Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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 of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Economic and Social Committee[1],

Having regard to the opinion of the Committee of the Regions[2],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The Communication of the Commission of 13 February 2008 entitled 'preparing the next steps in border management in the European Union'[3] outlined the need, as part of the European integrated border management strategy, to establish an Entry/Exit System (EES) which registers electronically the time and place of entry and exit of third country nationals admitted for a short stay to the territory of the Member States and which calculates the duration of their authorised stay.

(2) The European Council of 19 and 20 June 2008 underlined the importance of continuing to work on the development of the EU's integrated border management strategy, including better use of modern technologies to improve the management of external borders.

(3) The Communication of the Commission of 10 June 2009, entitled 'An area of freedom, security and justice serving the citizens', advocates establishing an electronic system for recording entry to and exit from Member States' territory via the crossing of external borders to ensure more effective management of access to this territory.

(4) The European Council of 23 and 24 of June 2011 called for work on "smart borders" to be pushed forward rapidly. The Commission published a Communication "Smart borders – options and the way ahead" on 25 October 2011.

(5) The European Council in its Strategic guidelines adopted in June 2014 stressed that "*the Schengen area, allowing people to travel without internal border controls, and the increasing numbers of people travelling to the EU require efficient management of the EU's common external borders to ensure strong protection. The Union must mobilise all*

1 OJ C , , p. .

2 OJ C , , p. .

3 COM(2008)0069 final.

the tools at its disposal to support the Member States in their task. To this end: integrated Border Management of external borders should be modernised in a cost efficient way to ensure smart border management inter alia with an entry-exit system and supported by the new agency for large-scale IT systems (eu-LISA)".

(6) The Communication of the Commission of 13 May 2015 entitled "A European agenda on migration" noted that "*a new phase would come with the "Smart Borders" initiative to increase the efficiency of border crossings, facilitating crossings for the large majority of 'bona fide' third country travellers, whilst at the same time strengthening the fight against irregular migration by creating a record of all cross-border movements by third country nationals, fully respecting proportionality".*

(6a) With a view to further improving the management of the external borders and, in particular, in order to verify the respect of the provisions on an authorised period of stay within the territory of the Member States, a system, called Entry/Exit System (EES), which registers electronically the time and place of entry and exit of third-country nationals admitted for a short stay to the territory of the Member States and which calculates the duration of their authorised stay should be established. It replaces the obligation to stamp passports of third country nationals which is applicable by all Member States.

(7) It is necessary to specify the objectives of the EES, the categories of data to be entered into the EES, the purposes for which the data are to be used, the criteria for their entry, the authorities authorised to access the data, further rules on data processing and the protection of personal data as well as the technical architecture of the system, rules concerning its operation and use and interoperability with other information systems. It is also necessary to define responsibilities for the system.

(8) The EES should apply to third country nationals admitted for a short stay to the territory of the Member States. It should also apply to third country nationals whose entry for a short stay has been refused.

(8a) The EES should be operated at the external borders of the Member States which apply the Schengen acquis in full. It is desirable that Member States not yet applying the Schengen acquis in full, apply it fully by the start of the operation of the EES. However, in case where the lifting of controls at internal borders cannot be achieved by the start of the operation of the EES, it is necessary to specify the conditions for the operation of the EES by these Member States and the provisions on the operation and use of the EES at internal borders where controls would have not yet been lifted.

As regards the conditions, the EES should be operated at the external borders of the Member States which do not yet apply the Schengen acquis in full but for which the verification in accordance with the applicable Schengen evaluation procedure has already been successfully completed, to which passive access to the Visa Information System (VIS) for the purpose of operating the EES has been granted and for which the provisions of the Schengen acquis relating to the Schengen Information System have been put into effect in accordance with the relevant Accession Treaty. As regards the specific provisions on the operation and use of the EES by the Member States fulfilling such conditions, the EES should be operated at all internal borders of those Member States where the controls have not yet been lifted. However, specific provisions with regard of the EES at such borders should apply, justified by reasons of economy of the process of the checks on such borders, while not affecting the level of security and the correct functioning of the EES and without prejudice to the other border control obligations under Regulation (EU) 2016/399.

(8aa) The length of the authorised stay of third country nationals in the territories of the Member States for the purpose of this Regulation results from the Schengen *acquis* applicable

(8b) The calculator included in the EES should take into account stays in the territory of the Member States which operate the EES for the calculation of the overall limit of 90 days in a 180-day period. Any extensions of authorised stay should be taken into account for the purpose of calculation of the overall limit of 90 days in any 180-day period upon the subsequent entry of the third country national to the territory of the Member States.

Pending their connection to the EES, stays in the territories of the Member States which do not operate the EES should be counted separately, on the basis of stamps affixed in the travel documents of third country nationals

(8c) Stays in Member States which do not yet apply the Schengen *acquis* in full but operate the EES should only be taken into account by the calculator for the purposes of verifying compliance with the overall limit of 90 days in any 180-day period and for the purposes of verifying the period of validity of the Schengen short stay visa.

The calculator should not calculate the duration of stay as authorised by a national short stay visa issued by a Member State which does not yet apply the Schengen *acquis* in full but operates the EES.

The calculator should not take into account stays in Member States which do not yet apply the Schengen *acquis* in full but operate the EES, when calculating the duration of stay authorised by a Schengen short stay visa.

(8d) Precise rules should be laid down as regards the responsibilities for the development and operation of the EES and the responsibilities of the Member States for the connection to the EES.. The 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 of the European Parliament and of the Council[4], should be responsible for the development and operational management of a centralised EES in accordance with this Regulation and the relevant provisions of Regulation (EU) No 1077/2011 should be amended accordingly.

(9) The objective of the EES should be to improve the management of external borders, to prevent irregular immigration and to facilitate the management of migration flows. The EES should, in particular and when relevant, contribute to the identification of any person who does not or no longer fulfils the conditions of duration of the authorised stay within the territory of the Member States. Additionally, the EES should contribute to the prevention, detection and investigation of terrorist offences and of other serious criminal offices.

(9a) The EES should consist of a Central System, which operates a computerised central database of biometric and alphanumeric data, a National Uniform Interface in each Member State, a Secure Communication Channel between the EES Central System and the Central Visa Information System (VIS Central System) of the Visa Information System (VIS), established by Council Decision 2004/512/EC[5], and the secure and encrypted Communication Infrastructure between the Central System and the National Uniform Interfaces. Each Member State should connect its national border infrastructures to the National Uniform Interface in a secure manner. In order to enable statistics and reporting, a data repository should be established at central level. In order to enable third country

---

4 Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 286, 1.11.2011, p 1).

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

nationals and carriers to verify at any moment the remaining authorised period of stay a web service should be developed. Relevant stakeholders should be consulted in the development phase of the web service. In establishing the technical specifications for accessing the carrier web service, the impact on passenger travel and carriers should be limited to the extent possible. For this purpose, appropriate integration with relevant systems should be considered.

(9b) Interoperability should be established between the EES and the VIS by way of a direct communication channel between the VIS Central System and the EES Central System to enable the border authorities using the EES to consult the VIS in order to retrieve visa-related data to create or update the entry/exit record or refusal of entry record, to enable the border authorities to verify the validity of the visa and the identity of the visa holder by means of fingerprints directly against the VIS at the borders at which the EES is operated and to enable the border authorities to verify the identity of visa exempt third country nationals against the VIS with fingerprints. Interoperability should also enable the border authorities and visa authorities using the VIS to directly consult the EES from the VIS for the purposes of examining visa applications and decisions relating to those applications and enabling visa authorities to update the visa-related data in the EES in the event that a visa is annulled, revoked or extended. Regulation (EC) No 767/2008 of the European Parliament and of the Council[6] should be amended accordingly. The launch of the automated processes between the EES and the VIS should in each case be subject to a confirmation by the authority concerned. The purpose limitation principle should be respected when establishing interoperability between the EES and VIS.

(9d) This Regulation should define the authorities of the Member States which may be authorised to have access to the EES to enter, amend, delete or consult data for the specific purposes of the EES and to the extent necessary for the performance of their tasks.

(9e) Any processing of EES data should be proportionate to the objectives pursued and necessary for the performance of the tasks of the competent authorities. When using the EES, the competent authorities should ensure that the human dignity and integrity of the person whose data are requested, are respected and should not discriminate against persons on grounds of sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

(10) The EES should collect and process alphanumeric data and biometric data (fingerprints and facial image) primarily for the purposes of improving the management of external borders, preventing irregular immigration and facilitating the management of migration flows. Furthermore, personal data collected in the EES may also be accessed to contribute to the prevention, detection and investigation of terrorist offences and of other serious criminal offices only under the conditions laid down in this Regulation. The use of biometrics, despite its impact on the privacy of travellers, is justified for two reasons. Firstly, biometrics are a reliable method to identify third country nationals within the territory of the Member States not in possession of travel documents or any other means of identification, a common situation for irregular migrants. Secondly, biometrics provide for the more reliable matching of entry and exit data of legal travellers. Where facial images are used in combination with fingerprint data, it allows for the reduction of fingerprints registered while enabling the same result in terms of accuracy of the identification.

(11) Four fingerprints of visa exempt third country nationals should be enrolled in the EES, if physically possible, to allow for accurate verification and identification (ensuring that the

---

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

third country national is not already enrolled under another identity or with another travel document) and to guarantee that sufficient data is available to achieve the objectives of the EES in every circumstance. The check of the fingerprints of visa holders will be done against the Visa Information System. (VIS) established by Council Decision 2004/512/EC7. The facial image of both visa exempt and visa holding third country nationals should be registered in the EES. Fingerprints or facial image should be used as a biometric identifier for verifying the identity of third country nationals who have been previously registered in the EES and for as long as their individual file has not been deleted. In order to take into account the specificities of each border crossing point and the different kind of borders, the national authorities should define for each border crossing whether the fingerprints or the facial image should be used as the main biometric identifier to perform the required verifications.

(12) (…)

(13) (…)

(14) (…)

(15) (…)

(16) In the fight against terrorist offences and other serious criminal offences, it is necessary that designated authorities have the most up-to-date information if they are to perform their tasks. Access to VIS data for law enforcement purpose has already proven its usefulness in identifying people who died violently or for helping investigators to make substantial progress in cases related to human being trafficking, terrorism or drug trafficking. Access to the information contained in the EES is necessary to prevent, detect and investigate terrorist offences as referred to in Council Framework Decision 2002/475/JHA[8] or other serious criminal offences as referred to in Council Framework Decision 2002/584/JHA[9]. The data generated by the EES may be used as an identity verification tool both in cases where the third country national has destroyed his/her documents and where designated authorities are investigating a crime through the use of fingerprints or facial image and wish to establish an identity. It may also be used as a tool to construct evidence by tracking the travel routes of a person suspected of having committed a crime or a victim of crime. Therefore, the data in the EES should be available, to the designated authorities of the Member States and the European Police Office ('Europol'), subject to the conditions and limitations set out in this Regulation. The conditions of access to the EES for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences should be such as to allow the designated authorities of the Member States to tackle the cases of suspects using multiple identities. For this purpose obtaining a hit during a consultation of a relevant database prior to acceding the EES should not prevent such access. From the perspective of the law enforcement purposes and in order to prevent, detect and investigate terrorist offences or other serious criminal offences a search of the database is proportionate if there is an overriding public security concern. Any search must be duly justified and proportionate in the light of the interest invoked.

(16a) Only designated authorities which are responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences for which Member States can guarantee that all provisions of this Regulation as well as those of Directive (EU) 2016/680 as transposed into national law apply and for which the correct application

---

8 Council Framework Decision 2002/475/JHA of 13 June 2002 on combatting terrorism (OJ L 164, 22.6.2002 p.6).

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

may be verified by the competent authorities including the supervisory authority established in accordance with Article 41(1) of Directive (EU) 2016/680 should be entitled to consult the data stored in the EES.

(17) Moreover, Europol plays a key role with respect to cooperation between Member States' authorities in the field of cross-border crime investigation in supporting Union-wide crime prevention, analyses and investigation. Consequently, Europol should also have access to the EES within the framework of its tasks and in accordance with Regulation (EU) 2016/794 of the European Parliament and of the Council[10]. The European Data Protection Supervisor should monitor the processing of data by Europol and ensure full compliance with applicable data protection rules.

(18) Access to the EES for the purpose of preventing, detecting or investigating terrorist offences or other serious criminal offences constitutes an interference with the fundamental rights to respect for the private life of individuals and to protection of personal data of persons whose personal data are processed in the EES. Any such interference must be in accordance with the law, which must be formulated with sufficient precision to allow individuals to adjust their conduct and it must protect individuals against arbitrariness and indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise. Any interference must be necessary in a democratic society to protect a legitimate and proportionate interest and proportionate to the legitimate objective to achieve.

