an individual case, in accordance with the purpose for which they were retrieved and with relevant Union law, in particular on data protection, and for no longer than strictly necessary in that individual case.

CHAPTER IV

PROCEDURE AND CONDITIONS FOR ACCESS TO THE EES FOR LAW ENFORCEMENT PURPOSES

Article 29

Member States' designated authorities

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

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

3. Each Member State shall designate a central access point which shall have access to the EES. The central access point shall verify that the conditions to request access to the EES laid down in Article 32 are fulfilled.

▼B

The designated authority 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 carry out independently.

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

4. Member States shall notify eu-LISA and the Commission of their central access points and may at any time amend or replace their notifications.

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 EES data through the central access points.

6. Only duly empowered staff of the central access points shall be authorised to access the EES in accordance with Articles 31 and 32.

Article 30

Europol

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

2. Europol shall designate a specialised unit with duly empowered Europol officials as the Europol central access point. The Europol central access point shall verify that the conditions to request access to the EES laid down in Article 33 are fulfilled.

The Europol 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 31

Procedure for access to the EES for law enforcement purposes

1. An operating unit as referred to in Article 29(5) shall submit a reasoned electronic or written request to a central access point as referred to in Article 29(3) for access to EES data. Upon receipt of a request for access, such a central access point shall verify whether the conditions for access referred to in Article 32 are fulfilled. If the conditions for access are fulfilled, such a central access point shall process the request. The EES data accessed shall be transmitted to an operating unit as referred to in Article 29(5) in such a way that the security of the data is not compromised.

▼B

2. In a case of urgency, where there is a need to prevent an imminent danger to the life of a person associated with a terrorist offence or another serious criminal offence, a central access point as referred to in Article 29(3) shall process the request immediately and shall only verify *ex post* whether all the conditions referred to in Article 32 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 determines that the access to EES data was not justified, all the authorities that accessed such data shall erase the information accessed from the EES and shall inform the relevant central access point of the Member State in which the request was made of the erasure.

Article 32

Conditions for access to EES data by designated authorities

1. Designated authorities may access the EES for consultation where all of the following conditions are met:

(a) access for consultation is necessary for the purpose of the prevention, detection ►C1 or investigation of a terrorist offence or another serious criminal offence; ◄

(b) access for consultation is necessary and proportionate in a specific case;

(c) evidence or reasonable grounds exist to consider that the consultation of the EES data will 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.

▼M2

1a. In cases where the designated authorities have launched a query of the CIR in accordance with Article 22 of Regulation (EU) 2019/817, they may access the EES for consultation where the conditions laid down in this Article are met and where the reply received as referred to in Article 22(2) of Regulation (EU) 2019/817 reveals that data are stored in the EES.

▼B

2. Access to the EES as a tool for the purpose of identifying an unknown suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence shall be allowed where, in addition to the conditions listed in paragraph 1, the following conditions are met:

(a) a prior search has been conducted in national databases; and

(b) in the case of searches with fingerprints, a prior search has been launched in the automated fingerprint identification system of the other Member States under Decision 2008/615/JHA where comparisons of fingerprints are technically available, and either that search has been fully carried out, or that search has not been fully carried out within two days of being launched.

▼B

However, the additional conditions in points (a) and (b) of the first subparagraph shall not apply where there are reasonable grounds to believe that a comparison with the systems of the other Member States would not lead to the verification of the identity of the data subject or in a case of urgency where there is a need to prevent an imminent danger to the life of a person associated with a terrorist offence or another serious criminal offence. Those reasonable grounds shall be included in the electronic or written request sent by the operating unit of the designated authority to the central access point.

A request for consultation of the VIS on the same data subject may be submitted in parallel to a request for consultation of the EES in accordance with the conditions laid down in Council Decision 2008/633/JHA ([1]).

3. Access to the EES as a tool to consult the travel history or the periods of 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 shall be allowed when the conditions listed in paragraph 1 are met.

4. Consultation of the EES for the purpose of identification as referred to in paragraph 2 shall be limited to searching in the individual file with any of the following EES data:

(a) fingerprints of visa-exempt third-country nationals or of holders of an FTD. In order to launch this consultation of the EES, latent fingerprints may be used and may therefore be compared with the fingerprints stored in the EES;

(b) facial images.

Consultation of the EES, in the event of a hit, shall give access to any other data taken from the individual file as listed in Article 16(1) and (6), Article 17(1) and Article 18(1).

5. Consultation of the EES for the travel history of the third-country national concerned shall be limited to searching with one or several of the following EES data in the individual file, in the entry/exit records or in the refusal of entry records:

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

(b) type and number of travel document or documents, three letter code of the issuing country and date of expiry of the validity of the travel document;

(c) visa sticker number and the date of expiry of the validity of the visa;

(d) fingerprints, including latent fingerprints;

([1]) 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).

▼B

(e) facial image;

(f) date and time of entry, authority that authorised the entry and entry border crossing point;

(g) date and time of exit and exit border crossing point.

Consultation of the EES shall, in the event of a hit, give access to the data listed in the first subparagraph as well as to any other data taken from the individual file, the entry/exit records and refusal of entry records, including data related to the revocation or extension of an authorisation for short stay in accordance with Article 19.

Article 33

Procedure and conditions for access to EES data by Europol

1. Europol shall have access to consult the EES where all the following conditions are met:

(a) the consultation is necessary to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences falling under Europol's mandate;

(b) the consultation is necessary and proportionate in a specific case;

(c) evidence or reasonable grounds exist to consider that the consultation of the EES data will 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.

▼M2

1a. In cases where Europol has launched a query of the CIR in accordance with Article 22 of Regulation (EU) 2019/817, it may access the EES for consultation where the conditions laid down in this Article are met and where the reply received as referred to in Article 22(2) of Regulation (EU) 2019/817 reveals that data are stored in the EES.

▼B

2. Access to the EES as a tool for the purpose of identifying an unknown suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence shall be allowed where the conditions listed in paragraph 1 are met and the consultation, as a matter of priority, of the data stored in the databases that are technically and legally accessible by Europol has not made it possible to identify the person in question.

A request for consultation of the VIS on the same data subject may be submitted in parallel to a request for consultation of the EES in accordance with the conditions laid down in Decision 2008/633/JHA.

3. The conditions laid down in Article 32(3), (4) and (5) shall apply accordingly.

▼B

4. The Europol designated authority may submit a reasoned electronic request for the consultation of all EES data or a specific set of EES data to the Europol central access point referred to in Article 30(2). Upon receipt of a request for access, the Europol central access point shall verify whether the conditions for access set out in paragraphs 1 and 2 of this Article are fulfilled. If all conditions for access are fulfilled, the duly authorised staff of the Europol central access point shall process the requests. The EES data accessed shall be transmitted to the Europol designated authority in such a way that the security of the data is not compromised.

5. Europol shall only process information obtained from a consultation of EES data subject to the authorisation of the Member State of origin. That authorisation shall be obtained via the Europol national unit of that Member State.

CHAPTER V

RETENTION AND AMENDMENT OF THE DATA

Article 34

Data retention period

1. Each entry/exit record or refusal of entry record linked to an individual file shall be stored ►**M2** in the CIR and in the EES Central System ◄ for three years following the date of the exit record or of the refusal of entry record, as applicable.

2. Each individual file together with the linked entry/exit record or records or refusal of entry records shall be stored ►**M2** in the CIR and in the EES Central System ◄ for three years and one day following the date of the last exit record or of the refusal of entry record if there is no entry record within three years from the date of the last exit record or refusal of entry record.

3. If there is no exit record following the date of expiry of the period of authorised stay, the data shall be stored for a period of five years following the date of expiry of the period of authorised stay. The EES shall automatically inform the Member States three months in advance of the scheduled erasure of data on overstayers in order to enable them to adopt the appropriate measures.

4. By way of derogation from paragraph 1, each entry/exit record registered for third-country nationals who have the status referred to in point (b) of Article 2(1) shall be stored in the EES for a maximum of one year after the exit of such third-country nationals. If there is no exit record the data shall be stored for a period of five years from the date of the last entry record.

5. Upon expiry of the retention period referred to in paragraphs 1 to 4, the data in question shall automatically be erased ►**M2** from the EES Central System and from the CIR ◄.