(19) Comparisons of data on the basis of a latent fingerprint, which is the dactyloscopic trace which may be found at a crime scene, is fundamental in the field of police cooperation. The possibility to compare a latent fingerprint with the fingerprint data which is stored in the EES in cases where there are reasonable grounds for believing that the perpetrator or victim may be registered in the EES is necessary for the designated authorities of the Member States to prevent, detect or investigate terrorist offences or other serious criminal offences, when for example the only evidence at a crime scene are latent fingerprints.

(20) It is necessary to designate the competent authorities of the Member States as well as the central access point through which the requests for access to EES data are made and to keep a list of the operating units within the designated authorities that are authorised to request such access for the specific purposes for the prevention, detection or investigation of terrorist offences or of other serious criminal offences.

(21) Requests for access to data stored in the Central System should be made by the operating units within the designated authorities to the central access point and should be duly justified. The operating units within the designated authorities that are authorised to request access to EES data should not act as a verifying authority. The central access point should be a body or entity entrusted by national law to exercise public authority and be capable, through the quality and the quantity of its staffing, to effectively verify that the conditions to request access to the EES are fulfilled in the concrete case at hand. The central access points should act independently of the designated authorities and should be responsible for ensuring, in an independent manner, strict compliance with the conditions for access as established in this Regulation. In a case of urgency, where early access is necessary to respond to a specific and actual threat related to terrorist offences or other serious criminal offences, the central access point should be able to process the request immediately and only carry out the verification afterwards.

---

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

(22) To protect personal data and to exclude systematic searches, the processing of EES data should only take place in specific cases and when it is necessary for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences. The designated authorities and Europol should only request access to the EES when they have reasonable grounds to believe that such access will provide information that will substantially assist them in preventing, detecting or investigating a terrorist offence or other serious criminal offence.

(23) In addition, access to the EES for identification of unknown suspects, perpetrators or victims of terrorist offences or other serious criminal offences should be allowed only on the condition that searches in the national databases of the Member State have been carried out. In addition, the search with the automated fingerprinting identification systems of all other Member States under Council Decision 2008/615/JHA[11] has been fully conducted, or the search has not been fully conducted within 2 days of being launched

(24) For the purpose of efficient comparison and exchange of personal data, Member States should fully implement and make use of the existing international agreements as well as of Union law concerning the exchange of personal data already in force, in particular of Decision 2008/615/JHA.

(25) The personal data stored in the EES should be kept for no longer than strictly necessary for the purposes for which the data are processed. It is sufficient to keep in the EES the data related to third country nationals who have respected the duration of authorised stay for a period of three years for border management purposes in order to avoid the need for third country nationals to re-enrol in the EES before that period has lapsed. The three-year data retention period will reduce the frequency of re-enrolments and will be beneficial for all travellers as both the average border crossing time and the waiting time at border crossing points will decrease. Even for a traveller entering only once in the territory of the Member States , the fact that other travellers already registered in the EES do not have to re-enrol before the expiry of this three-year period will reduce the waiting time at the border crossing point. This three-year data retention period is also necessary to facilitate and expedite border crossings including by using automated and self-service systems. It is also appropriate to set a three-year data retention period for third-country nationals whose entry for a short stay has been refused For third country nationals who are family members of a Union citizen to whom Directive 2004/38/EC[12] applies or of a national of a third country enjoying the right of free movement under Union law and who do not hold a residence card referred to under Directive 2004/38/EC, it is appropriate to store each coupled entry/ exit record for a maximum period of one year after the exit. Following the expiry of the relevant data retention periods the data should be automatically erased.

(25a) A retention period of five ears is necessary for data on third-country nationals who have not exited the territory of the Member States within the authorised period of stay in order to support the identification and return process. The data should be automatically erased after the period of five years, unless there are grounds to delete it earlier.

(26) A *three* year data retention period ~~is~~ *for the personal data of third-country nationals who have respected the duration of authorised stay and of third-country nationals whose entry for a short stay has been refused and a five year data retention period for the personal*

---

11 Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 1).

12 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).

data of third country nationals who have not exited the territory of the Member States within the authorised period of stay are necessary to allow the border guard *to perform* the necessary risk analysis requested by the Schengen Borders Code before authorising a traveller *to enter* the territory of the Member States. The processing of visa *applications* in consular posts *also* requires analysing the travel history of the applicant to assess the use of previous visas and *whether* the conditions of authorised stay *have been respected*. The abandoning of passport stamping will be compensated by a consultation of the EES. The travel history available in the system should therefore cover a period of time which is sufficient for the purpose of visa issuance.

While performing the risk analysis at the border and while processing a visa application, the travel history of third-country nationals should be checked in order to determine whether they have exceeded the maximum duration of their authorised stay in the past. It is thus necessary to retain the personal data of third-country nationals who have not exited the territory of the Member States within the authorised period of stay for the longer period of five years compared to that for the personal data of the third-country nationals who have respected the duration of authorised stay and of third-country nationals whose entry for a short stay has been refused.

(27) (…)

(28) (…)

(29) Rules on the liability of the Member States in respect to damage arising from any breach of this Regulation should be laid down.

(30) Without prejudice to more specific rules laid down in this Regulation for the processing of personal data, Regulation (EU) 2016/679 of the European Parliament and of the Council[13] applies to the processing of personal data by the Member States in application of this Regulation unless such processing is carried out by the designated authorities or central access points of the Member States for the purposes of the prevention, *investigation, or* detection of terrorist offences or of other serious criminal offences.

(31) Without prejudice to more specific rules laid down in this Regulation for the processing of personal data, the national laws, regulations and administrative provisions adopted pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council[12a] apply to the processing of personal data by the competent authorities of the Member States for the purposes of the prevention, investigation, or detection of terrorist offences or of other serious criminal offences pursuant to this Regulation[14].

(32) Regulation (EC) No 45/2001 of the European Parliament and the Council[15] applies to the activities of the Union institutions or bodies when carrying out their tasks as responsible for the operational management of EES.

(33) Personal data obtained by Member States pursuant to this Regulation should not be transferred or made available to a third country, an international organisation or any private party established in or outside the Union except if necessary in individual cases in order to

---

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

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

15 Regulation (EC) No 45/2001 of the European Parliament and the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

assist the identification of a third country national in relation to his/her return and subject to strict conditions. In the absence of an adequacy decision pursuant to Article 45(3) of the GDPR or of appropriate safeguards pursuant to Article 46 of the GDPR, personal data of third country nationals for the purpose of return stored in the EES can exceptionally be transferred to a third country or to an international organisation, only if it is necessary for important reasons of public interest as referred to in Art. 49(1)(d) of GDPR.

(33b) Personal data obtained by Member States pursuant to this Regulation may also be transferred to a third country in an exceptional case of urgency, where there is an imminent danger associated with a terrorist offence or an imminent danger for ~~or~~ the life of a person ~~is~~ associated with a serious criminal offence as defined in accordance with Framework Decision 2008/977/JHA.

An imminent danger for the life of a person should be understood as covering a danger from a serious criminal offence against that person such as grievous bodily injury, illicit trade in human organs and tissue, kidnapping, illegal restraint and hostage-taking, sexual exploitation of children and child pornography, rape.

Such data should only be transferred to a third country if 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.

The information contained in the EES may be provided to Member States not operating the EES, and to Member States to which this Regulation does not apply, by the competent authorities of the Member States whose designated authorities have access to the EES pursuant to this Decision. Such provision of information should be subject to a duly motivated request, and limited to where it is necessary for the prevention, detection or investigation of a terrorist offence or another serious criminal offence. A Member State that operates the EES may only provide such information if a reciprocal provision of any information on entry/exit records held by the requesting Member State to the Member States operating the EES is ensured. Directive (EU) 2016/680 applies to all the subsequent treatment of data obtained from the EES.

(34) The independent supervisory authorities established in accordance with Article *51* of Regulation (EU) 2016/679 should monitor the lawfulness of the processing of personal data by the Member States, whilst the European Data Protection Supervisor as established by Regulation (EC) No 45/2001 should monitor the activities of the Union institutions and bodies in relation to the processing of personal data. The European Data Protection Supervisor and the supervisory authorities should cooperate with each other in the monitoring of the EES.

(35) National supervisory authorities established in accordance with Article 41 of Directive (EU) 2016/680 should monitor the lawfulness of the processing of personal data for law enforcement purposes by the Member States.

(36) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 21 September 2016.

(37) The proposal establishes strict access rules to the EES system and the necessary safeguards. It also sets out the individuals' rights of access, rectification, completion, erasure and redress, in particular the right to a judicial remedy and the supervision of processing operations by public independent authorities. This Regulation therefore respects the fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the European Union, in particular the right to dignity (Article 1 of the Charter); the prohibition of slavery and forced labour (Article 5 of the Charter); the right to liberty and security (Article 6 of the Charter), respect for private and family life (Article 7 of the Charter), the protection of personal data (Article 8 of the Charter), the

right to non-discrimination (Article 21 of the Charter), the rights of the child (Article 24 of the Charter), the rights of elderly (Article 25 of the Charter), the rights of persons with disabilities (article 26 of the Charter) and the right to an effective remedy (Article 47 of the Charter).

(37a) This Regulation is without prejudice to the obligations deriving from the Geneva Convention Relating to the Status of Refugees of 28 July 1951, as supplemented by the New York Protocol of 31 January 1967.

(37b) Further to the provisions on information to be provided in accordance with Regulation (EU) 2016/679, third country nationals whose data is to be recorded in EES should be provided with appropriate information in relation to the recording of their data in the EES. This information should be provided by Member States in writing by any appropriate means, including leaflet, poster or appropriate electronic means.

(38) The effective monitoring of the application of this Regulation requires evaluation at regular intervals. The Member States should lay down rules on penalties applicable to infringements of the provisions of this Regulation and ensure that they are implemented.

(39) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[16].

(40) The establishment of a common EES and the creation of common obligations, conditions and procedures for use of data cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and impact of the action, be better achieved at Union level in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, the Regulation does not go beyond what is necessary in order to achieve this objective.

(41) Following the entry into operation of the EES, Article 20(2) of the Convention implementing the Schengen Agreement should be amended with regard to bilateral agreements concluded by Member States and the authorised length of stay beyond 90 days in any 180-day period of third country nationals exempt from the visa obligation". In its overall evaluation of the EES the Commission should include an assessment of the use made of the bilateral agreements of Member States. The first evaluation report may include options in view of phasing them out and replacing them with a European instrument.

(42) The projected costs of the EES are lower than the budget earmarked for Smart Borders in Regulation (EU) 515/2014 of the European Parliament and the Council[17]. Accordingly, following the adoption of this Regulation, pursuant to Article 5(5)(b) of Regulation (EU) 515/2014, the Commission should, by means of a delegated act, re-allocate the amount currently attributed for developing IT systems supporting the management of migration flows across the external borders.

(43) (…)

(44) This Regulation is without prejudice to the application of Directive 2004/38/EC.

---

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

[17] Regulation (EU) No 515/2014 of the European Parliament and of the Council of 16 April 2014 establishing as part of the Internal Security Fund, the Instrument for financial support for external borders and visa and repealing Decision No 574/2007/EC (OJ L 150, 20.5.2014, p. 143).

(45) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Given that this Regulation builds upon the Schengen *acquis*, Denmark shall, in accordance with Article 4 of that Protocol, decide within a period of six months after the Council has decided on this Regulation whether it will implement it in its national law.

(46) This Regulation constitutes a development of the provisions of the Schengen acquis in which the United Kingdom does not take part, in accordance with Council Decision 2000/365/EC[18]; the United Kingdom is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(47) This Regulation constitutes a development of the provisions of the Schengen *acquis* in which Ireland does not take part, in accordance with Council Decision 2002/192/EC[19]; Ireland is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(48) As regards Iceland and Norway, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latters' association with the implementation, application and development of the Schengen acquis[20] which fall within the area referred to in Article 1, point A of Council Decision 1999/437/EC[21] .

(49) As regards Switzerland, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*[22] which fall within the area referred to in Article 1, point A of Council Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/146/EC[23] and with Article 3 of Council Decision 2008/149/JHA[24].

(50) As regards Liechtenstein, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss

---

18 Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis* (OJ L 131, 1.6.2000, p. 43).

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

20 OJ L 176, 10.7.1999, p. 36.

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

22 OJ L 53, 27.2.2008, p. 52.

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

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

Confederation's association with the implementation, application and development of the Schengen *acquis*[25] which fall within the area referred to in Article 1, point A of Council Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU[26] and with Article 3 of Council Decision 2011/349/EU.[27]

(51) As regards Cyprus, Bulgaria, Romania and Croatia, the provisions of this Regulation referring to SIS and VIS constitute provisions building upon, or otherwise relating to, the Schengen acquis within, respectively, the meaning of Article 3(2) of the 2003 Act of Accession, Article 4(2) of the 2005 Act of Accession and Article 4(2) of the 2011 Act of Accession read in conjunction with Council Decision 2010/365/EU28, Council Decision (EU) 2017/73329 and Council Decision of …/2017 on the putting into effect of certain provisions of the Schengen acquis relating to the Visa Information System in the Republic of Bulgaria and Romania.