▼B

Article 35

Amendment of data and advance data erasure

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

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

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

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

5. The data of identified persons referred to in Article 12 shall be erased without delay from the list referred to in that Article and shall be rectified or completed in the EES where the third-country national concerned provides evidence, in accordance with the national law of the Member State responsible or of the Member State to which the request has been made, that he or she was forced to exceed the duration of authorised stay due to unforeseeable and serious events,

▼B

that he or she has acquired a legal right to stay or in case of errors. Without prejudice to any available administrative or non-judicial remedy, that third-country national shall have access to an effective judicial remedy to ensure the data are rectified, completed or erased.

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

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

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

Where a third-country national has acquired the nationality of Andorra, Monaco or San Marino ►C1 or where a third-country national is in possession of a passport issued by the Vatican City State or the Holy See, he or she shall inform ◄ the competent authorities of the Member State he or she next enters of that change. That Member State shall erase his or her data without delay from the EES. The third-country national in question shall have access to an effective judicial remedy to ensure that the data are erased.

▼M2

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

▼B

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

CHAPTER VI

DEVELOPMENT, OPERATION AND RESPONSIBILITIES

Article 36

Adoption of implementing acts by the Commission prior to development

The Commission shall adopt the implementing acts necessary for the development and technical implementation ►M2 of the EES Central System and the CIR ◄, the NUIs, the Communication Infrastructure, the web service referred to in Article 13 and the data repository referred to in Article 63(2), in particular measures for:

▼B

(a) the specifications for the quality, resolution and use of fingerprints for biometric verification and identification in the EES;

(b) the specifications for the quality, resolution and use of the facial image for biometric verification and identification in the EES, including where taken live or extracted electronically from the eMRTD;

(c) entering the data in accordance with Articles 16 to 20;

(d) accessing the data in accordance with Articles 23 to 33;

(e) amending, erasing and advance erasure of data in accordance with Article 35;

(f) keeping and accessing the logs in accordance with Article 46;

(g) performance requirements, including the minimum specifications for technical equipment and requirements regarding the biometric performance of the EES, in particular in terms of the required False Positive Identification Rate, False Negative Identification Rate and Failure To Enrol Rate;

(h) the specifications and conditions for the web service referred to in Article 13, including specific provisions for the protection of the data where provided by or to carriers;

(i) the establishment and the high level design of interoperability as referred to in Article 8;

(j) the specifications and conditions for the data repository referred in Article 63(2);

(k) the establishment of the list of identified persons referred to in Article 12(3) and the procedure to make that list available to Member States;

(l) the specifications for technical solutions to connect central access points in accordance with Articles 31, 32 and 33 and for a technical solution to collect the statistical data required pursuant to Article 72(8).

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 68(2).

For the adoption of the implementing acts set out in point (i) of the first paragraph of this Article, the Committee set up by Article 68 of this Regulation shall consult the VIS Committee set up by Article 49 of Regulation (EC) No 767/2008.

▼B

Article 37

Development and operational management

▼M2

1. eu-LISA shall be responsible for the development of the EES Central System and the CIR, the NUIs, the Communication Infrastructure and the Secure Communication Channel between the EES Central System and the VIS Central System. eu-LISA shall also be responsible for the development of the web service referred to in Article 13 in accordance with the detailed rules referred to in Article 13(7) and the specifications and conditions adopted pursuant to point (h) of the first paragraph of Article 36 and for the development of the data repository referred to in Article 63(2).

▼B

eu-LISA shall define the design of the physical architecture of the EES including its Communication Infrastructure, as well as the technical specifications and their evolution regarding the EES Central System, the NUIs, the Communication Infrastructure, the Secure Communication Channel between the EES Central System and the VIS Central System, the web service referred to in Article 13 of this Regulation and the data repository referred to in Article 63(2) of this Regulation. Those technical specifications shall be adopted by eu-LISA's Management Board, subject to a favourable opinion of the Commission. eu-LISA shall also implement any necessary adaptations to the VIS deriving from the establishment of interoperability with the EES as well as from the implementation of the amendments to Regulation (EC) No 767/2008 set out in Article 61 of this Regulation.

eu-LISA shall develop and implement the EES Central System, the NUIs, the Communication Infrastructure, the Secure Communication Channel between the EES Central System and the VIS Central System, the web service referred to in Article 13 and the data repository referred to Article 63(2) as soon as possible after the adoption by the Commission of the measures provided for in Article 36.

The development shall consist of the elaboration and implementation of the technical specifications, testing and overall project coordination.

When developing, and when implementing, the EES Central System, the NUIs, the Communication Infrastructure, the Secure Communication Channel between the EES Central System and the VIS Central System, the web service referred to in Article 13 and the data repository referred to in Article 63(2), the tasks of eu–LISA shall also be to:

(a) perform a security risk assessment;

(b) follow the principles of privacy by design and by default during the entire lifecycle of the development of the EES;

(c) conduct a security risk assessment regarding the interoperability with the VIS referred to in Article 8 and assess the required security measures needed for the implementation of the interoperability with the VIS.

▼B

2. During the designing and development phase, a Programme Management Board composed of a maximum of ten members shall be established. It shall be composed of seven members appointed by eu-LISA's Management Board from among its members or alternate members, the Chair of the EES Advisory Group referred to in Article 69, a member representing eu-LISA appointed by its Executive Director and one member appointed by the Commission. The members appointed by eu-LISA's Management Board shall be elected only from those Member States which are fully bound under Union law by the legislative instruments governing the development, establishment, operation and use of all the large-scale IT systems managed by eu-LISA and which comply with the conditions set out in Article 66(2).

The Programme Management Board shall meet regularly and at least three times per quarter. It shall ensure the adequate management of the design and development phase of the EES and ensure the consistency between central and national EES projects.

The Programme Management Board shall submit written reports every month to eu-LISA's Management Board on the progress of the project. The Programme Management Board shall have no decision-making power nor any mandate to represent the members of eu-LISA's Management Board.

eu-LISA's Management Board shall establish the rules of procedure of the Programme Management Board which shall include in particular rules on:

(a) its chairmanship;

(b) meeting venues;

(c) the preparation of meetings;

(d) the admission of experts to meetings;

(e) communication plans ensuring full information to non-participating members of eu-LISA's Management Board.

The chairmanship of the Programme Management Board shall be held by a Member State which is fully bound under Union law by the legislative instruments governing the development, establishment, operation and use of all the large-scale IT systems managed by eu-LISA.

All travel and subsistence expenses incurred by the members of the Programme Management Board shall be paid by eu-LISA and Article 10 of the eu-LISA Rules of Procedure shall apply *mutatis mutandis*. eu-LISA shall provide the Programme Management Board with a secretariat.

During the designing and development phase, the EES Advisory Group referred to in Article 69 shall be composed of national EES project managers and chaired by eu-LISA. It shall meet regularly and at least three times per quarter until the start of operations of the EES. It shall report after each meeting to the Programme Management Board. It shall provide the technical expertise to support the tasks of the Programme Management Board and shall follow-up on the state of preparation of the Member States.

▼M2

3. eu-LISA shall be responsible for the operational management of the EES Central System and the CIR, the NUIs and the Secure Communication Channel between the EES Central System and the VIS Central System. 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 the EES Central System and the CIR, the NUIs, the Communication Infrastructure, the Secure Communication Channel between the EES Central System and the VIS Central System, the web service referred to in Article 13 and the data repository referred to in Article 63(2). eu-LISA shall also be responsible for the operational management of the Communication Infrastructure between the EES Central System and the NUIs, for the web service referred to in Article 13 and the data repository referred to in Article 63(2).

▼B

Operational management of the EES shall consist of all the tasks necessary to keep the EES functioning 24 hours a day, 7 days a week in accordance with this Regulation, in particular the maintenance work and technical developments necessary to ensure that the EES functions at a satisfactory level of operational quality, in particular as regards the response time for interrogation of the EES Central System by border authorities, in accordance with the technical specifications.

4. Without prejudice to Article 17 of the Staff Regulations of Officials of the European Union and the Conditions of Employment of Other Servants of the Union, laid down in Council Regulation (EEC, Euratom, ECSC) No 259/68 [1], eu-LISA shall ensure that those members of its staff who are required to work with EES data or with data stored in the EES apply appropriate rules of professional secrecy or other equivalent duties of confidentiality. That obligation shall also apply after such staff leave office or employment or after the termination of their activities.