In addition, the operation of the EES requires that a passive access to the VIS has been granted and that all the provisions of the Schengen acquis relating to the Schengen Information System have been put into effect in accordance with the relevant Council Decisions. These conditions can only be met once the verification in accordance with the applicable Schengen evaluation procedure has been successfully completed. Therefore, the EES should be operated only by those Member States which fulfil these conditions by the start of the operations of the EES. Member States not operating the EES from the initial start of operation should be connected to the EES in accordance with the procedure set out in this Regulation, as soon as all the above conditions are met,

---

25 OJ L 160, 18.6.2011, p. 21.

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

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

28 Council Decision of 29 June 2010 on the application of the provisions of the Schengen acquis relating to the Schengen Information System in the Republic of Bulgaria and Romania, OJ L 166, 1.7.2010, p. 17

29 Council Decision of 25 April 2017 on the application of the provisions of the Schengen acquis relating to the Schengen Information System in the Republic of Croatia, OJ L 108, 26.4.2017, p. 31

HAVE ADOPTED THIS REGULATION:

CHAPTER 1
General Provisions

Article 1
Subject matter

1. This Regulation establishes an 'Entry/Exit System' (EES) for the recording and storage of information on the date, time and place of entry and exit of third country nationals crossing the borders at which the EES is operated of the Member States, for the calculation of the duration of their authorised stay, and for the generation of alerts to Member States when the authorised stay has expired as well as for the recording 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 for the refusal.

2. For the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences, this Regulation also lays down in its Chapter IV the conditions under which Member States' designated authorities and the European Police Office (Europol) may obtain access for consultation of the EES.

Article 2
Scope

1. This Regulation applies to third country nationals admitted for a short stay in the territory of the Member States subject to border checks in accordance with Regulation (EU) 2016/399 when crossing the borders at which the EES is operated. When entering and exiting the territory of the Member States, it applies to third country nationals:

i) who are family members 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) who do not hold a residence card referred to under Directive 2004/38/EC or a residence permit pursuant to Regulation (EC) No 1030/2002.

2. This Regulation also applies to third country nationals whose entry for a short stay to the territories 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;

(b) third country nationals who are members of the family 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 who hold a residence card pursuant to Directive 2004/38/EC or a residence permit pursuant to Regulation 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;

(ca) third country nationals exercising mobility in accordance with Directive 2014/66/EU or Directive (EU) 2016/801;

(d) holders of long-stay visas;

(e) nationals of Andorra, Monaco, San Marino, and holders of a passport issued by the Vatican City State;

(f) persons or categories of persons exempt from border checks or benefiting from facilitation of border crossing as referred to in Article 6a (3)(d) of Regulation (EU) 2016/399

(g) persons or categories of persons as referred to in Article 6a (3) (e), (f), (g) and (h) of Regulation (EU) 2016/399.

This Regulation does not apply to third country nationals who are members of the family referred to in points (a) and (b) of the first subparagraph even if they are not accompanying or joining the Union citizen or a third country national enjoying the right of free movement.

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:

i) who are family members 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) who do not hold a residence card referred to under 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' mean external borders as defined in Article 2(2) of Regulation (EU) 2016/399;

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

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

(3) ‘immigration authorities’ mean the competent authorities responsible, in accordance with national law, for:

(a) checking within the territory of the Member States whether the conditions for entry to or of authorised stay in the territory of the Member States are fulfilled and/or

(b) *examining* the conditions and taking decisions related to the residence of third country nationals on the territory of the Member States insofar as these authorities do not constitute "determining authorities" as defined in Article 2(f) of Directive 2013/32/EU, and where relevant providing advice in accordance with Regulation (EU) 377/2004 and/or;

c) the return of third country nationals to a third country of origin or transit.

(4) 'visa authorities' mean the authorities as defined in Article 4(3) of Regulation (EC) No 767/2008;

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

(6) '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;

(7) 'short stay' means stays in 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;

(8) 'short stay visa' means visa as defined in Article 2(2)(a) of Regulation (EC) No 810/2009[30];

(8a) '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 in the territory of that Member State of a duration of no more than 90 days in any 180-day period;

(9) (…)

(9a) (…)

(9b) 'authorised stay' means the exact number of days during which a third country national may legally stay in the territory of Member States, counting from the date of the entry in accordance with the applicable provisions;

(10) (…)

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

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

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

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

(15) '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;

(16) 'facial image' means digital images of the face;

(17) 'biometric data' means fingerprint data and facial image;

(18) '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;

(19) '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;

(20) (…)

(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;

(22) (…)

[30] 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).

(23) (…)

(24) ‘EES data’ means all data stored in the Central System in accordance with Articles 13, 14, 15, 16, 17 and 18;

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

(26) 'terrorist offences' mean the offences under national law which correspond or are equivalent to those referred to in Articles 1 to 4 of Framework Decision 2002/475/JHA;

(26a) 'designated authorities' means authorities which are responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences and designated by Member States pursuant to Article 26.

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

(28) ‘Self Service System’ means an automated system as defined in Article 2(23) of Regulation (EU) 2016/399;

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

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

(31) ‘False Positive Identification Rate (FPIR) ‘ means the proportion of returned matches which do not belong to the checked traveller;

(32) ‘False Negative Identification Rate (FNIR) ‘ means the proportion of missed matches during biometric search although the traveller was registered with biometric data.

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 5(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 law enforcement purposes laid down in Article 5(1a) of this Regulation.

Article 3a
Borders at which the EES applies and use of the EES at these borders

1. The EES shall apply at the external borders of the Member States.

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.

2a. 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.

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

3. At the internal land borders between two Member States which do not yet apply the Schengen acquis in full but operate the EES, those Member States shall introduce the EES without biometric functionalities by derogation from Art. 21(2) third and fourth subparagraphs, as well as Art. 25. At these internal borders, where the third country national is not yet registered into the EES, the individual file shall be created without recording biometric data. Biometric data shall be added at the next border crossing where the EES is operated with the biometric functionalities.

Article 4
Set-up of the EES

'eu-LISA' shall develop the EES and ensure its operational management, including the functionalities for processing biometric data referred to in Article 14(1)(f) and Article 15 (1) (b) and (c), as well as adequate security.

Article 5
Objectives of the EES

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

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

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

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

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

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

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

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

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

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

j) (…)

k) (…)

l) (…)

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

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

(b) to enable generating information for investigations related to terrorism or other serious criminal offences, including identification of perpetrators, suspects and victims of these offences having crossed the external borders.

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

- enabling the national competent authorities referred to in Article 8e 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 23;
- notifying the border authorities that access is granted to the national facilitation programme.

Article 6
Technical architecture of the EES

1. The EES shall be composed of:

(a) a Central System;

(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 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 Central System and the National Uniform Interfaces.

(e) the web service referred to in Article 12;

(f) the data repository referred to in Article 57(2) which shall be established at a central level.

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 34(3).

3. Without prejudice to Commission Decision 2008/602/EC[27], some 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 and EES data shall be ensured.

Article 7
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 systems shall only be possible if both this Regulation and Regulation 767/2008 provide for it. Retrieval, importation and updating of visa related data directly from the VIS into the EES shall be an automated process once the operation in question is launched by the authority concerned.

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

(a) retrieve and import the visa related data directly from the VIS 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 13, 14 and 16 of this Regulation and Article 18a of Regulation (EC) No 767/2008;

(b) retrieve and import the visa related data directly from the VIS in order to update the entry/exit record in the event that a visa is annulled, revoked or extended in accordance with Article 17 of this Regulation and Articles 13, 14 and 18a of Regulation (EC) No 767/2008;

(c) verify pursuant to Article 21 of this Regulation and Article 18(2) of Regulation (EC) No 767/2008 the authenticity and validity of the visa or whether the conditions for entry to the territory of the Member States in accordance with Article 6 of Regulation (EU) 2016/399 are fulfilled;

(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 21 of this Regulation and Article 19a of Regulation (EC) No 767/2008;

(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 with fingerprints against the VIS in accordance with Article 21 of this Regulation and Article 18(6) of Regulation (EC) No 767/2008.

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

(a) to examine visa applications and adopt decisions relating to those applications in accordance with Article 22 of this Regulation and Article 15(4) of Regulation (EC) No 767/2008;

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

(b) to 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 17 of this Regulation and Articles 13 and 14 of Regulation (EC) No 767/2008.

4 For the operation of the EES webservice referred to in Article 12, the separate read-only database referred to in Article 12(4) of [Regulation establishing an Entry/Exit System (EES)] shall be on a daily basis updated by the VIS via a one-way extraction of the minimum necessary subset of VIS data.

Article 8
Access to the EES for entering, amending, deleting and consulting data

1. Access to the EES for entering, amending, deleting and consulting the data referred to in Articles 13, 14, 15, 16, 17 and 18 shall be reserved exclusively to duly authorised staff of the authorities of each Member State which are competent for the purposes laid down in Articles 21 to 32. That access shall be limited to the extent needed for the performance of the tasks in accordance with this purpose, and proportionate to the objectives pursued.

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

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

Article 9
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, shall be in accordance with the safeguards laid down in the Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms, in the Charter of Fundamental Rights of the European Union and in the United Nations Convention on the Rights of the Child. In particular, when capturing a child's data, the best interest of the child shall be a primary consideration.

Article 10
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 calculator shall not apply to third country nationals:

i) who are family members 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) who do not hold a residence card referred to under 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 short stay visa issued for single or double entry have been previously used

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

(c) upon 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.

3. The border authorities shall inform the third country national of the maximum number of days of authorised stay which shall take into account the number of entries and the length of stay authorised by the visa, in accordance with Article 8(9) of Regulation (EU) 2016/399. The information may be provided either by the border guard at the moment of the border check or by means of an equipment installed at the border crossing point enabling the third countriy nationals to consult the webservice as referred to in Article 12 (1).

4. With regard to third country nationals subject to 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 visa.

In this case, the calculator shall only verify:

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

b) and for the short stay visas, the compliance with the period of validity of the visa.

4a. For the purpose of verifying whether or not third country nationals holding a single or double entry short stay visa have already used the number of entries authorised by their short stay visa, the calculator shall only take into account the entries performed in the Member States which apply the Schengen acquis in full. This verification shall not be carried out at the entry into the territories of the Member States which do not yet apply the Schengen acquis in full but operate the EES.

5. The automated calculator shall apply also for short stays based on a short stay visa with limited territorial validity issued on the basis of Article 25(1)(b) of Regulation (EC) No 810/2009. In this case, the calculator shall take into account the authorised stay as defined by such visa, irrespective of whether his/her cumulative stay exceeds 90 days within any 180-days.

Article 11
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 the authorised stay and identify records for which the maximum authorised stay was exceeded.

1a. For the third country nationals who perform their border crossing on the basis of valid Facilitated Transit Document (FTD) issued in accordance with Regulation (EC) 693/2003, the EES shall include a mechanism that shall automatically identify which entry/exit records do not have exit data immediately following the time of expiry of the duration of authorised stay and identify records for which the maximum period of authorised stay allowance has been exceeded.

A list generated by the system containing the data referred to in Article 14 and 15 of all identified overstayers shall be available to the designated competent national authorities according to Article 8(2) in order for them to adopt appropriate measures.

Article 12
Web service

1. In order to enable third country nationals to verify at any moment the remaining days of authorised stay, a secure internet access to a web service hosted by eu-LISA in its technical sites shall allow those third country nationals to provide the data required pursuant to Article 14(1)(b) together with the anticipated entry and exit date. On that basis, the web service shall provide them with an OK/NOT OK answer, and the information on the remaining number of days of authorised stay.

1a. By way of derogation to 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 those situations, 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 days under that limit. This information shall be provided for the stays performed in the 180-day period preceding the consultation of the web service or an anticipated date of entry /exit.

2. In view of fulfilling their obligations under Article 26(1)(b) of the Convention implementing the Schengen Agreement, carriers shall use the web service referred to in paragraph 2aa to verify whether or not third country nationals holding a single or double entry short stay visa have already used the number of entries authorised by their visa. The carrier shall provide the data listed under Article 14(1)(a), (b) and (c).The web service shall on that basis provide the carriers with an OK/NOT OK answer. Carriers may store the information sent and the answer received in accordance to the applicable law. Carriers shall establish an authentication scheme to ensure that only authorised staff may access the web service. The OK/NOT OK answer cannot be regarded as a decision to authorise or refuse entry in accordance with Regulation (EU) 2016/399.