Article 38

Responsibilities of Member States and Europol

1. Each Member State shall be responsible for:

(a) the integration of the existing national border infrastructure and its connection to the NUI;

(b) the organisation, management, operation and maintenance of its existing national border infrastructure and of its connection to the EES for the purpose of Article 6 with the exception of Article 6(2);

(c) the organisation of central access points and their connection to the NUI for the purpose of law enforcement;

(d) the management of, and arrangements for, access by the duly authorised staff, and by the duly empowered staff, of the competent national authorities to the EES in accordance with this Regulation and the creation and regular update of a list of those staff and their profiles.

2. Each Member State shall designate a national authority, which shall provide the competent authorities referred to in Article 9(2) with access to the EES. Each Member State shall connect that national authority to the NUI. Each Member State shall connect their respective central access points referred to in Article 29 to the NUI.

[1] OJ L 56, 4.3.1968, p. 1.

▼B

3. Each Member State shall use automated procedures for processing EES data.

4. Member States shall ensure that the technical performance of the border control infrastructure, its availability, the duration of the border checks and the data quality are closely monitored in order to ensure that they meet the overall requirements for the proper functioning of the EES and an efficient border check procedure.

5. Before being authorised to process data stored in the EES, the staff of the authorities having a right to access the EES shall be given appropriate training on, in particular, data security and data protection rules, as well as on relevant fundamental rights.

6. Member States shall not process the data in or from the EES for purposes other than those laid down in this Regulation.

7. Europol shall assume the responsibilities provided for in point (d) of paragraph 1 and in paragraphs 3, 5 and 6. It shall connect, and be responsible for the connection of, the Europol central access point to the EES.

Article 39

Responsibility for data processing

1. In relation to the processing of personal data in the EES, 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 communicate the details of that authority to the Commission.

Each Member State shall ensure that the data collected and recorded in the EES is processed lawfully and, in particular, that only duly authorised staff have access to the data for the performance of their tasks. The Member State responsible shall ensure, in particular, that the data are:

(a) collected lawfully and in full respect of the human dignity of the third-country national concerned;

(b) registered lawfully in the EES;

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

2. eu-LISA shall ensure that the EES is operated in accordance with this Regulation and the implementing acts referred to in Article 36. In particular, eu-LISA shall:

(a) take the necessary measures to ensure the security of the EES Central System and the Communication Infrastructure between the EES Central System and the NUI, without prejudice to the responsibilities of the Member States;

(b) ensure that only duly authorised staff have access to data processed in the EES.

3. eu-LISA shall inform the European Parliament, the Council and the Commission, as well as the European Data Protection Supervisor, of the measures it takes pursuant to paragraph 2 in view of the start of operations of the EES.

▼B

Article 40

Keeping of data in national files and national entry/exit systems

1. A Member State may keep the alphanumeric data which that Member State entered in the EES, in accordance with the purposes of the EES, in its national entry/exit system or equivalent national files, in full respect of Union law.

2. The data shall not be kept in the national entry/exit systems or equivalent national files for longer than they are kept in the EES.

3. Any use of data which does not comply with paragraph 1 shall be considered a misuse under the national law of each Member State as well as under Union law.

4. This Article shall not be construed as requiring any technical adaptation of the EES. Member States may keep data in accordance with this Article at their own cost and risk and using their own technical means.

Article 41

Communication of data to third countries, international organisations and private entities

1. Data stored in the EES shall not be transferred or made available to any third country, to any international organisation or to any private entity.

2. By way of derogation from paragraph 1 of this Article, the data referred to in Article 16(1) and points (a), (b) and (c) of Article 17(1) of this Regulation may be transferred by border authorities or immigration authorities to a third country or to an international organisation listed in the Annex I to this Regulation in individual cases, if necessary in order to prove the identity of third-country nationals for the sole purpose of return, only where one of the following conditions is satisfied:

(a) the Commission has adopted a decision on the adequate protection of personal data in that third country in accordance with Article 45(3) of Regulation (EU) 2016/679;

(b) appropriate safeguards as referred to in Article 46 of Regulation (EU) 2016/679 have been provided, such as through a readmission agreement which is in force between the Union or a Member State and the third country in question; or

(c) point (d) of Article 49(1) of Regulation (EU) 2016/679, applies.

3. The data referred to in Article 16(1) and points (a), (b) and (c) of Article 17(1) of this Regulation may be transferred in accordance with paragraph 2 of this Article 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, including Chapter V of Regulation (EU) 2016/679, and readmission agreements, and the national law of the Member State transferring the data;

(b) the third country or international organisation has agreed to process the data only for the purposes for which they were provided; and

▼B

(c) a return decision adopted pursuant to Directive 2008/115/EC has been issued in relation to the third-country national concerned, provided that 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.

4. 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*.

5. Personal data obtained from the EES Central System 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.

6. By way of derogation from paragraph 5 of this Article, the data referred to in points (a), (b) and (c) of Article 16(1), points (a) and (b) of Article 16(2), points (a) and (b) of Article 16(3) and point (a) of Article 17(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 such a terrorist offence or serious criminal offence;

(c) the designated authority has access to such data in accordance with the procedure and the conditions set out in Articles 31 and 32;

(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; and

(f) the reciprocal provision of any information on entry/exit records held by the requesting third country to the Member States operating the EES 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 established in accordance with Article 41(1) of Directive (EU) 2016/680, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.

Article 42

Conditions for communication of data to a Member State which does not yet operate the EES and to a Member State to which this Regulation does not apply

1. The data referred to in points (a), (b) and (c) of Article 16(1), points (a) and (b) of Article 16(2), points (a) and (b) of Article 16(3) and point (a) of Article 17(1) may be transferred by a designated

▼B

authority to a Member State which does not yet operate the EES and to a Member State to which this Regulation does not apply, 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) a serious criminal offence;

(b) the transfer of data is necessary for the prevention, detection or investigation of such a terrorist offence or serious criminal offence;

(c) the designated authority has access to such data in accordance with the procedure and the conditions set out in Articles 31 and 32;

(d) Directive (EU) 2016/680 applies;

(e) a duly motivated written or electronic request has been submitted; and

(f) the reciprocal provision of any information on entry/exit records held by the requesting Member State to the Member States operating the EES 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 established in accordance with Article 41(1) of Directive (EU) 2016/680, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.

2. Where data is provided pursuant to this Article, the same conditions as provided for in Article 43(1), Article 45(1) and (3), Article 48 and Article 58(4) shall apply *mutatis mutandis*.

Article 43

Data security

1. The Member State responsible shall ensure the security of the data before and during the transmission to the NUI. Each Member State shall ensure the security of the data it receives from the EES.

2. Each Member State shall, in relation to its national border infrastructure, adopt the necessary measures, including a security plan and a business continuity and disaster recovery plan, in order to:

(a) physically protect data, including by making contingency plans for the protection of critical infrastructure;

(b) deny unauthorised persons access to data-processing equipment and national installations in which the Member State carries out operations in accordance with the purposes of the EES;

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

(d) prevent the unauthorised entering of data and the unauthorised inspection, modification or erasure of stored personal data;

▼B

(e) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment;

(f) prevent the unauthorised processing of data in the EES and any unauthorised modification or erasure of data processed in the EES;

(g) ensure that persons authorised to access the EES have access only to the data covered by their access authorisation, by means of individual and unique user identities and confidential access modes only;

(h) ensure that all authorities with a right of access to the EES create profiles describing the functions and responsibilities of persons who are authorised to enter, amend, erase, consult and search the data and make their profiles available to the supervisory authorities;

(i) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment;

(j) ensure that it is possible to verify and establish which data have been processed in the EES, as well as when, by whom and for what purpose they have been processed;

(k) prevent the unauthorised reading, copying, modification or erasure of personal data during the transmission of personal data to or from the EES or during the transport of data media, in particular by means of appropriate encryption techniques;

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

(m) ensure reliability by making sure that any faults in the functioning of the EES are properly reported;

(n) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Regulation.

3. As regards the operation of the EES, eu-LISA shall take the necessary measures in order to achieve the objectives set out in paragraph 2, including the adoption of a security plan and a business continuity and disaster recovery plan. eu-LISA shall also ensure reliability by making sure that 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 EES.

4. eu-LISA and the Member States shall cooperate in order to ensure a harmonised data security approach based on a security risk management process encompassing the entire EES.

▼B

Article 44

Security incidents

1. Any event that has or may have an impact on the security of the EES and may cause damage or loss to data stored in the EES 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 EES Central System, eu-LISA shall notify the Commission and the European Data Protection Supervisor.

4. Information regarding a security incident that has or may have an impact on the operation of the EES or on the availability, integrity and confidentiality of the data shall be provided to the Member States and reported in compliance with the incident management plan to be provided by eu-LISA.

5. The Member States concerned and eu-LISA shall cooperate in the event of a security incident.

Article 45

Liability

1. Any person or Member State that has suffered material or immaterial damage as a result of an unlawful processing operation or any act not compliant with this Regulation shall be entitled to receive compensation from the Member State which is responsible for the damage suffered. That Member State shall be exempted from liability, in whole or in part, if it proves that it is not in any way 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 EES, that Member State shall be held liable for such damage, unless and insofar as eu-LISA or another Member State participating in the EES failed to take reasonable measures to prevent the damage from occurring or to minimise its impact.

3. Claims for compensation against a Member State for the damage referred to in paragraphs 1 and 2 shall be governed by the provisions of national law of the defendant Member State.

Article 46

Keeping of logs by eu-LISA and Member States

1. eu-LISA shall keep logs of all data processing operations within the EES. Those logs shall include the following:

▼B

(a) the purpose of access referred to in Article 9(2);

(b) the date and time;

(c) the data transmitted as referred to in Articles 16 to 19;

(d) the data used for interrogation as referred to in Articles 23 to 27;

(e) the name of the authority entering or retrieving the data; and

▼M2

(f) a reference to the use of the ESP to query the EES as referred to in Article 7(2) of Regulation (EU) 2019/817.

▼B

2. For the consultations listed in Article 8, a log of each data processing operation carried out within the EES and the VIS shall be kept in accordance with this Article and Article 34 of Regulation (EC) No 767/2008. eu-LISA shall ensure, in particular, that the relevant log of the concerned data processing operations is kept when the competent authorities launch a data processing operation directly from one system to the other.

3. In addition to paragraphs 1 and 2, each Member State shall keep logs of the staff duly authorised to process the EES data.

4. Such logs may be used only for data protection monitoring, including checking the admissibility of a request and the lawfulness of data processing, and for ensuring data security pursuant to Article 43. Those logs shall be protected by appropriate measures against unauthorised access and erased one year after the retention period referred to in Article 34 has expired, unless they are required for monitoring procedures which have already begun.

Article 47

Self-monitoring

Member States shall ensure that each authority entitled to access EES data takes the measures necessary to comply with this Regulation and cooperates, where necessary, with the supervisory authorities.

Article 48

Penalties

Member States shall take the necessary measures to ensure that any use of data entered in the EES in a manner contrary to this Regulation is punishable by effective, ►C1 proportionate and dissuasive penalties in accordance with ◄ national law, Article 84 of Regulation (EU) 2016/679 and Article 57 of Directive (EU) 2016/680.

Article 49

Data Protection

1. Regulation (EC) No 45/2001 shall apply to the processing of personal data by eu-LISA on the basis of this Regulation.

▼B

2. Regulation (EU) 2016/679 shall apply to the processing of personal data by national authorities on the basis of this Regulation, with the exception of processing for the purposes referred to in Article 1(2) of this Regulation.

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

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

CHAPTER VII

RIGHTS AND SUPERVISION ON DATA PROTECTION

Article 50

Right of information

1. Without prejudice to the right of information in Article 13 of Regulation (EU) 2016/679, third-country nationals whose data are to be recorded in the EES shall be informed by the Member State responsible of the following:

(a) the fact that the EES may be accessed by the Member States and Europol for law enforcement purposes;

(b) the obligation on visa-exempt third-country nationals and on holders of an FTD to have their fingerprints taken;

(c) the obligation on all third-country nationals subject to registration in the EES to have their facial image recorded;

(d) that the collection of the data is mandatory for the examination of entry conditions;

(e) the fact that entry will be refused if a third-country national refuses to provide the requested biometric data for registration, verification or identification in the EES;

(f) the right to receive information about the maximum remaining duration of their authorised stay in accordance with Article 11(3);

(g) the fact that personal data stored in the EES may be transferred to a third country or an international organisation listed in Annex I for the purposes of return, to a third country in accordance with Article 41(6) and to Member States in accordance with Article 42;

(h) the existence of the right to request from the controller 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 controller and the supervisory authorities, or of the European Data Protection Supervisor if applicable, which shall hear complaints concerning the protection of personal data;

▼B

(i) the fact that EES data will be accessed for border management and facilitation purposes and that overstays will automatically lead to the addition of their data to the list of identified persons referred to in Article 12(3), as well as the possible consequences of overstaying;

(j) the data retention period set for entry and exit records, refusal of entry records, and for individual files pursuant to Article 34;

(k) the right for overstayers to have their personal data erased from the list of identified persons referred to in Article 12(3) and rectified in the EES, where they provide evidence that they exceeded the authorised duration of stay due to unforeseeable and serious events;

(l) the right to lodge a complaint to the supervisory authorities.

2. The information provided in paragraph 1 of this Article shall be provided in writing, by any appropriate means, in a concise, transparent, intelligible and easily accessible form, and it shall be made available, using clear and plain language, in a linguistic version the person concerned understands or is reasonably expected to understand, in order to ensure that third-country nationals are informed of their rights, at the time when the individual file of the person concerned is being created in accordance with Article 16, 17 or 18.

3. The Commission shall also set up a website containing the information referred to paragraph 1.

4. The Commission shall adopt implementing acts drawing up the information referred to in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 68(2).

5. The Commission shall provide the information referred to in paragraph 1 of this Article in a template. The template shall be drawn up in such a manner as to enable Member States to complete it with additional Member State specific information. That Member State specific information shall include at least the rights of the data subject, the possibility of assistance by the supervisory authorities, as well as contact details of the office of the controller and of the data protection officer and the supervisory authorities. The Commission shall adopt implementing acts concerning the specifications and conditions for the website referred to in paragraph 3 of this Article. Those implementing acts shall be adopted prior to the start of operations of the EES in accordance with the examination procedure referred to in Article 68(2).

Article 51

Information campaign

The Commission shall, in cooperation with the supervisory authorities and the European Data Protection Supervisor, accompany the start of operations of the EES with an information campaign informing the public and, in particular, third-country nationals, about the objectives of the EES, the data stored in the EES, the authorities having access and the rights of persons concerned. Such information campaigns shall be conducted regularly.

▼B

Article 52

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

1. The requests of third-country nationals in relation to the rights set out in Articles 15 to 18 of Regulation (EU) 2016/679 may be addressed to the competent authority of any Member State.

The Member State responsible or the Member State to which the request has been made shall reply to such requests within 45 days of receipt of the request.

2. If a request for rectification, completion or erasure of personal data or restriction of the processing thereof is made to a Member State other than the Member State responsible, the authorities of the Member State to which the request has been made shall check the accuracy of the data and the lawfulness of the data processing in the EES within 30 days of the receipt of the request where that check can be done without consulting the Member State responsible. Otherwise, the Member State to which the request has been made shall contact the authorities of the Member State responsible within seven days and the Member State responsible shall check the accuracy of the data and the lawfulness of the data processing within 30 days of such contact.

3. In the event that data recorded in the EES are factually inaccurate, incomplete or have been recorded unlawfully, the Member State responsible or, where applicable, the Member State to which the request has been made shall rectify, complete or erase the personal data or restrict the processing of personal data in accordance with Article 35. The Member State responsible or, where applicable, the Member State to which the request has been made shall confirm in writing to the person concerned without delay that it has taken action to rectify, complete or erase the personal data of that person or to restrict the processing of such personal data.