2a. For the purpose of implementing Article 26(2) of the Convention implementing the Schengen Agreement and/ 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 website by the carriers. Those logs shall show the date and time of each operation, the data used for interrogation, the data transmitted by the webservice and the name of the carrier.

Each log shall be stored for two years. The log shall be protected by appropriate measures against unauthorised access.

2aa. The web service shall use 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 ~~the controller~~ responsible for the security of the web service, for the security of the personal data it contains and the process to extract the personal data into the separate read-only database.

2aaa. In accordance to Article 12(4), the web service shall not enable carriers to verify whether or not third country nationals holding a single or double entry national short stay visa have already used the number of entries authorised by their national short stay visa.

3. Detailed rules on the conditions for operation of the web service and the data protection and security rules applicable to the web service shall be adopted in accordance with the examination procedure referred to in Article 61(2).

CHAPTER II
Entry and use of data by competent authorities

Article 13
Procedures for entering data in the EES

1. Border authorities shall verify, in accordance with Article 21, whether a previous individual file has been created in the EES for the third country national as well as his/her identity. Where a third country national uses a self-service system for pre-enrolment of data or for the performance of border checks, a verification may be carried out through the self service system.

2. Where a previous individual file has been created, the border authority shall, if necessary, update the individual file data, referred to in Articles 14, 15 and 16 as applicable, enter an entry or exit record for each entry and exit in accordance with Articles 14 and 15 or, where applicable, a refusal of entry record in accordance with Article 16. That record shall be linked to the individual file of the third country national concerned. Where applicable, the data referred to in Article 17(1), (1a), (3) and (4) shall be added to the entry/exit record of the third country national concerned. The different 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 file has been registered and the third country national presents a *valid* travel document which differs from the one which was previously registered, the data *referred to in* Article 14(1)(f) shall and Article 15(1) (b) also be updated in accordance with Article 13a.

3. Where it is necessary to enter or update the entry/exit record data of a visa holder, the border authorities may retrieve and import the data provided for in Article 14([…]2) (c), (d), (e) and (f) directly from the VIS in accordance with Article 7 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 the individual file of the person by entering the data referred to in Articles 14(1), (6), 15(1) and 16(1) as applicable.

5. Where a third country national uses a self-service system for pre-enrolment of data, Article 8c 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 needs 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 verification referred to in paragraph 1 of this Article shall be carried out through the self service system. The data listed in Article 14(2) (c), (d), (e) and (f) may be retrieved and imported from the VIS.

6. Where a third country national uses a self-service system for the performance of the border checks, Article 8d 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 border, Article 8d 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 concerned individual file shall be carried out through the e-gate.

8. (…)

9. Without prejudice to Article 18 of this Regulation and Article 12(3) of Regulation (EU) 2016/399, if the authorised stay of a third country national who is present on the territory of a Member State starts directly after the stay based on residence permit or long-stay visa and no individual file has been created, the third country national may request the competent authorities according to Article 8(2) to create the individual file and the entry/exit record by entering the data referred to in Articles 14(1), (2) and (6) and 15(1). Instead of the data referred to in Article 14(2)(a), they shall insert the date of start of the authorised stay and, instead of the data in Article 14(2)(b), they shall insert the authority that authorised the authorised stay.

Article 13a
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 Article 14(1)(f) and Article 15(1)(b), the facial image shall be taken live.

2. By way of derogation to 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 Documents (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 concerned third country national.

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

4. Within a period of two years after the start of the operation of the EES, the Commission shall produce a report on the quality standards of the facial image stored in the VIS and on whether they are such that they enable biometric matching with a view to using the facial image stored in the VIS at borders and within the territory for the verification of the identity of third country nationals subject to a visa requirement, without storing such facial image into the EES. The Commission shall transmit the report to the European Parliament and the Council. On the basis of that report, the Commission may, using its right of initiative in accordance with the Treaty, make the necessary proposals, including proposals to amend this Regulation and/or Regulation (EC) No 767/2008, as regards the use of the facial image of third country nationals stored in the VIS for the purposes mentioned above.

Article 14
Personal data for third country national subject to a visa requirement

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

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

(b) type and number of the travel document or documents and 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(s);

(d) (…)

(e) (…)

(f) the facial image which shall have sufficient image resolution and quality to be used in automated biometric matching, in accordance with Article 13a;

(g) (…)

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. That record 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 file:

a) date and time of the entry;

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

(c) if applicable, the status of the person indicating that it is a third country national who:

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

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

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

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

(f) if applicable, the information indicating that the short stay visa has been issued with limited territorial validity, on the basis of Article 25(1)(b) of the Regulation (EC) 810/2009;

(g) (...)

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

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

(a) date and time of the exit;

(b) the border crossing point of the exit.

(c) Where a third country national subject to a visa requirement uses a different visa than the visa recorded in the last entry record, the data of the entry/exit record listed in paragraph 2(d), (e), (f) and (h) shall be updated accordingly.

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 mark or flag by the system and the data of the third country national subject to a visa requirement is identified as an overstayer shall be entered into the list referred to in Article 11.

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 paragraph 2 (c), (d), (e) and (f) and may be retrieved and imported from the VIS by the border authority in accordance with Article 18a of Regulation (EC) No 767/2008.

6. Member States shall insert a notification in the individual file if the third country national benefits from their national facilitation programme in accordance with Article 8e of Regulation (EU) 2016/399 specifying the Member State's national facilitation programme concerned.

7. The specific provisions set out in Annex II shall apply for third country nationals who perform their border crossing on the basis of a valid Facilitated Transit Document (FTD) issued in accordance with Regulation (EC) 693/2003.

Article 15

Personal data for third country nationals exempt from the visa obligation

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

(a) provided for in Article 14(1) (a), (b) and (c);

(b) the facial image which shall have sufficient image resolution and quality to be used in automated biometric matching, in accordance with Article 13a;

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

(d) where relevant data provided for in Article 14(6).

1a. For third country nationals exempt from the visa obligation, Articles 14(2)(a), (b) and (c), 14(3) (a) and (b) and 14(4) shall apply *mutatis mutandis.*

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

3. 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, this fact shall be recorded in the system and the person shall be required to give the fingerprints at the exit or the subsequent entry. The border authorities shall be entitled to request further clarification on the grounds for the temporary impossibility to provide fingerprints. This information shall be deleted from the system once the fingerprints have been given.

Member States shall ensure that appropriate procedures guaranteeing the dignity of the person are in place in the event of difficulties encountered in capturing fingerprints.

4. Where the person concerned is exempt from the requirement to give fingerprints pursuant to paragraphs 2 or 3, the specific data field shall be marked as 'not applicable'.

Article 16
Personal data for 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 Regulation (EU) 2016/399 and Annex V thereto, to refuse the entry of a third country national referred to in Article 2(2) of this Regulation to the territories of the Member States, and where no previous file has been registered in the EES for that third country national, the border authority shall create an individual file in which it shall enter:

a) in the case of third country nationals subject to a visa requirement: the alphanumeric data required pursuant to Article 14(1) and, where relevant, the data referred to under Article 14(6)

b) in the case of visa exempt third country nationals: the alphanumeric data required pursuant to Article 15(1)

1a. In the specific case where the third country national is refused entry on the basis of a reason corresponding to letter(s) B, D and/or H of Annex V, Part B of Regulation (EU) 2016/399 and where no previous file has been registered in the EES for that third country national, the border authority shall create an individual file in which it shall enter the alphanumeric data referred to in paragraph 1 as well as the following data:

a) in the case of third country nationals subject to a visa requirement: the facial image referred to in Article 14(1) (f)

b) in the case of a visa exempt third country nationals the biometric data required pursuant to Article 15(1) (b) and (c)

c) in the case of third country nationals subject to a visa requirement who are not registered in the VIS: the facial image referred to in Article 14(1) (f) and the fingerprint data as referred to Article 15(1) (c)

1aa. By way of derogation to paragraph 1a, where the reason corresponding to letter H applies, and the biometric data of the third country national are recorded in the SIS alert resulting in the refusal of entry, the biometric data of the third country national shall not be entered in the EES.

1aaa. In the specific case where the third country national is refused entry on the basis of a reason corresponding to letter I of Annex V, Part B of Regulation (EU) 2016/399 and where no previous file has been registered in the EES for that third country national, the biometric data shall only be entered in the EES when 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.

1ab. If a third country national is refused entry on the basis of a reason corresponding to letter J of Annex V, Part B of Regulation (EU) 2016/399, the border check authority shall create the individual file without biometric data. If the third country national possesses an eMRTD the facial image shall be extracted from this eMRTD.

2. For both third country nationals subject to a visa requirement and visa exempt third country nationals 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 letter(s) corresponding to the reason(s) for refusing entry, in accordance with Annex V, Part B of Regulation (EU) 2016/399.

In addition, for third country nationals subject to a visa requirement the data provided for in Article 14(2)(d), (e), (f) and (h) 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 Article 14(2)(d), (e) and (f) may be retrieved and imported from the VIS into the EES by the competent border checks authority in accordance with Article 18a of Regulation (EC) No 767/2008.

3. The record provided for in paragraph 2 shall be linked to the individual file of the third country national.

Article 17

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 the authorised stay or visa, the competent authority that has taken the 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 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) the period of the extension of the duration of authorised stay;

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

1a. 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 shall add the data regarding the period of extension of the authorised stay to the latest relevant entry/exit record and the indication that the authorised stay was extended in accordance with Article 20(2)(b) of the Convention implementing the Schengen Agreement.

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

3. The entry/exit record shall indicate the ground(s) for revocation or annulment of the authorised stay, which shall be:

(a) a return decision adopted pursuant to Directive 2008/115/EC[28c];

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

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

5. When a person has departed or has been removed from the territories of the Member States pursuant to a decision as referred to in paragraph 3, the competent authority shall enter the data in accordance with Article 13(2) in the entry/exit record of that specific entry.

Article 18

Data to be added in case of rebuttal of the presumption that the third country national does not fulfil the conditions of duration of authorised stay in accordance with Article 12 of Regulation (EU) 2016/399

Without prejudice to Article 20, where a third country national present on the territory of a Member State has no individual file created in the EES or there is no last relevant entry/exit record, 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 that case Article 12 of Regulation (EU) 2016/399 shall apply and if that presumption is rebutted in accordance with Article 12(3) of that Regulation, the competent authorities shall create an individual file for that third country national in the EES if necessary, or update the latest entry/exit record by entering the missing data in accordance with Articles 14 and 15 or delete an existing file where Article 32 applies.

Article 19

Fall-back procedures in case of technical impossibility to enter data or failure of the EES

1. Where it is technically impossible to enter data in the Central System or in the event of a failure of the Central System, the data referred to in Articles 14, 15, 16, 17 and 18 shall be temporarily stored in the National Uniform Interface as provided for in Article 6. Where this is not possible, the data shall be temporarily stored locally in an electronic format. In both cases, the data shall be entered into the Central System of the EES 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 the Central System and in the National Uniform Interface, and it is technically impossible to temporarily store the data locally in an electronic format, shall manually store entry/exit data in accordance with Articles 14, 15, 16, 17 and 18 , 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 inserted into the Central System as soon as technically possible. Member States shall inform the Commission of the stamping of travel documents in the event of exceptional situations mentioned in first subparagraph. Detailed rules on the information to the Commission shall be adopted in accordance with the examination procedure referred to in Article 61(2).

3. The EES shall indicate that data referred to in Articles 14, 15, 16, 17 and 18 were entered during fall-back procedure and that the individual file created according to paragraph 2 is missing biometric data. The biometric data shall be enrolled at the next border crossing.

Article 20
Transitional period and transitional measures

1. For a period of *180 days* after the EES has started operations, in order to verify at entry and at exit that third country nationals admitted for a short stay have not exceeded the duration of the maximum authorised stay and, where relevant, to verify at entry that the third country national has not exceeded the number of entries authorised by the short stay visa issued for single or double entry, the competent border authorities shall take into account the stays in the territories 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 14(2). This rule shall not be limited to the six months after the EES has started operations as referred to in paragraph 1. In case of discrepancy between the entry stamp and the data recorded in the EES, the stamp shall prevail.

Article 21
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 data registered into the EES where necessary and for consulting the data to the extent required for the performance of border *checks.*

2. Pursuant to paragraph 1, the border authorities shall have access to search with the data referred to in Article 14(1)(a), (b) and (c) and Article 15(1)(a).

In addition, for the purposes of carrying out the consultation of 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, consult the VIS in accordance with Article 18(2a) of Regulation (EC) No 767/2008 .

If the search in the EES with those data 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 Article 14(1)(f) and Article 15(1)(b) 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 (EU) 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 Regulation (EC) No 767/2008.

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

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(s) or refusal of entry record(s) linked to it.