In the event that visa-related data recorded in the EES are factually incorrect, incomplete or have been recorded unlawfully, the Member State responsible or, where applicable, the Member State to which the request has been made shall first check the accuracy of these data against the VIS and shall, if necessary, amend them in the EES. Should the data recorded in the VIS be the same as in the EES, the Member State responsible or, where applicable, the Member State to which the request has been made, shall contact the authorities of the Member State which is responsible for entering these data in the VIS within seven days. The Member State which is responsible for entering the data in the VIS shall check the accuracy of the visa-related data and the lawfulness of their processing in the EES within 30 days of such contact and inform the Member State responsible or the Member State to which the request has been made which shall, if necessary, rectify or complete the personal data of the person concerned or restrict the processing of such data in, or erase such data from, the EES without delay and, where applicable, from the list of identified persons referred to in Article 12(3).

4. If the Member State responsible or, where applicable, the Member State to which the request has been made does not agree that data recorded in the EES are factually inaccurate, incomplete or have been recorded unlawfully, that Member State shall adopt an administrative

▼B

decision explaining in writing to the third-country national concerned without delay why it is not prepared to rectify, complete or erase the personal data relating to him or her or restrict the processing of such data.

5. The Member State which has adopted the administrative decision pursuant to paragraph 4 of this Article shall also provide the third-country national concerned with information explaining the steps which he or she can take if he or she does not accept the explanation. This shall include information on how to bring an action or a complaint before the competent authorities or courts of that Member State and any assistance that is available in accordance with the laws, regulations and procedures of that Member State, including from the supervisory authority established in accordance with Article 51(1) of Regulation (EU) 2016/679.

6. Any request made pursuant to paragraphs 1 and 2 shall contain the minimum information necessary to identify the third-country national concerned. Fingerprints may be requested for this purpose only in duly justified cases and where there are substantive doubts as to the identity of the applicant. That information shall be used exclusively to enable that third-country national to exercise the rights referred to in paragraph 1 and shall be erased immediately afterwards.

7. Whenever a person makes a request in accordance with paragraph 1 of this Article, the competent authority of the Member State responsible or of the Member State to whom the request has been made shall keep a record in the form of a written document that such a request was made. That document shall contain information on how that request was dealt with and by which authority. The competent authority shall make that document available to the supervisory authority established in accordance with Article 51(1) of Regulation (EU) 2016/679, within seven days.

Article 53

Cooperation to enforce the rights on data protection

1. The competent authorities of the Member States shall cooperate actively to enforce the rights laid down in Article 52.

2. In each Member State, the supervisory authority established in accordance with Article 51(1) of Regulation (EU) 2016/679 shall, upon request, assist and advise the data subject in exercising his or her right to rectify, complete or erase personal data relating to him or her or to restrict 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 which transmitted the data and the supervisory authority of the Member State to which the request has been made shall cooperate with each other.

▼B

Article 54

Remedies

1. Without prejudice to Articles 77 and 79 of Regulation (EU) 2016/679, in each Member State any person shall have the right to bring an action or a complaint before the competent authorities or courts of that Member State which refused the right of access to, or right of rectification, completion or erasure of, data relating to him or her provided for in Article 52 and Article 53(2) of this Regulation. The right to bring such an action or complaint shall also apply in cases where requests for access, rectification, completion or erasure were not responded to within the deadlines provided for in Article 52 or were never dealt with by the data controller.

2. The assistance of the supervisory authority established in accordance with Article 51(1) of Regulation (EU) 2016/679 shall remain available throughout the proceedings.

Article 55

Supervision by the supervisory authority

1. Each Member State shall ensure that the supervisory authority established in accordance with Article 51(1) of Regulation (EU) 2016/679 independently monitors the lawfulness of the processing of personal data referred to in Chapters II, III, V and VI of this Regulation by the Member State concerned, including their transmission to and from the EES.

2. The supervisory authority established in accordance with Article 51(1) of Regulation (EU) 2016/679 shall ensure that an audit of the data processing operations in the national border infrastructure is carried out in accordance with relevant international auditing standards at least every three years from the start of operations of the EES. 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 ([1]). The supervisory authority established in accordance with 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.

3. Member States shall ensure that their supervisory authority established in accordance with Article 51(1) of Regulation (EU) 2016/679 has sufficient resources to fulfil the tasks entrusted to it under this Regulation and has access to advice from persons with sufficient knowledge of biometric data.

4. Member States shall supply any information requested by the supervisory authority established in accordance with Article 51(1) of Regulation (EU) 2016/679 and shall, in particular, provide it with information on the activities carried out in accordance with Article 38,

([1]) 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).

▼B

Article 39(1) and Article 43. Member States shall grant the supervisory authority established in accordance with Article 51(1) of Regulation (EU) 2016/679 access to their logs pursuant to Article 46 and allow it access at all times to all their EES related premises.

Article 56

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 concerning the EES and for ensuring that such activities are carried out in accordance with Regulation (EC) No 45/2001 and with this Regulation.

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 three years. A report of that audit shall be sent to the European Parliament, to the Council, to the Commission, to eu-LISA and to the supervisory authorities. eu-LISA shall be given an opportunity to make comments before the report is adopted.

3. eu-LISA shall supply information requested by the European Data Protection Supervisor, give him or her access to all documents and to its logs referred to in Article 46 and allow him or her access to all its premises at any time.

Article 57

▼C1

Cooperation between supervisory authorities and the European Data Protection Supervisor

▼B

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 and shall ensure coordinated supervision of the EES and the national border infrastructures.

2. The supervisory authorities and the European Data Protection Supervisor 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 purpose 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 established by Regulation (EU) 2016/679 (the 'European Data Protection

▼B

Board'). The costs of those meetings shall be borne and their organisation shall be undertaken by that Board. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary.

4. A joint report of activities shall be sent by the European Data Protection Board to the European Parliament, to the Council, to the Commission and to eu-LISA every two years. That report shall include a chapter on each Member State prepared by the supervisory authorities of that Member State.

Article 58

Protection of personal data accessed in accordance with Chapter IV

1. Each Member State shall ensure that the national laws, regulations and administrative provisions adopted pursuant to Directive (EU) 2016/680 are also applicable to the access to the EES by its national authorities in line with Article 1(2) of this Regulation, including in relation to the rights of the persons whose data are so accessed.

2. The supervisory authority established in accordance with Article 41(1) of Directive (EU) 2016/680 shall monitor the lawfulness of the access to personal data by the Member States in accordance with Chapter IV of this Regulation, including their transmission to and from the EES. Article 55(3) and (4) of this Regulation shall apply accordingly.

3. The processing of personal data by Europol pursuant to this Regulation shall be carried out in accordance with Regulation (EU) 2016/794 and shall be supervised by the European Data Protection Supervisor.

4. Personal data accessed in the EES in accordance with Chapter IV shall only be processed for the purposes of the prevention, detection or investigation of the specific case for which the data have been requested by a Member State or by Europol.

5. The EES Central System, the designated authorities, the central access points and Europol shall keep records of the searches for the purpose of enabling the supervisory authority established in accordance with Article 41(1) of Directive (EU) 2016/680 and the European Data Protection Supervisor to monitor the compliance of data processing with Union and national data protection rules. With the exception of that purpose, personal data, as well as the records of searches, shall be erased from all national and Europol files after 30 days, unless those data and records are required for the purposes of the specific ongoing criminal investigation for which they were requested by a Member State or by Europol.

Article 59

Logging and documentation

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

▼B

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

(a) the exact purpose of the request for access to EES data, including the terrorist offence or other serious criminal offence concerned and, for Europol, the exact purpose of the request for access;

(b) the reasonable grounds given for not making comparisons with other Member States under Decision 2008/615/JHA, in accordance with point (b) of Article 32(2) of this Regulation;

(c) the national file reference;

(d) the date and exact time of the request for access by the central access point to the EES Central System;

(e) the name of the authority which requested access for consultation;

(f) where applicable, the use of the urgency procedure referred to in Article 31(2) of this Regulation and the decision taken with regard to the *ex-post* verification;

(g) the data used for consultation;

(h) in accordance with national rules or with Regulation (EU) 2016/794, the unique user identity of the official who carried out the search and of the official who ordered the search.

3. Logs and documentation shall be used only for monitoring the lawfulness of data processing and for ensuring data integrity and security. Only logs which do not contain personal data may be used for the monitoring and evaluation referred to in Article 72 of this Regulation. The supervisory authority established in accordance with Article 41(1) of Directive (EU) 2016/680, which is responsible for checking the admissibility of the request and monitoring the lawfulness of the data processing and data integrity and security, shall have access to these logs at its request for the purpose of fulfilling its duties.