4. Where the search with the alphanumeric data set out in paragraph 2 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 to the identity of the third country national, the border authorities shall have access to data for identification in accordance with Article 25.

In addition, 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 that third country national is 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. In circumstances where a verification of the person 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 who are not found in the EES further to the identification run in accordance with Article 25, 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 who had their individual file 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 reccorded on the system on the basis of a national short stay visa, the border authorities shall consult the VIS in accordance with point(a) of paragraph 4 of this Article when, for the first time after the creation of the individual file, the third country national intends to cross the border of a Member which applies the Schengen acquis in full at which the EES is operated.

CHAPTER III
Use of the EES by other authorities

Article 22
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 the relevant provisions of Regulation (EU) No 810/2009 of the European Parliament and of the Council[31].

In addition, visa authorities of a Member State which does not yet apply Schengen acquis in full, but operate the EES, shall consult 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.

2. The visa authority 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 Article 14(1)(a), (b) and (c);

(b) the short stay visa sticker number, including the three letter code of the issuing Member State referred to in Article 14(2)(d);

(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 and also refusals of entry record linked to it. Visa authorities shall be given access to consult the automated calculator in order to check the maximum remaining duration of an authorised stay. They shall also be able to consult the EES and its calculator when examining and taking decision on a new visa application, so as to automatically establish the maximum duration of authorised stay.

4. Visa authorities of a Member State which does not yet apply Schengen acquis in full but operates the EES shall be given access to search the EES with one or several of the data provided under paragraph 2 of this Article. 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 and also refusals of entry record linked to it. Visa authorities of a Member State which does not yet apply 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. They shall also be able to consult the EES and its automated calculator when examining and taking decision on a new visa application, so as to establish the maximum duration of authorised stay.

Article 23

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

1. The competent authorities referred to in Article 8e 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 as regards the use of the Entry/Exit System 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 authority shall be given access to search with one or several of the following data:
(a) the data referred to in Article 14(1)(a), (b) and (c) or the data referred to in Article 15(1)(a);
(b) 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, the competent authority shall be given access to consult the data

[31] 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)

of the individual file of that third country national and the entry/exit records and also refusals of entry records linked to it.

Article 24
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 and/or checking or verifying if the conditions for entry to or authorised stay on the territory of the Member States are fulfilled, the immigration authorities of the Member States shall have access to search with the data referred to in Article 14(1)(a), (b), (c) and 15(1)(a).
If the search indicates that data on the third country national are recorded in the EES, the immigration authorities may compare the live facial image of the third country national with the facial image referred to in Article 14(1)(f) and 15(1) (b) or the immigration authorities may 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 is recorded in the EES, the immigration authority shall be given access to consult the data of the individual file of that person, the entry/exit record(s), the automated calculator and refusals of entry record(s) linked to it.

3. Where the search with the data set out in paragraph 1 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 25.

Article 25
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 or no longer fulfils the conditions for entry or, for authorised stay on the territory of the Member States.

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 fingerprints has failed, the search shall be carried out with all or some of the data referred to in Articles 14(1)(a), (b), (c), and 15(1)(a).

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, the linked entry/exit records and refusal of entry records.

Article 25c
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 26
Member States' designated authorities

1. Member States shall designate the authorities which are entitled to consult the data stored in the EES 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 29 are fulfilled.

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 perform independently.

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

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

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

6. Only duly empowered staff of the central access point(s) shall be authorised to access the EES in accordance with Articles 28 and 29.

Article 27
Europol

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

2. Europol shall designate a specialised unit with duly empowered Europol officials as the

central access point. The central access point shall verify that the conditions to request access to the EES laid down in Article 30 are fulfilled.

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

Article 28
Procedure for access to the EES for law enforcement purposes

1. The operating units referred to in Article 26(5) shall submit a reasoned electronic or written request to the central access points referred to in Article 26(3) for access to data stored in the EES. Upon receipt of a request for access, the central access point(s) shall verify whether the conditions for access referred to in Article 29 are fulfilled. If the conditions for access are fulfilled, the central access point(s) shall process the requests. The EES data accessed shall be transmitted to the operating units referred to in Article 26(5) in such a way as to not compromise the security of the data.

2. In a case of urgency, where there is a need to prevent an imminent danger associated with a terrorist offence or another serious criminal offence, the central access point(s) shall process the request immediately and shall only verify ex post whether all the conditions of Article 29 are fulfilled, including whether a case of urgency actually existed. The ex post verification shall take place without undue delay and in any event no later than 7 working days after the processing of the request

3. Where an ex post verification determines that the access to EES data was not justified, all the authorities that accessed such data shall erase the information accessed from the EES and shall inform the central access points of the erasure.

Article 29
Conditions for access to EES data by designated authorities of Member States

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

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

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

(c) 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;

2. The 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 when the conditions listed in paragraph 1 are met and the following additional conditions are met:

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

(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 conducted, or the search has not been fully conducted within 2 days of being launched.

However, the additional conditions in sub-paragraphs (a) and (b) of this paragraph 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 case of urgency where there is a need to prevent an imminent danger associated with a terrorist offence or another serious criminal offence. Those reasonable grounds shall be included in the electronic or written request for comparison with EES data sent by the operating unit of the designated authority to the central access point(s).

Since fingerprint data of third country nationals subject to a visa requirement are only stored in the VIS, 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 access to the EES as a tool to consult the travel history or the periods of authorised stay on the territory of the Member States of a known suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence shall be allowed when the conditions listed in paragraph 1 are met.

4. Consultation of the EES for 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 a Facilitated Transit Document (FTD) issued in accordance with Regulation (EC) 693/2003. 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 image.

Consultation of the EES, in case of a hit, shall give access to any other data taken from the individual file as listed in Article 14(1), 14(6), Article 15(1) and Article 16(1).

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

(a) Surname(s) (family name)~~;~~, first name(s) (given names), date of birth, nationality or nationalities and/or sex;

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

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

(d) Fingerprints, including latent fingerprints;

(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 this paragraph as well as to any other data taken from the individual file, the entry/exit records and refusal of entry records including data entered in respect of revocation or extension of authorised stay in accordance with Article 17.

Article 30
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;

1a. 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 concerned.
Since fingerprint data of visa-holding third-country nationals are only stored in the VIS, 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.

2. The conditions laid down in Article 29 (3) to (5) shall apply accordingly.

3. Europol's designated authority may submit a reasoned electronic request for the consultation of all data or a specific set of data stored in the EES to the Europol central access point referred to in Article 27. Upon receipt of a request for access the Europol central access point shall verify whether the conditions for access referred to in paragraphs 1 and 1a are fulfilled. If all conditions for access are fulfilled, the duly authorised staff of the central access point(s) shall process the requests. The EES data accessed shall be transmitted to the operating units referred to in Article 27 (1) in such a way as not to compromise the security of the data.

4. The processing of information obtained by Europol from consultation with EES data shall be subject to the authorisation of the Member State of origin. That authorisation shall be obtained via the Europol national unit of that Member State.

CHAPTER V
Retention and amendment of the data

Article 31
Retention period for data storage

1. Each entry/exit record or refusal of entry record linked to an individual file shall be stored 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(s) or refusal of entry records shall be stored in the EES Central System for three years and one day following the date of the last exit record if there is no entry record within three years from that 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 last day of the authorised stay. The EES shall automatically inform the Member States three months in advance of the scheduled deletion of data on overstayers in order for them to adopt the appropriate measures.

4. By way of derogation from paragraph (1) each entry/exit record(s) generated by third country nationals who are family members 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 who do not hold a residence card referred to under Directive 2004/38/EC or a residence permit pursuant to Regulation (EC) No 1030/2002 shall be stored in the EES for a maximum of one year after the exit. If there is no exit record the data shall be stored for a period of five years from the last entry record.

5. Upon expiry of the retention period referred to in paragraphs 1 to 4 such data shall automatically be erased from the Central System.

Article 32
Amendment of data and advance data deletion

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

2 If the Member State responsible has evidence to suggest that data recorded in the EES are factually inaccurate, incomplete or that data were processed in the EES in contravention of this Regulation, it shall check the data concerned and, if necessary, shall rectify, complete or erase them without delay from the EES and, where applicable, from the list of identified persons referred to in Article 11. This may also be done at the request of the person concerned in accordance with Article 46.

3. By way of derogation from paragraphs 1 and 2, if a Member State other than the Member State responsible has evidence to suggest that data recorded in the EES are factually inaccurate, *incomplete* or that data were processed in the EES in contravention of this Regulation, it shall check the data concerned if it is possible to do this without consulting the Member State responsible and, if necessary, rectify, complete or erase them without delay from the EES and, where applicable, from the list of identified persons referred to in Article 11. Otherwise the Member State shall contact the authorities of the Member State responsible within a time limit of 7 days and the Member State responsible shall check the accuracy of the data and the lawfulness of its processing within a time limit of one month. This may also be done at the request of the person concerned in accordance with Article 46.

4. In the event that a Member State has evidence to suggest that visa-related data recorded in the EES are factually inaccurate, incomplete or that such data were processed in the EES in contravention of this Regulation they shall first check the accuracy of these data against the VIS and if necessary shall rectify, complete or erase them in the EES. Should the data recorded in the VIS be the same as in the EES, they 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 the data concerned and if necessary rectify, complete or erase them immediately from the VIS and inform the Member State concerned which shall, if necessary, rectify, complete or erase them from the EES without delay and, where applicable, from the list of identified persons referred to in Article 11.

5 The data of identified persons referred to in Article 11 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 provides evidence, in accordance with the national law of the Member State responsible or of the Member State to which the request has been made, that he or she was forced to exceed the duration of authorised stay due to unforeseeable and serious events, that he or she has acquired a legal right to short stay or in case of errors. Without prejudice to any available administrative or non-judicial remedy, the third country national shall have access to an effective judicial-remedy to ensure the data is 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 period referred to in Article 31, the individual file and the entry/exit records linked to it in accordance with Articles 14 and 15 and refusal of entry records in accordance with Article 16 shall be deleted from the EES as well as, where applicable, from the list of identified persons referred to in Article 11 without delay, and in any case not later than 5 working days from when the 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 31:

(a) by 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, San Marino or where the third country national is in a possession of a passport issued by the Vatican City State he or she shall inform the competent authorities of the Member State he or she next enters of this change. That Member State shall delete their data without delay from the EES. The individual shall have access to an effective judicial remedy to ensure the data is deleted.

7. The Central System shall immediately inform all Member States of the erasure of data from the EES and where applicable from the list of identified persons referred to in Article 11.

8. In case another Member State than the Member State responsible has amended or erased data in accordance with this Regulation, this Member State shall be responsible for the amendments or erasure. The system will record all amendments and erasures applied.

CHAPTER VI
Development, Operation and Responsibilities

Article 33
Adoption of implementing measures by the Commission prior to development

The Commission shall adopt the following measures necessary for the development and technical implementation of the Central System, the National Uniform Interfaces, the Communication Infrastructure, the web service referred to in Article 12 and the data repository referred to Article 57(2), in particular measures for:

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

(a1) 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;

(b) entering the data in accordance with Article 14, 15, 16, 17 and 18;

(c) accessing the data in accordance with Articles 21 to 30;

(d) amending, deleting and advance deleting of data in accordance with Article 32;

(e) keeping and accessing the records in accordance with Article 41;

(f) performance requirements, including minimal specifications for technical equipment and requirements on 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;

(g) the specifications and conditions for the web-service referred to in Article 12, including specific provisions for the protection of the data where provided by or to carriers;

(h) (…)

(i) (…)

(j) the establishment and the high level design of the interoperability referred to in Article 7;

(k) for the specifications and conditions for the central repository referred in Article 57 (2);

(l) (…)

(m) the establishment of the list referred to in Article 11(2) and procedure to make the list available to Member States;

(n) the specification for technical solutions to connect central access points in accordance with Articles 28 and 29 and for a technical solution to collect the statistical data required in accordance with Article 64(8).

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 61(2).

For the adoption of the measures set down for the establishment and the high level design of the interoperability specified in point (j), the Committee set up by Article 61 of this Regulation shall consult the VIS Committee set up by Article 49 of Regulation (EC) 767/2008.

Article 34
Development and operational management

1. eu-LISA shall be responsible for the development of the Central System, the National Uniform Interfaces, the Communication Infrastructure and the Secure Communication Channel between the EES Central System and the VIS Central System. It shall also be responsible for the development of the web service referred to in Article 12 *and the data repository to in Article 57(2)*in accordance with the specifications and conditions adopted in accordance with the examination procedure referred to in Article 61(2).

eu-LISA shall define the design of the physical architecture of the system including its Communication Infrastructure as well as the technical specifications and their evolution as regards the Central System, the Uniform Interfaces, the Secure Communication Channel between the EES Central System and the VIS Central System and the Communication Infrastructure, the web service referred to in Article 12 and the data repository referred to Article 57(2), which shall be adopted by the 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 referred to in Article 55.

eu-LISA shall develop and implement the Central System, the National Uniform Interfaces, the Secure Communication Channel between the EES Central System and the VIS Central System, and the Communication Infrastructure, the web service referred to in Article 12 and the data repository referred to Article 57(2) as soon as possible after the entry into force of this Regulation and the adoption by the Commission of the measures provided for in Article 33.