CHAPTER VIII

AMENDMENTS TO OTHER UNION INSTRUMENTS

Article 60

Amendment to the Convention implementing the Schengen Agreement

Article 20 of the Convention implementing the Schengen Agreement is amended as follows:

(1) paragraph 2 is replaced by the following:

‘2. Paragraph 1 shall not affect each Contracting Party’s right to extend beyond 90 days in any 180-day period an alien’s stay on its territory:

(a) in exceptional circumstances; or

▼B

(b) in accordance with a bilateral agreement concluded before the entry into force of this Convention and notified to the Commission in accordance with paragraph 2d.';

(2) the following paragraphs are inserted:

'2a. The stay of an alien on the territory of a Contracting Party may be extended in accordance with a bilateral agreement pursuant to point (b) of paragraph 2, upon request of the alien, and lodged with the competent authorities of that Contracting Party on entry or during the stay of the alien at the latest on the last working day of his or her 90-day stay in any 180-day period.

Where the alien has not lodged a request during the 90-day stay in any 180-day period, his or her stay may be extended pursuant to a bilateral agreement concluded by a Contracting Party and his or her stay beyond the 90-day stay in any 180-day period preceding that extension may be presumed lawful by the competent authorities of that Contracting Party, provided that that alien presents credible evidence which proves that during that time he or she stayed only on the territory of that Contracting Party.

2b. Where the stay is extended pursuant to paragraph 2 of this Article, the competent authorities of that Contracting Party shall enter the data related to the extension in the latest relevant entry/exit record linked to the alien's individual file contained in the Entry/Exit System established by Regulation (EU) 2017/2226 of the European Parliament and of the Council (*). Such data shall be entered in accordance with Article 19 of that Regulation.

2c. Where the stay is extended pursuant to paragraph 2, the alien concerned shall be authorised to stay only on the territory of that Contracting Party and exit at the external borders of that Contracting Party.

The competent authority which extended the stay shall inform the alien concerned that the extension of stay authorises the alien concerned to stay only on the territory of that Contracting Party and that he or she is to exit at the external borders of that Contracting party.

2d. By 30 March 2018, the Contracting Parties shall notify the text of their relevant applicable bilateral agreements as referred to in point (b) of paragraph 2 to the Commission. If a Contracting Party ceases to apply any of those bilateral agreements, it shall notify the Commission thereof. The Commission shall publish information about such bilateral agreements in the *Official Journal of the European Union*, including at least the Member States and third countries concerned, the rights derived for aliens from those bilateral agreements, as well as any changes thereto.

(*) Regulation (EU) 2017/2226 of the European Parliament and of the Council of 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).'.

▼B

Article 61

Amendments to Regulation (EC) No 767/2008

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

(1) Article 10(1) is amended as follows:

(a) the following point is inserted:

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

(b) the following point is added:

‘(l) if applicable, the status of the person indicating that the third-country national is a member of the family of a Union citizen to whom Directive 2004/38/EC of the European Parliament and of the Council (*) 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).’;

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

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

(*) 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).’;

(3) in Article 14, the following paragraph is added:

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

▼B

(4) Article 15 is amended as follows:

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

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

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

(b) the following paragraphs are added:

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

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

(5) in Chapter III, the following Article is inserted:

‘Article 17a

Interoperability with the EES

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

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

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

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

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

▼B

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

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

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

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

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

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

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

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

(6) Article 18 is replaced by the following:

'Article 18

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

1. For the sole purpose of verifying the identity of the visa holders, the authenticity, temporal and territorial validity and status of the visa or whether the conditions for entry to the territory of the Member States in accordance with Article 6 of

▼B

Regulation (EU) 2016/399 are fulfilled, or both, the competent authorities for carrying out checks at borders at which the EES is operated shall have access to the VIS to search using the following data:

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

(b) the number of the visa sticker.

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

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

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

(a) the status information and the data taken from the application form, ►C2 referred to in points (2) and (4) of Article 9; ◄

(b) photographs;

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

In addition, for those visa holders for whom certain data are not required to be provided for legal reasons or factually cannot be provided, the competent authority for carrying out checks at

▼B

borders at which the EES is operated shall receive a notification related to the specific data field or fields concerned which shall be marked as ‘not applicable’.

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

(a) the status information and the data taken from the application form, ►C2 referred to in points (2) and (4) of Article 9; ◄

(b) photographs;

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

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

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

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

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

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

(iv) of any other reason;

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

The competent authorities for carrying out checks at borders at which the EES is operated shall verify the fingerprints of the visa holder against the fingerprints recorded in the VIS. For visa

▼B

holders whose fingerprints cannot be used, the search referred to in paragraph 1 shall be carried out only with the alphanumeric data provided for in paragraph 1.

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

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

(7) the following Article is inserted:

'Article 18a

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

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

(8) the following Article is inserted:

'Article 19a

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

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

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

▼B

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

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

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

(a) the status information and the data taken from the application form, ►C2 referred to in points (2) and (4) of Article 9; ◄

(b) photographs;

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

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

(9) in Article 20(1), the first subparagraph 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 may not, or may no longer, fulfil the conditions for the entry to, or stay or residence on, the territory of the Member States, the authorities

▼B

competent for carrying out checks at borders at which the EES is operated or within the territory of the Member States as to whether the conditions for entry to, or stay or residence on, the territory of the Member States are fulfilled, shall have access to search in the VIS with the fingerprints of that person.';

(10) in Article 26, the following paragraph is inserted:

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

(11) Article 34 is amended as follows:

(a) paragraph 1 is replaced by the following:

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

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

(b) the date and time;

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

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

(e) the name of the authority entering or retrieving the data.

In addition, each Member State shall keep records of the staff duly authorised to enter or retrieve the data.';

(b) the following paragraph is inserted:

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

Article 62

Amendments to Regulation (EU) No 1077/2011

Regulation (EU) No 1077/2011 is amended as follows:

(1) in Article 1, paragraph 2 is replaced by the following:

▼B

‘2. The Agency shall be responsible for the operational management of the second-generation Schengen Information System (SIS II), the Visa Information System (VIS), Eurodac and the Entry/Exit System established by Regulation (EU) 2017/2226 of the European Parliament and of the Council (*) (EES).

(*) 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).’;

(2) the following Article is inserted:

‘Article 5a

Tasks relating to the EES

In relation to the EES, the Agency shall perform:

(a) the tasks conferred on it by Regulation (EU) 2017/2226;

(b) tasks relating to training on the technical use of the EES.’;

(3) in Article 7, paragraphs 5 and 6 are replaced by the following:

‘5. Tasks related to the operational management of the communication infrastructure may be entrusted to external private-sector entities or bodies in accordance with Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council (*). In such a case, the network provider shall be bound by the security measures referred to in paragraph 4 of this Article and shall have no access to SIS II, VIS, Eurodac or EES operational data, or to the SIS II-related SIRENE exchange, by any means.

6. Without prejudice to the existing contracts on the network of SIS II, VIS, Eurodac and EES, the management of encryption keys shall remain within the competence of the Agency and shall not be outsourced to any external private-sector entity.