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

By developing and implementing the Central System, the National Uniform Interfaces, the Secure Communication Channel between the EES Central System and the VIS Central System, and the Communication Infrastructure, eu –LISA shall:

(a) perform a security risk assessment as part of the development of the EES;

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

(c) conduct a security risk assessment regarding the interoperability with the VIS referred to in Article 7 and assess the required security measures needed for its implementation.

2. During the designing and development phase, a Programme Management Board composed of a maximum of 10 members shall be established. It shall be composed of seven members appointed by eu-LISA's Management Board from among its members or their alternates, the Chair of the EES Advisory Group referred to in Article 62, 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 will participate in the EES.

The Programme Management Board will 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 the Management Board on progress of the project. It shall have no decision-making power nor any mandate to represent the members of the Management Board.

The Management Board shall establish the rules of procedure of the Programme Management Board which shall include in particular rules on:

(a) chairmanship;

(b) meeting venues;

(c) preparation of meetings;

(d) admission of experts to the meetings;

(e) communication plans ensuring full information to non-participating Members of the Management Board.

The chairmanship 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 the Agency and Article 10 of the eu-LISA Rules of Procedure shall apply mutatis mutandis. The Programme Management Board's secretariat shall be ensured by eu-LISA.

During the designing and development phase, the EES Advisory Group referred to in Article 62 shall be composed of the 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.

3. eu-LISA shall be responsible for the operational management of the Central System, the Secure Communication Channel between the EES Central System and the VIS Central System and the National Uniform Interfaces. 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 Central System, the Secure Communication Channel between the EES Central System and the VIS Central System the National Uniform Interfaces, the Communication Infrastructure between the Central system and the National Uniform Interfaces, the web service referred to in Article 12 and the data repository referred to Article 57(2). eu-LISA shall also be responsible for the operational management of the Communication Infrastructure between the Central system and the National Uniform Interfaces, for the web-service referred to in Article 12 and the data repository referred to Article 57(2).

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 system functions at a satisfactory level of operational quality, in particular as regards the response time for interrogation of the central database by border crossing points, in accordance with the technical specifications.

4. Without prejudice to Article 17 of the Staff Regulations of Officials of the European Union, eu-LISA shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality to its entire staff required to work with EES data. This obligation shall also apply after such staff leave office or employment or after the termination of their activities.

Article 35
Responsibilities of Member States and Europol

1. Each Member State shall be responsible for:

(a) the integration of the existing national infrastructure necessary for border check and the connection to the National Uniform Interface;

(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 5 with the exception of Article 5(1a);

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

(d) the management and arrangements for access of duly authorised staff of the competent national authorities to the EES in accordance with this Regulation and to establish and regularly update a list of such staff and their profiles.

2. Each Member State shall designate a national authority, which shall provide the competent authorities referred to in Article 8 with access to the EES. Each Member State shall connect that national authority to the National Uniform Interface. Each Member State shall connect their respective central access points referred to in Article 26 to the National Uniform Interface.

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

3a. Member States shall ensure that the technical performance of the border control infrastructure, availability, duration of the border checks and the data quality is closely monitored to ensure that they meet the overall requirements for the proper functioning of the EES and an efficient border check process.

4. 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 about data security and data protection rules in particular and on relevant fundamental rights.

4a. Member States shall not process the data in/from the EES for purposes other than those laid down in this Regulation.

5. Europol shall assume the responsibilities foreseen under paragraphs 3, 4 and 4a. It shall connect its central access point referred to in Article 27 to the EES and shall be responsible for that connection.

Article 36
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 Article 4(7) of Regulation (EU) 2016/679 and which shall have central responsibility for the processing of data by this Member State. Each Member State shall communicate the details of this 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:

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

(b) the data are registered lawfully into the EES;

(c) the data are 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 33. In particular, eu-LISA shall:

(a) take the necessary measures to ensure the security of the Central System and the Communication Infrastructure between the Central System and the National Uniform Interface, without prejudice to the responsibilities of each Member State;

(b) ensure that only duly authorised staff has 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 for the start of operations of the EES.

Article 37
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 into 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 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, risk and with their own technical means.

Article 38
Communication of data to third countries, international organisations and private parties

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

2. By way of derogation from paragraph 1, the data referred to in Article 14(1)(a), (b), (c) and (f) and Article 15(1)(a), (b), and (c) may be transferred by border authorities or immigration authorities to a third country or to an international organisation listed in the Annex I in individual cases, if necessary in order to prove the identity of third country nationals for the sole purpose of return, only where the following conditions are satisfied:

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

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

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

In all cases,

- the data shall be transferred in accordance with the relevant provisions of Union law, in particular data protection, including Chapter V of Regulation 2016/679 on transfers of personal data to third countries or international organisations, and readmission agreements, and the national law of the Member State which transferred the data;

- the third country or international organisation agrees to process the data only for purposes for which they were provided,

- a return decision adopted pursuant to Directive 2008/115(EC) has been issued in relation to the individual concerned provided its enforcement is not suspended and provided no appeal has been lodged which may lead to the suspension of the enforcement of the return decision.

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

4. Personal data obtained from the 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 if those data are further processed at national level or between Member States pursuant to Directive (EU) 2016/680.

4a. By way of derogation from paragraph 4, the data referred to in Article 14(1)(a), (b) and (c) 14 (2) (a) and (b), 14 (3) (a) and (b) and 15(1) (a) may be transferred by the designated authority to a third country in individual cases, only if the following cumulative conditions are met:

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

(i) an imminent danger associated with a terrorist offence as defined under Article 3(1)(26) of this Regulation, or

(ii) an imminent danger for the life of a person and this danger is associated with a serious criminal offence as defined under Article 3(1) (27) of this Regulation,

(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 offence or offences;

(c) the designated authority has access to such data in accordance with the procedure and the conditions set out in Articles 28 and 29;

(d) the transfer is carried out in accordance with the applicable conditions set out in Directive (EU) 2016/680, in particular Chapter V thereof on transfers of personal data to third countries or international organisations;

(e) a duly motivated written or electronic request from the third country is submitted;

(f) and 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 based on this paragraph, such a transfer shall be documented and the documentation shall be made available to the supervisory authority established in accordance with Article 41(1) of Directive (EU) 2016/680 on request, 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 38a

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

1. By way of derogation from paragraph 4, the data referred to in Article 14(1)(a), (b) and (c) 14 (2) (a) and (b), 14 (3) (a) and (b) and 15(1) (a) may be transferred by the designated 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 if the following cumulative conditions are met:

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

(i) an imminent danger associated with a terrorist offence as defined under Article 3(1)(26) of this Regulation

(ii) or a serious criminal offence as defined under Article 3(1) (27) of this Regulation,

(b) the transfer of data is necessary for the prevention, detection or investigation of such offence or offences;

(c) the designated authority has access to such data in accordance with the procedure and the conditions set out in Articles 28 and 29;

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

(e) a duly motivated written or electronic request is submitted

(f) and 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 based on this paragraph, such a transfer shall be documented and the documentation shall be made available to the supervisory authority established in accordance with Article 41(1) of Directive (EU) 2016/680 on request, 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. In cases where information is provided pursuant to this Article, the same conditions as referred to in Article 39(1), Article 40(1) and (3), Article 43 and 52(4) shall apply *mutatis mutandis.*

Article 39
Data security

1. The Member State responsible shall ensure the security of the data before and during the transmission to the National Uniform Interface. 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 infrastructure necessary for border check, 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 input of data and the unauthorised inspection, modification or deletion of stored personal data;

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

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

(f) 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;

(g) 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,

delete, consult and search the data and make their profiles available to the supervisory authorities.

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

(i) ensure that it is possible to verify and establish what data has been processed in the EES, when, by whom and for what purpose;

(j) prevent the unauthorised reading, copying, modification or deletion 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;

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

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

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

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.

3a. 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.

Article 39a
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 EES data shall be considered to be a security incident, especially 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 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) No 2016/679 and/ or to Article 30 of Directive (EU) No 2016/680, Member States shall notify the Commission, eu-LISA and the European Data Protection Supervisor of security incidents. In the event of a security incident on 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 collaborate in the event of a security incident.

Article 40
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 incompatible with this Regulation shall be entitled to receive compensation from the Member State which is responsible for the damage suffered. That Member State shall be exempted from its liability, in whole or in part, if it proves that it is not *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 41
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 show the purpose of access referred to in Article 8, the date and time, the data transmitted as referred to in Article 14 to 17, the data used for interrogation as referred to in Articles 21 to 25 and the name of the authority entering or retrieving the data.

2. For the consultations listed in Article 7, 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) 767/2008. eu-LISA shall ensure in particular that the relevant log of the concerned data processing operations are kept when the competent authorities launch a data processing operation directly from one system to the other.

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

3. Such logs may be used only for the data protection monitoring of the admissibility of data processing as well as to ensure data security pursuant to Article 39. Those logs shall be protected by appropriate measures against unauthorised access and deleted one year after the retention period referred to in Article 31 has expired, unless they are required for monitoring procedures which have already begun.

Article 42
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 43
Penalties

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

Article 43a
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.

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).

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).

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 44
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) an explanation using clear and plain language, of 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 a Facilitated Transit Document (FTD) issued in accordance with Regulation (EC) 693/2003 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;

(d1) an explanation that entry shall be refused if a third country national refuses to provide the requested biometric data for registration, verification and/or identification in the EES;

(d2) the right to receive information about the maximum remaining number of days of his/her authorised stay in accordance with Article 10(3);

(d3) an explanation of 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 according to the provisions of Article 38(4a) and to Member States according to the provisions of Article 38a**;

(e) 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 and that incomplete personal data relating to them be completed or that unlawfully processed personal data concerning them be erased or 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.

(ea) an explanation of the fact that EES data shall be accessed for border management and facilitation purposes, specifying that overstays will automatically lead to the addition of the third-country national's data to a list, as well as the possible consequences of overstaying;

(eb) the data retention period set for entry and exit records, refusal of entry records, and for individual files pursuant to Article 31;

(ec) the right for overstayers to have their personal data erased from the list referred to in Article 11(2) and rectified on the EES, where they provide evidence that they exceeded the authorised duration of stay due to unforeseeable and serious events;

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

The information provided in paragraph 1 of this Article shall be provided in a concise, transparent, intelligible and easily accessible form in writing, by any appropriate means, which ensures that the third-country national is informed of his or her rights, at the time when the individual file of the person concerned is being created in accordance with Articles 14,15 or 16.

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

The information referred to in paragraph 1 of this Article shall be drawn up and set up by the Commission in accordance with the examination procedure referred to in Article 61(2) and the content shall be clear and plain language and available in a linguistic version the person concerned understands or is reasonably supposed to understand.

The Commission shall provide the common information in a template. The template shall be established in such a manner as to enable Member States to complete them 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 specifications and conditions for the website referred to in paragraph 2 should also be adopted by the Commission according to the examination procedure referred to in Article 61(2) prior to the start of the operation of the EES.

Article 45
Information campaign

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

Article 46
Right of access to, rectification, completion, erasure and of restriction of the processing of personal data

1. The requests of third country nationals related to the rights set out in Articles 15, 16, 17 and 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 whom 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 of personal data 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 a time limit of 1 month if that check can be done without consulting the Member State responsible. Otherwise the Member State other than the Member State responsible shall contact the authorities of the Member State responsible within a time limit of seven days and the Member State responsible shall check the accuracy of the data and the lawfulness of the data processing within a time limit of 1 month.

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 32. 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 concerning him or her 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 if necessary will 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 responsible for entering these data in the VIS within a time limit of seven days. The Member State responsible for entering the data in the VIS shall check the accuracy of the visa related data and the lawfulness of its processing in the EES within a time limit of one month and inform the Member State responsible or the Member State to which the request has been made (concerned) which shall, if necessary, rectify, complete or erase the personal data concerning him or her or restrict the processing of such data without delay from the EES and, where applicable, from the list of persons referred to in Article 11(2).

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 decision explaining in writing to the person 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 shall also provide the person concerned with information explaining the steps which he can take if he 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 person concerned. Fingerprints may be requested for this purpose only in duly justified cases where there are substantive doubts as to the identity of the applicant. That information shall be used exclusively to enable the exercise of the rights referred to in paragraphs 1 and 2 and shall be erased immediately afterwards.

7. Whenever a person made a request in accordance with paragraph 1, the competent authority of the Member State reponsible 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 and how it was addressed and by which authority and 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 47
Cooperation to ensure the rights on data protection

1. The competent authorities of the Member States shall cooperate actively to enforce the rights laid down in Article 46.

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 such data in accordance with Regulation (EU) 2016/679.

In order to achieve those aims, 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.

Article 48
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, provided for in Article 46 and 47(2). The right to bring such an action or complaint shall also apply in cases where requests for access, correction or deletion were not answered within the deadlines provided for in Article 46 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 49
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 shall independently monitor 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 referred to in paragraph 1 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. The supervisory authority referred to in paragraph 1 shall publish annually the number of requests for corrections of data, the action subsequently taken and the number of corrections made in response to requests by the persons concerned

3. Member States shall ensure that their supervisory authority referred to in paragraph 1 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. (…)

5. Each Member State shall supply any information requested by the supervisory authority referred to in paragraph 1 and shall, in particular, provide it with information on the activities carried out in accordance with Articles 35, 36(1) and 39. Each Member State shall grant the

supervisory authority access to their logs pursuant to Article 41 and allow it access at all times to all their EES related premises.

Article 50
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, the Council, the Commission, eu-LISA and 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 access to all documents and to its logs referred to in Article 41 and allow him access to all its premises at any time.

Article 51
Cooperation between supervisory authorities and the European Data Protection Supervisor

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

2. They shall exchange relevant information, assist each other in carrying out audits and inspections, examine difficulties over 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. The supervisory authorities and the European Data Protection Supervisor shall meet for that purpose at least twice a year within the framework of the European Data Protection Board established by Regulation (EU) 2016/679. The costs and servicing of these meetings shall be borne by the Board established by Regulation (EU) 2016/679. 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 established by Regulation (EU) 2016/679 to the European Parliament, the Council, the Commission and eu-LISA every two years. That report shall include a chapter of each Member State prepared by the supervisory authorities of that Member State.

Article 52
Protection of personal data accessed in accordance with Chapter IV

1. Each Member State shall ensure that the provisions adopted under national law implementing Directive (EU) 2016/680 are also applicable to the access to EES by its national authorities in line with Article 1(2), including in relation to the rights of the persons whose data is so accessed.

2. The monitoring of the lawfulness of the access to personal data by the Member States in accordance with Chapter IV of this Regulation, including their transission to and from the EES,

shall be carried out by the supervisory authority established in accordance with Article 41(1) of Directive (EU) 2016/680. Article 49(3) and (5) applies 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 Central System, the designated authorities, the central access points and Europol shall keep records of the searches for the purposes of enabling the supervisory authorities referred to in paragraph 2 and the European Data Protection Supervisor to monitor the compliance of data processing with Union and national data protection rules. Other than for such purpose, personal data, as well as the records of the searches, shall be erased in all national and Europol files after a period of one month, 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 53
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.

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 Article 29(2)(b) 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 Central System;

(da) the name of the authority having requested access for comparison

(e) where applicable, the use of the urgent procedure referred to in Article 28(2) and the decision taken with regard to the ex-post verification;

(f) the data used for comparison;

(g) in accordance with national rules or with Regulation (EU) 2016/794, the identifying mark of the official who carried out the search and of the official who ordered the search or supply.

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 64. 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 their request for the purpose of fulfilling their duties.

CHAPTER VIII
Amendments to other Union instruments

Article 54
Amendment to the Convention implementing the Schengen Agreement

In Article 20, of the Convention implementing the Schengen Agreement, 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 in its territory

a) in exceptional circumstances or

b) in accordance with a bilateral agreement concluded before the entry into force of this Convention and notified to the Commission in accordance with the last subparagraph of this paragraph.

2a. The stay of an alien in the territory of a Contracting Party may be extended in accordance with a bilateral agreement pursuant to paragraph 2(b), upon request of the alien and lodged with the competent authorities of that Contracting Party upon entry or during the stay of the alien at the latest on the last working day of his/her 90-day stay in any 180-day period.
In case the alien has not lodged a request during the 90-day stay in any 180-day period, his/her stay may be extended based on a bilateral agreement concluded by a Contracting Party and his/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/she has stayed only at the territory of that Contracting party.

2b. In case where the stay is extended pursuant to paragraph 2, the competent authorities of that Contracting Party shall enter the data related to the extension in the latest relevant entry/exit record in accordance with Article 17 of the Regulation establishing the Entry/Exit system.

2c. The alien shall be authorised to stay only in the territory of that Contracting Party and exit at the external borders of that Contracting party.
The competent authority that has extended the stay shall inform the alien concerned that the extension of stay is authorised only in the territory of that Contracting party and he/she shall exit at the external border of that Contracting party.

2d. The Contracting Parties shall notify to the Commission within three months after entry into force of the Regulation establishing the Entry/Exit System the text of their relevant applicable bilateral agreements pursuant to paragraph 2(b). If the Contracting party ceases to apply any of those bilateral agreements it shall notify the Commission thereof. The Commission shall publish information about the bilateral agreements, including at least the Member States and third countries concerned, the rights derived for third country nationals from those agreements as well as any changes thereto in the Official Journal of the European Union."

Article 55
Amendments to Regulation (EC) 767/2008 concerning the Visa Information System

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

(0) In Article 10(1) the following indents are added:

(dd) if applicable, the information indicating that the visa has been issued with limited territorial validity, on the basis of Article 25(1)(b) of the Regulation (EC) 810/2009.

(l) if applicable, the status of the person indicating that the third country national is member of the family of a Union citizen to whom the Directive 2004/38/EC applies or of a third country national enjoying the right of free movement under Union law.

(1) In Article 13 the following paragraph is added:

"3. Where a decision has been taken to annul or to revoke an issued visa, the visa authority which has taken the decision shall immediately retrieve and export from the VIS into the Entry/Exit System (EES) the data listed under paragraph 1 of Article 17 of [Regulation N° XXX of the European Parliament and the Council 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 of the European Union and determining the conditions for access to the EES for law enforcement purposes][32]."

(2) In Article 14 the following paragraph is added:

"3. The visa authority which has taken a decision to extend the period of validity and/or the duration of stay of an issued visa shall immediately retrieve and export from the VIS into the EES the data listed under paragraph 1 of Article 17 of [Regulation establishing an Entry/Exit System (EES)]."

(3) Article 15 is amended as follows:

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

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

(c) 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 carrying out the consultation of the EES for examining and deciding on visa applications in accordance with Article 22 of [Regulation establishing an Entry/Exit System (EES)], 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. In circumstances where the search with the data referred to in paragraph 2 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."

(4) In Chapter III a new Article 17a is added:

"*Article 17a*
Interoperability with the EES

1. From the start of operations of the EES referred to in Article 60(1) of [Regulation establishing an Entry/Exit System (EES)], interoperability between the EES and the VIS is established to ensure

[32] Regulation No XXX of the European Parliament and the Council 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 of the European Union and determining the conditions for access to the EES for law enforcement purposes (OJ …) [full title + OJ reference]

more efficiency and rapidity of border checks. To this effect 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 systems shall only be possible if both this Regulation and [Regulation establishing an Entry/Exit System (EES) […] provide for it. Retrieval, exportation and importation of visa related data directly from the VIS into the EES shall be an automated process once the operation in question is launched by the authority concerned.

2. The interoperability shall enable the visa authorities using the VIS to consult the EES from the VIS in order to:

(a) consult the EES when examining and deciding on visa applications as referred to in Article 22 of [Regulation establishing an Entry/Exit System (EES)] and Article 15(4) of this Regulation;

(b) to retrieve and export the visa related data directly from the VIS into the EES in case a visa is annulled, revoked or extended in accordance with Article 17 of [Regulation establishing an Entry/Exit System (EES)] and Articles 13 and 14 of this Regulation;

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

(a) retrieve and import the visa related data directly from the VIS to the EES in order to create or update the entry/exit record or refusal of entry record of a visa holder in the EES in accordance with Articles 13, 14 and 16 [Regulation establishing an Entry/Exit System (EES)] and Article 18a of this Regulation;

(b) retrieve and import the visa related data directly from the VIS in case a visa is annulled, revoked or extended in accordance with Article 17 of [Regulation establishing an Entry/Exit System (EES)] and Articles 13 and 14 of this Regulation;

(c) verify the authenticity and validity of the visa and/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 as referred to in Article 18(2) of this Regulation;

(d) check whether third country nationals exempt from the visa obligation who do not have an individual file recorded in the EES were previously registered in the VIS in accordance with Article 21 of [Regulation establishing an Entry/Exit System (EES)] and Article 19a of this Regulation;

e) where the identity of a visa holder is verified using fingerprints, verify the identity of a visa holder with fingerprints against the VIS in accordance with Articles 21(2) and 21(4) of [Regulation establishing an Entry/Exit System (EES)] and 18(6) of this Regulation.

3a For the operation of the EES webservice referred to in Article 12 of [Regulation establishing an Entry/Exit System (EES)], the VIS shall on a daily basis update the separate read-only database referred to in Article 12(4) of [Regulation establishing an Entry/Exit System (EES)] via a one-way extraction of the minimum necessary subset of VIS data.

4. In accordance with Article 33 of the [Regulation establishing an Entry/Exit System (EES)], the Commission shall adopt the measures necessary for the establishment and the high level design of the interoperability in accordance with Article 34 of the [Regulation establishing an Entry/Exit System (EES)]. In order to establish the interoperability with the EES, the Management Authority shall develop the required evolutions and/or adaptations of the Central Visa Information System, the National Interface in each Member State, and the communication infrastructure between the Central Visa Information System and the National Interfaces. The national infrastructures shall be adapted and/or developed by the Member States.

(5) 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 and/or whether the conditions for entry to the territory of the Member States in accordance with Article 6 of Regulation (EU) 2016/399 are fulfilled, the competent authorities for carrying out checks at borders at which the EES is operated shall have access to search using the following data:

(a) surname (family name), first name(s) (given names); date of birth, nationality; 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) or the number of the visa sticker.

2. Solely for the purposes referred to in paragraph 1, where a search is launched in the EES pursuant to Article 21(2) of [Regulation establishing an Entry/Exit System (EES)], 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.

2a. By way of derogation to paragraph 2, where a search is launched in the EES pursuant to Article 21(2) or Article 21(4) of [Regulation establishing an Entry/Exit System (EES)], the competent border authority may search the VIS without making use of the interoperability with the EES if specific circumstances so require, in particular, where the specific situation of a third country national makes more appropiate a search using the data referred to in point (b) of paragraph 1, or in case of a temporary technical impossibility to consult the EES data or of a failure of the EES.

3. If the search with the data listed in paragraph 1 indicates that the VIS stores data on one or more issued or extended visa(s)), which are under 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 of the concerned application file as well as of linked application file(s) pursuant to Article 8(4), solely for the purposes referred to in paragraph 1:

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

(b) photographs;

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

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

4. If the search with the data listed in paragraph 1 indicates that data on the person are recorded in the VIS but that the visa(s) recorded are not valid, the competent authority for carrying out checks at borders at which the EES is operated shall be given access to consult the following data of the application file(s) as well as of the linked application file(s) pursuant to Article 8(4), solely for the purposes referred to in paragraph 1:

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

(b) photographs;

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

5. In addition to the consultation carried out under paragraph 1, 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 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 21(2) of [Regulation establishing an Entry/Exit System (EES)], when:

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

(ii)in the concerned border crossing point, the identity is verified using fingerprints in accordance with Article 21(2) of [Regulation establishing an Entry/Exit System (EES)],

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

(iv) for any other reason, the identity of the visa holder cannot be verified against the EES;

(b) the identity of the person can be verified against the EES but Article 21(5) of the [Regulation establishing an Entry/Exit System (EES)] applies.

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

6. For the purpose of a verifying the fingerprints against the VIS as laid down under paragraph 5, the competent authority may launch a search from the EES to the VIS.

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

(6) The following Article 18a is inserted:

"*Article 18a*
Retrieval of VIS data for creating or updating entry/exit record or the refusal of entry record of a visa holder into the EES

1. Solely for the purpose of creating or updating the entry/exit record or refusal of entry record of a visa holder in the EES in accordance with Article 13(2) and Article 14 and 16 of [Regulation establishing an Entry/Exit System (EES)], the competent authority for carrying out checks at borders at which the EES is operated shall be given access to retrieve in the VIS and import to the EES, the data stored in the VIS and listed in Article 14(2) (c), (d), (e) and (f) of [Regulation establishing an Entry/Exit System (EES)].