(*) Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council of 25 October 2012 on the financial rules applicable to the general budget of the Union and repealing Council Regulation (EC, Euratom) No 1605/2002 (OJ L 298, 26.10.2012, p. 1).’;

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

‘1. The Agency shall monitor the developments in research relevant for the operational management of SIS II, VIS, Eurodac, EES and other large-scale IT systems.’;

(5) in Article 12, paragraph 1 is amended as follows:

▼B

(a) the following point is inserted:

‘(sa) adopt the reports on the development of the EES pursuant to Article 72(2) of Regulation (EU) 2017/2226;’;

(b) point (t) is replaced by the following:

‘(t) adopt the reports on the technical functioning of SIS II pursuant to Article 50(4) of Regulation (EC) No 1987/2006 and Article 66(4) of Decision 2007/533/JHA, of VIS pursuant to Article 50(3) of Regulation (EC) No 767/2008 and Article 17(3) of Decision 2008/633/JHA and of EES pursuant to Article 72(4) of Regulation (EU) 2017/2226;’;

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

‘(v) make comments on the European Data Protection Supervisor’s reports on the audits pursuant to Article 45(2) of Regulation (EC) No 1987/2006, Article 42(2) of Regulation (EC) No 767/2008, Article 31(2) of Regulation (EU) No 603/2013 and Article 56(2) of Regulation (EU) 2017/2226 and ensure appropriate follow-up to those audits;’;

(d) the following point is inserted:

‘(xa) publish statistics related to the EES pursuant to Article 63 of Regulation (EU) 2017/2226;’;

(e) the following point is inserted:

‘(za) ensure annual publication of the list of competent authorities pursuant to Article 65(2) of Regulation (EU) 2017/2226;’;

(6) in Article 15, paragraph 4 is replaced by the following:

‘4. Europol and Eurojust may attend the meetings of the Management Board as observers when a question concerning SIS II, in relation to the application of Decision 2007/533/JHA, is on the agenda. Europol may also attend the meetings of the Management Board as an observer when a question concerning VIS, in relation to the application of Decision 2008/633/JHA, a question concerning Eurodac, in relation to the application of Regulation (EU) No 603/2013, or a question concerning the EES, in relation to the application of Regulation (EU) 2017/2226, is on the agenda.’;

(7) Article 17 is amended as follows:

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

‘(g) without prejudice to Article 17 of the Staff Regulations, establish confidentiality requirements in order to comply with Article 17 of Regulation (EC) No 1987/2006, Article 17 of Decision 2007/533/JHA, Article 26(9) of Regulation (EC) No 767/2008, Article 4(4) of Regulation (EU) No 603/2013 and Article 37(4) of Regulation (EU) 2017/2226;’;

▼B

(b) in paragraph 6, the following point is added:

‘(k) reports on the state of play of the development of the EES referred to in Article 72(2) of Regulation (EU) 2017/2226.’;

(8) Article 19 is amended as follows:

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

‘(da) EES Advisory Group;’;

(b) paragraph 3 is replaced by the following:

‘Europol and Eurojust may each appoint a representative to the SIS II Advisory Group. Europol may also appoint a representative to the VIS, Eurodac and EES Advisory Groups.’.

CHAPTER IX

FINAL PROVISIONS

Article 63

Use of data for reporting and statistics

1. The duly authorised staff of the competent authorities of Member States, the Commission and eu-LISA shall have access 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 10(2):

(a) status information;

(b) nationality, sex and year of birth of the third-country national;

(c) date and border crossing point of the entry to a Member State and date and border crossing point of the exit from a Member State;

(d) the type of the travel document and the three letter code of the issuing country;

(e) the number of persons identified as overstayers referred to in Article 12, the nationalities of persons identified as overstayers and the border crossing point of entry;

(f) the data entered in respect of any stay revoked or any stay whose validity is extended;

(g) the three letter code of the Member State that issued the visa, if applicable;

(h) the number of persons exempt from the requirement to give fingerprints pursuant to Article 17(3) and (4);

▼B

(i) the number of third-country nationals refused entry, the nationalities of third-country nationals refused entry, the type of border (land, air or sea) of the border crossing point at which entry was refused and the reasons for which entry has been refused as referred to in point (d) of Article 18(6).

The duly authorised staff of the European Border and Coast Guard Agency established by Regulation (EU) 2016/1624 of the European Parliament and of the Council [1] shall have access 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 11 and 13 of that Regulation.

▼M2

2. For the purpose 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 the Regulation (EU) 2019/817.

▼B

3. The procedures put in place by eu-LISA to monitor the development and the functioning of the EES referred to in Article 72(1) shall include the possibility to produce regular statistics for ensuring that monitoring.

4. Every quarter, eu-LISA shall publish statistics on the EES showing in particular the number, nationality, age, sex, duration of stay and border crossing point of entry of overstayers, of third-country nationals who were refused entry, including the grounds for refusal, and of third-country nationals whose authorisation for stay was revoked or extended, as well as the number of third-country nationals exempt from the requirement to give fingerprints.

▼M2

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

▼B

5. 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 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 national supervisory authorities.

6. At the request of the Commission, eu-LISA shall provide it with statistics on specific aspects related to the implementation of this Regulation as well as the statistics pursuant to paragraph 3.

[1] Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC (OJ L 251, 16.9.2016, p. 1).

▼B

Article 64

Costs

1. The costs incurred in connection with the establishment and operation of the EES Central System, the Communication Infrastructure, the NUI, the web service and the data repository referred to in Article 63(2) shall be borne by the general budget of the Union.

2. Costs incurred in connection with the integration of the existing national border infrastructure and its connection to the NUI as well as in connection with hosting the NUI shall be borne by the general budget of the Union.

The following costs shall be excluded:

(a) Member States' project management office (meetings, missions, offices);

(b) hosting of national IT systems (space, implementation, electricity, cooling);

(c) operation of national IT systems (operators and support contracts);

(d) customisation of existing border checks and policing systems for national entry-exit systems;

(e) project management of national entry-exit systems;

(f) design, development, implementation, operation and maintenance of national communication networks;

(g) automated border control systems, self-service systems and e-gates.

3. The costs incurred by the central access points referred to in Articles 29 and 30 shall be borne, respectively, by each Member State and Europol. The costs for the connection of those central access points to the NUI and to the EES shall be borne by each Member State and Europol, respectively.

4. Each Member State and Europol shall set up and maintain at their expense the technical infrastructure necessary to implement Chapter IV and shall be responsible for bearing the costs resulting from access to the EES for that purpose.

▼M1

5. Funding to be mobilised from the envelope referred to in point (b) of Article 5(5) of Regulation (EU) No 515/2014 to cover the costs referred to in paragraphs 1 to 4 of this Article shall be implemented under indirect management for the costs incurred by eu-LISA and under shared management for the costs incurred by the Member States.

▼B

Article 65

Notifications

1. Member States shall notify the Commission of the authority which is to be considered as controller as referred to in Article 39.

2. Member States shall notify the Commission and eu-LISA of the competent authorities referred to in Article 9(2) which have access to enter, rectify, complete, erase, consult or search data. Three months after the EES has started operations in accordance with Article 66, eu-LISA shall publish a consolidated list of those authorities in the *Official Journal of the European Union*. Member States shall also notify without delay any changes thereto. In the event of such changes, eu-LISA shall publish once a year an updated consolidated version of that information.

3. Member States shall notify the Commission and eu-LISA of their designated authorities and of their central access points referred to in Article 29 and shall notify without delay any amendments thereto.

4. Europol shall notify the Commission and eu-LISA of the authority it designates and its central access point referred to in Article 30 and shall notify without delay any amendments thereto.

5. eu-LISA shall notify the Commission of the successful completion of the test referred to in point (b) of Article 66(1).

6. The Commission shall publish the information referred to in paragraphs 1, 3 and 4 in the *Official Journal of the European Union*. In the event of changes thereto, the Commission shall publish once a year an updated consolidated version of that information. The Commission shall maintain a continuously updated public website containing that information.

Article 66

Start of operations

1. The Commission shall decide the date from which the EES is to start operations, after the following conditions are met:

(a) the measures referred to in Article 36 and Article 50(4) and (5) have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the EES, which is to be conducted by eu-LISA in cooperation with the Member States;

(c) the Member States have validated the technical and legal arrangements to collect and transmit the data referred to in Articles 16 to 20 to the EES and have notified them to the Commission;

(d) the Member States have notified the Commission as referred to in Article 65(1), (2) and (3).

▼B

2. The EES shall be operated by:

(a) the Member States which apply the Schengen *acquis* in full; and

(b) the Member States which do not yet apply the Schengen *acquis* in full but for which all the following conditions are met:

(i) the verification in accordance with applicable Schengen evaluation procedures has been successfully completed;

(ii) the provisions of the Schengen *acquis* relating to the SIS have been put into effect in accordance with the relevant Act of Accession; and

(iii) the provisions of the Schengen *acquis* relating to the VIS which are necessary for the operation of the EES as defined in this Regulation have been put into effect in accordance with the relevant Act of Accession.

3. A Member State which is not covered by paragraph 2 shall be connected to the EES as soon as the conditions referred to in points (b), (c) and (d) of paragraph 1 and point (b) of paragraph 2 are met. The Commission shall decide the date from which the EES is to start its operations in those Member States.