(7) The following Article 19a is inserted:

"Article 19a
Use of the VIS before creating in the EES the individual files of third country nationals exempt from the visa obligation as laid down in Article 21 of [Regulation establishing an Entry/Exit System (EES)]

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 third country nationals exempt from the visa obligation as laid down in Article 15 of [Regulation establishing an Entry/Exit System (EES)];

2. For the purpose of paragraph 1, where Article 21(4) of [Regulation establishing an Entry/Exit System (EES)] applies and the search referred to in Article 25 of that Regulation indicates that data on a person are not recorded in the EES or where Article 21(5) of [Regulation establishing an Entry/Exit System (EES)] applies, the competent authority for carrying out checks at borders at which the EES is operated shall have access to search using the following data: surname (family name), first name(s) (given names); date of birth, nationality; sex; type and number of the travel document; three letter code of the issuing country of the travel document, and the date of expiry of the validity of the travel document.

3. Solely for the purposes referred to in paragraph 1, further to a search launched in the EES pursuant to Article 21(4) of [Regulation establishing an Entry/Exit System (EES)] or where Article 21(5) of [Regulation establishing an Entry/Exit System (EES)] applies, 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 foreseen under paragraph 2.

4. In addition, if the search with the data listed in paragraph 2 indicates that data on the person are recorded on the VIS, the competent authority for carrying out checks at borders at which the EES is operated shall verify the fingerprints of the person against the fingerprints recorded in the VIS. That authority may launch such verification from the EES. For persons whose fingerprints cannot be used, the search shall be carried out only with the alphanumeric data foreseen under paragraph 2 of this Article.

5. If the search with the data listed in paragraph 2 and the verification of paragraph 4 indicates that data on the person are recorded on 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 of the concerned application file(s) as well as of linked application file(s) pursuant to Article 8(4), solely for the purposes referred to in paragraph 1:

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

(b) photographs;

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

6. In circumstances where the verification provided under paragraphs 2 and/or 5 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 those competent authorities 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 of this Regulation."

(8) In Article 20, the first subparagraph of paragraph 1 is replaced by the following:

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

the conditions for entry to, stay or residence on the territory of the Member States are fulfilled, shall have access to search with the fingerprints of that person.

(9) In Article 26 the following paragraph is inserted:

"3a. [*Six months after the entry into force of Regulation establishing an Entry/Exit System (EES)*], the Management Authority shall be responsible for the tasks referred to in paragraph 3 of this Article."

(10) In Article 34, 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. These records shall show the purpose of access referred to in Article 6(1) and in Articles 15 to 22, the date and time, the type of data transmitted as referred to in Articles 9 to 14, the type of data used for interrogation as referred to in Articles 15(2), 17, 18(1), 18 (5), 19(1), 19a(2), 19a(5), 20(1), 21(1) and 22(1) and the name of the authority entering or retrieving the data. In addition, each Member State shall keep records of the staff duly authorised to enter or retrieve the data.

1a. For the operations listed in Article 17a a record of each data processing operation carried out within the VIS and the EES shall be kept in accordance with this Article and Article 41 of the [Regulation establishing an Entry/Exit System (EES)]."

Article 56
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:

“2. The Agency shall be responsible for the operational management of the second generation Schengen Information System (SIS II), the Visa Information System, Eurodac and the Entry/Exit System (EES).

(2) A new Article 5a is added after Article 5:

"*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) No XXX/20XX of the European Parliament and of the Council of X.X.X establishing an Entry/Exit System to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes;

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

(3) Article 7 is amended as follows:

(a) 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 (EC, Euratom)1605/2002. In such a case, the network provider shall be bound by the security measures referred to in paragraph 4 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.″

(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 information systems”.

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

(a) a new point (sa) is added after point (s):

“(sa) adopt the reports on the development of the EES pursuant to Article 64(2) of Regulation (EU) XX/XX of XXX”.

(a) 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 respectively, 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 64(4) of Regulation (EU) XX/XX of XXX."

(b) 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 50(2) of Regulation (EU) XX/XX of XXX and ensure appropriate follow-up of those audits”.

(b) a new point (xa) is inserted after point x:

“(xa) publish statistics related to EES pursuant to Article 57 of Regulation (EU) No XXXX/XX.

(c) a new point (za) is added to point z:

“(za) ensure annual publication of the list of competent authorities pursuant to Article 8(2) of Regulation (EU) No XXXX/XX.

(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 observer when a question concerning VIS, in relation to the application of Decision 2008/633/JHA, or a question concerning Eurodac, in relation to the application of Regulation (EU) No 603/2013, or a question concerning EES in relation to the application of Regulation (EU) XX/XX of XXX is on the agenda”.

(7) In Article 17 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 34(4) of [Regulation (EU) XX/XX of XXX.]”

(8) Article 19 is amended as follows:

(a) paragraph 1 is replaced by the following:

“1. The following Advisory Groups shall provide the Management Board with expertise relating to large-scale IT systems and, in particular, in the context of the preparation of the annual work programme and the annual activity report:

(a) SIS II Advisory Group;

(b) VIS Advisory Group;

(c) Eurodac Advisory Group;

(d) 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 57
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 while ensuring non-discrimination as referred to in Article 9(2 and the duly authorised staff of the European Border and Coast Guard Agency shall have access to consult the following data for the purpose of carrying out risk analyses and vulnerability assessments as referred to in Articles 11 and 13 of Regulation (EU) 2016/1624:

(a) status information;

(b) nationality, gender 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 three letter code of the issuing country;

(e) number of overstayers referred to in Article 11, nationalities and border crossing point of entry;

(f) the data entered in respect of any stay revoked or 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 15(2) and (3);

(i) the number of third country nationals refused entry, the nationalities of third country nationals refused entry and the type of border (land, air or sea), […] the border crossing point at which entry was refused and the grounds on which entry has been refused as referred to in Article 16(2)(d).

2. For the purpose of paragraph 1, eu-LISA shall establish, implement and host a repository at a central level in its technical sites containing the data referred to in paragraph 1 which would not allow for the identification of individuals and would allow the authorities listed in paragraph 1 to obtain customisable reports and statistics on the entries and exits, refusals of entry and overstay of third country nationals to enhance the efficiency of border checks, to help consulates processing the visa applications and to support evidence-based Union migration policymaking. The repository shall also contain daily statistics on the data referred to in paragraph 4. Access to the central repository shall be granted by means of secured access through S-TESTA with control of access and specific user profiles solely for the purpose of reporting and statistics. Detailed rules on the operation of the central repository and the data protection and security rules applicable to the repository shall be adopted in accordance with the examination procedure referred to in Article 61(2).

3. The procedures put in place by eu-LISA to monitor the development and the functioning of the EES referred to in Article 64(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, gender, 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 stays were revoked or extended as well as the number of third country nationals exempt from the requirement to give fingerprints.

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.

Article 58
Costs

1. The costs incurred in connection with the establishment and operation of the Central System, the Communication Infrastructure the National Uniform Interface, *the webservice and the repository* at central level shall be borne by the general budget of the Union.

2. Costs incurred by the integration of the existing national border infrastructure and the connection to the National Uniform Interface as well as by hosting the National Uniform Interface 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 check 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) Automatic Border Control systems, self-service systems and e-gates.

3. The costs incurred by the central access points as referred to in article 26 and 27 shall be borne by each Member State and Europol, respectively. The costs for the connection of these central access points to the National Uniform Interface 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.

Article 59
Notifications

1. Member States shall notify the Commission of the authority which is to be considered as controller referred to in Article 49.

2. Member States shall notify the Commission and eu-LISA of the competent authorities referred to in Article 8(2) which have access to enter, amend, delete, consult or search data. Within three months after the EES has started operations in accordance with Article 60, 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 amendments thereto. Where there are amendments thereto, eu-LISA shall publish once a year an updated consolidated version of this 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 26 and shall notify without delay any amendments thereto.

4. Europol shall notify the Commission and eu-LISA of its designated authority and its central access point referred to in Article 27 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 Article 60(1)(b).

6. The Commission shall publish the information referred to in paragraphs 1, 3 and ~~to~~ 4 in the Official Journal of the European Union. Where there are amendments thereto, the Commission shall publish once a year an updated consolidated version of this information. The Commission shall maintain a constantly updated public website containing this information.

Article 60
Start of operations

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

(a) the measures referred to in Article 33 have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the EES, which shall 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 14 to 18 to the EES and have notified them to the Commission;

(d) the Member States have completed the notifications to the Commission referred to in Article 59 (1) and (3).

1a. The EES shall be operated by:

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

(b) the Member States which do not yet apply 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 Schengen Information System have been put into effect in accordance with the relevant Accession Treaty, and

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

1b. A Member State which is not covered by paragraph 1a, shall be connected to the EES as soon as the conditions referred to in paragraph 1(b), (c), (d) and paragraph 1a(b) are met. The Commission shall determine the date from which the EES is to start the operations in that Member State.

2. 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.

3. The Commission decision referred to in paragraph 1 and 1b shall be published in the *Official Journal*.

4. 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 1b.

Article 60a
Ceuta and Melilla

The provisions of 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 61
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 62
Advisory group

An Advisory Group shall be established by eu-LISA and 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, Article 34(2) applies.

Article 63
Training

eu-LISA shall perform tasks related to providing training on the technical use of the EES in accordance with the relevant provisions in Regulation 1077/2011.

Article 63a
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 Handbook shall provide technical and operational guidelines, recommendations and best practices. The Commission shall adopt the Handbook in the form of a recommendation.

Article 64
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 [Six months after the entry into force of this Regulation – OPOCE, please replace with the actual date] and every six months thereafter during the development phase of the EES, eu-LISA shall submit a report to the European Parliament and the Council on the state of play of the development of the Central System, the Uniform Interfaces and the Communication Infrastructure between the Central System and the Uniform Interfaces. This report shall contain detailed information about the costs incurred and information as to any risks which may impact on the overall costs of the system to be borne by the general budget of the Union in accordance with Article 58(1) and (2) first subparagraph. Once the development is finalised, a report shall be submitted to the European Parliament and 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, the Council and 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 the Regulation;

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

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

(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 under Article 19(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 evaluation shall include any necessary recommendations. The Commission shall transmit the evaluation report to the European Parliament, the Council, the European Data Protection Supervisor and the European Agency for Fundamental Rights.

Those evaluations shall also include an assessment of the use made of the provisions referred to in Article 54 both in terms of frequency (number of third country nationals making use of these provisions per Member State, their nationality, average duration of their stay) and practical implications as well as taking 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 54 and replacing them with a European instrument. It shall be accompanied, if appropriate, by a legislative proposal amending Article 54 of this Regulation.

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 and/or eu-LISA. 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 made for the purpose of identification or for entry/exit records, and the type of terrorist or serious criminal offence;

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

(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 Article 29(2)(b);

(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 procedure was 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 this data pursuant to Chapter IV for the purpose of generating statistics referred to in this paragraph.

The specifications shall be adopted by the Commission by means of implementing acts in accordance with the examination procedure referred to in Article 61(2).

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

Article 65
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 determined by the Commission in accordance with Article 60(1), with the exception of Articles 4, 33, 34, 35,39, 55(4)(4), 55(9) 56, 58, 59, 60, and 61, 62, 63 and 64(2) which shall apply from the date of entry into force of this Regulation.

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

Done at Brussels,

For the EP	*For the Council*
The President	*The President*

ANNEX I

List of international organisations referred to in Article 38(2)

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

ANNEX II

The specific provisions for third country nationals who perform their border crossing on the basis of a valid Facilitated Transit Document

(1) By way of derogation from Article 14(1) to (3) of this Regulation, for third country nationals who perform their border crossing on the basis of a valid Facilitated Transit Document (FTD) issued in accordance with Regulation (EC) 693/2003, the border check authorities shall:

a) create/update their individual file which shall contain the data foreseen under Article 15(1) (a), (b) and (c) of this Regulation. In addition, their individual file shall indicate that the person holds a Facilitated Transit Document (FTD). That indication shall automatically result in the multiple entry characteristic of the FTD to be added to the entry/exit record,

b) enter in an entry/exit record for each of their entries performed on the basis of a valid Facilitated Transit Document (FTD), the data listed under Articles 14(2)(a) to (c) 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 system in accordance with Article 3(2) of Regulation (EC) 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 14(3) and (4) of this Regulation shall be applicable *mutatis mutandis* to third country nationals holding a Facilitated Transit Document (FTD) issued in accordance with Regulation (EC) 693/2003.

(4) For verification at a border at which the EES is operated and within the territories of the Member States, third country nationals who perform their border crossing on the basis of a valid Facilitated Transit Document (FTD) shall be subject mutatis mutandis to the verifications and identifications provided under Articles 21 and 24 of this Regulation and Articles 18 and 19a of Regulation (EC) No 767/2008 that are applicable to third country nationals who are not subject to a visa requirement.

(5) The provisions of paragraph 1 to 4 shall not apply to third country nationals who perform their border crossing on the basis of a valid Facilitated Transit Document (FTD) issued in accordance with Regulation (EC) 693/2003 provided that the following cumulative conditions are met:

(a) they perform their transit by train;

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