4. The Commission shall inform the European Parliament and the Council of the results of the test carried out pursuant to point (b) of paragraph 1.

5. The Commission decision referred to in paragraphs 1 and 3 shall be published in the *Official Journal of the European Union*.

6. The Member States and Europol shall start using the EES from the date determined by the Commission in accordance with paragraph 1 or, where applicable, with paragraph 3.

Article 67

Ceuta and Melilla

This Regulation shall not affect the special rules applying to the cities of Ceuta and Melilla, as defined in the Declaration of the Kingdom of Spain on the cities of Ceuta and Melilla in the Final Act to the Agreement on the Accession of the Kingdom of Spain to the Convention implementing the Schengen Agreement of 14 June 1985.

Article 68

Committee procedure

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

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Article 69

Advisory Group

An Advisory Group shall be established by eu-LISA in order to provide it with the expertise related to the EES, in particular in the context of the preparation of its annual work programme and its annual activity report. During the design and development phase of the EES, Article 37(2) shall apply.

▼B

Article 70

Training

eu-LISA shall perform tasks related to provision of training on the technical use of the EES in accordance with Regulation (EU) No 1077/2011.

Article 71

Practical handbook

The Commission shall, in close cooperation with the Member States, eu-LISA and other relevant agencies, make available a practical handbook for the implementation and management of the EES. The practical handbook shall provide technical and operational guidelines, recommendations and best practices. The Commission shall adopt the practical handbook in the form of a recommendation.

Article 72

Monitoring and evaluation

1. eu-LISA shall ensure that procedures are in place to monitor the development of the EES in light of objectives relating to planning and costs and to monitor the functioning of the EES in light of objectives relating to the technical output, cost-effectiveness, security and quality of service.

2. By 30 June 2018, and every six months thereafter during the development phase of the EES, eu-LISA shall submit a report to the European Parliament and to the Council on the state of play of the development of the EES Central System, the Uniform Interfaces and the Communication Infrastructure between the EES Central System and the Uniform Interfaces. That report shall contain detailed information about the costs incurred and information as to any risks which may impact the overall costs of the EES to be borne by the general budget of the Union in accordance with Article 64(1) and the first subparagraph of Article 64(2). Following the development of the EES, eu-LISA shall submit a report to the European Parliament and to the Council explaining in detail how the objectives, in particular relating to planning and costs, were achieved, as well as justifying any divergences.

3. For the purposes of technical maintenance, eu-LISA shall have access to the necessary information relating to the data processing operations performed in the EES.

4. Two years after the start of operations of the EES and every two years thereafter, eu-LISA shall submit to the European Parliament, to the Council and to the Commission a report on the technical functioning of EES, including the security thereof.

5. Three years after the start of operations of the EES and every four years thereafter, the Commission shall produce an overall evaluation of the EES. This overall evaluation shall include:

(a) an assessment of the application of this Regulation;

(b) an examination of the results achieved against objectives and the impact on fundamental rights;

(c) an assessment of the continuing validity of the underlying rationale of the EES;

▼B

(d) an assessment of the adequacy of the biometric data used for the proper functioning of the EES;

(e) an assessment of the use of stamps in the exceptional circumstances referred to in Article 21(2);

(f) an assessment of the security of the EES;

(g) an assessment of any implications, including any disproportionate impact on the flow of traffic at border crossing points and those with a budgetary impact on the Union budget.

The evaluations shall include any necessary recommendations. The Commission shall transmit the evaluation report to the European Parliament, to the Council, to the European Data Protection Supervisor and to the European Union Agency for Fundamental Rights established by Council Regulation (EC) No 168/2007 ([1]).

Those evaluations shall also include an assessment of the use made of the provisions referred to in Article 60 both in terms of frequency — number of third-country nationals making use of these provisions per Member State, their nationality and average duration of their stay — and practical implications, and shall take into account any related developments in the Union's visa policy. The first evaluation report may include options in view of phasing out the provisions referred to in Article 60 and replacing them with a Union instrument. It shall be accompanied, where appropriate, by a legislative proposal amending the provisions referred to in Article 60.

6. The Member States and Europol shall provide eu-LISA and the Commission with the information necessary to draft the reports referred to in paragraphs 4 and 5 according to the quantitative indicators predefined by the Commission, eu-LISA, or both. This information shall not jeopardise working methods or include information that reveals sources, staff members or investigations of the designated authorities.

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

8. 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 EES data for law enforcement purposes containing information and statistics on:

(a) whether the consultation was carried out for the purpose of identification or for entry/exit records, and the type of terrorist offence or serious criminal offence that led to the consultation;

(b) the grounds given to substantiate the suspicion that the person concerned was covered by this Regulation;

([1]) Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights (OJ L 53, 22.2.2007, p. 1).

▼B

(c) the grounds given not to launch the consultation of other Member States' automated fingerprint identification systems under Decision 2008/615/JHA in accordance with point (b) of Article 32(2) of this Regulation;

(d) the number of requests for access to the EES for law enforcement purposes;

(e) the number and type of cases in which access to the EES for law enforcement purposes led to successful identifications;

(f) the number and type of cases in which the urgency procedures referred to in Article 31(2) and in the second subparagraph of Article 32(2) were used, including those cases where that urgency was not accepted by the *ex post* verification carried out by the central access point.

A technical solution shall be made available to Member States in order to facilitate the collection of the data listed in the first subparagraph of this paragraph for the purpose of generating statistics referred to in this paragraph. The Commission shall adopt implementing acts concerning the specifications of the technical solution. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 68(2).

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

Article 73

Entry into force and applicability

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 decided by the Commission in accordance with Article 66(1) thereof, with the exception of the following provisions, which shall apply from 29 December 2017: Articles 5, 36, 37, 38, 43, 51 of this Regulation; point (5) of Article 61 of this Regulation, as regards Article 17a(5) of Regulation (EC) No 767/2008; point (10) of Article 61 of this Regulation, as regards Article 26(3a) of Regulation (EC) No 767/2008; and Articles 62, 64, 65, 66, 68, 69 and 70 and Article 72(2) of this Regulation.

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

▼B

ANNEX I

LIST OF INTERNATIONAL ORGANISATIONS REFERRED TO IN ARTICLE 41(2)

1. UN organisations (such as the UNHCR);

2. The International Organization for Migration (IOM);

3. The International Committee of the Red Cross.

▼B

ANNEX II

SPECIFIC PROVISIONS FOR THIRD-COUNTRY NATIONALS WHO CROSS THE BORDER ON THE BASIS OF A VALID FTD

(1) By way of derogation from Article 16(1) to (3) of this Regulation, for third-country nationals who cross a border on the basis of a valid FTD, the border authorities shall:

(a) create or update their individual file containing the data referred to in points (a), (b) and (c) of Article 17(1) of this Regulation. In addition, their individual file shall indicate that the third-country national concerned holds an FTD. That indication shall automatically result in the addition of the multiple entry characteristic of the FTD to the entry/exit record,

(b) enter in an entry/exit record for each of the entries performed on the basis of a valid FTD the data set out in points (a), (b) and (c) of Article 16(2) of this Regulation, as well as the indication that the entry was performed on the basis of an FTD.

In order to calculate the maximum duration of the transit, the date and time of entry shall be considered as the starting point of that duration. The date and time of expiry of the authorised transit shall be calculated automatically by the EES in accordance with Article 3(2) of Regulation (EC) No 693/2003.

(2) In addition, at the first entry on the basis of an FTD, the date of expiry of the validity of the FTD shall be entered into the entry/exit record.

(3) Article 16(3) and (4) shall apply *mutatis mutandis* to third-country nationals holding an FTD.

(4) For verification at a border at which the EES is operated and within the territory of the Member States, third-country nationals who cross the border on the basis of a valid FTD shall be subject, *mutatis mutandis*, to the verifications and identifications provided for under Articles 23 and 26 of this Regulation and Article 19a of Regulation (EC) No 767/2008 that are applicable to visa-exempt third-country nationals.

(5) Points (1) to (4) shall not apply to third-country nationals who cross the border on the basis of a valid FTD, provided that all of the following conditions are met:

(a) they transit by train; and

(b) they do not disembark within the territory of a Member State.