



EUROPEAN
COMMISSION

Brussels, 6.4.2016
COM(2016) 194 final

2016/0106 (COD)

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

{SWD(2016) 114 final}
{SWD(2016) 115 final}
{SWD(2016) 116 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Background

In February 2013, the Commission tabled a package of legislative proposals on Smart Borders to modernise the Schengen area's external border management. The package consisted of three proposals: (1) a Regulation for an Entry/Exit System (EES) for the recording of information on the time and place of entry and exit of third country nationals entering the Schengen area, (2) a Regulation for a Registered Traveller Programme (RTP) to allow third country nationals who have been pre-vetted to benefit from facilitation of border checks at the Union external border, (3) a Regulation amending the Schengen Borders Code¹ in order to take into account the existence of the EES and RTP.²

During the first examination of the package which was completed in February 2014, the co-legislators voiced technical, financial and operational concerns on certain aspects of the design of the systems. However the preferred policy options proposed in 2013 (i.e. centralised systems based on biometrics) were not questioned. The European Parliament (EP) referred the proposal to its Committee on Civil Liberties, Justice and Home Affairs (LIBE). It did not issue a legislative resolution on the proposals.

In order to further assess the technical, organisational and financial impacts of the proposed policy options, the Commission initiated, with the support of both co-legislators, a so-called 'proof of concept' exercise consisting of two stages:

- A Commission-led Technical Study on Smart Borders (hereinafter 'The Technical Study') published in October 2014³, and
- A testing phase led by eu-LISA on the impact of the use of various biometric identifiers on the border control processes (hereinafter 'The Pilot') for which a report was published in November 2015⁴.

Based on the findings of the Technical Study, the results of The Pilot, the technical discussions with co-legislators and stakeholders as well as a public consultation⁵, the Commission prepared a detailed Impact Assessment which is accompanying this proposal. This Impact Assessment builds on the Impact Assessments⁶ accompanying the 2013 proposals, and focuses on elements of the 2013 proposals where modifications are proposed, notably (a) the architecture of the system, (b) biometrics to be used, (c) the use of process facilitators, (d) the retention of data and (e) access by law enforcement authorities.

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

² COM(2013) 95 FINAL, COM(2013) 97 FINAL and COM(2013) 96 FINAL.

³ Technical Study on Smart Borders, European Commission, DG HOME, 2014. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/index_en.htm

⁴ Final Report of the Smart Borders Pilot Project, eu-LISA, December 2015. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/index_en.htm

⁵ http://ec.europa.eu/dgs/home-affairs/what-is-new/public-consultation/2015/consulting_0030_en.htm

⁶ SWD(2013)47 final and SWD(2013)50 final

On the basis of these extensive preparations, the Commission has considered necessary improvements and simplifications to the 2013 proposals. The Commission has decided to:

- revise its 2013 proposal for a Regulation for the establishment of an Entry/Exit System (EES);
- revise its 2013 proposal for Regulation amending the Schengen Borders Code to integrate the technical changes that result from the new proposal for a Regulation establishing an Entry/Exit System (EES).
- withdraw its 2013 proposal for a Regulation for a Registered Traveller Programme (RTP).

• **Rationale for the establishment of an EU Entry/Exit System**

As explained in the Impact Assessment, the establishment of an EU Entry/Exit System is considered necessary to address the following challenges:

1. Addressing Border check delays and improving quality of border checks for third country nationals

Passenger flows at the external borders of the European Union have been growing and will continue to increase in the future. The total number of regular border crossings in 2025 is forecast to rise to 887 million, of which around one-third are expected to be by third country nationals traveling to Schengen countries for a short term visit. While 'minimum checks' are performed on EU citizens and persons enjoying the right of free movement, third country nationals crossing the Schengen area external borders are subject to 'thorough checks' made today manually at borders (both at entry and exit).

The Schengen Borders Code has no provisions on the recording of travellers' cross border movements into and out of the Schengen area. As a general rule, third country nationals have the right to enter for a short stay of up to 90 days within any 180 day period. Currently the stamping of the travel document indicating the dates of entry and exit is the sole method available to border guards and immigration authorities to calculate the duration of stay of third country nationals and to verify if someone is overstaying. These stamps can be difficult to interpret: they may be unreadable or the result of counterfeiting. Similarly, it is difficult for consulates having to process visa applications to establish the lawfulness of previous visas on the basis of stamps present in the travel document. As a result, the whole procedure is considered error prone and not always systematically implemented.

The introduction of the EES will ensure:

- precise information, rapidly delivered on demand to border guards during border checks, by replacing the current slow and unreliable system of manual stamping of passports; this will allow for both a better monitoring of the authorised stay as well as more efficient border checks;
- information to border guards on refusals of entry of third country nationals and will allow for refusals of entry to be checked electronically in the EES;
- precise information to travellers on the maximum length of their authorised stay;
- possibility for automated border controls for third country nationals under the supervision of the border guards in accordance with the conditions foreseen in Article 8d of the revised proposal to amend the Schengen Borders Code.

2. Ensuring systematic and reliable identification of ‘overstayers’

Irregular immigrants include both persons who crossed the borders irregularly – usually not at an official border crossing point - and the so-called “overstayers”: persons having legally entered the EU at an official border crossing point but who stayed after their entitlement to do so expired. The EES addresses this category of irregular migration. As border crossings by third country nationals are currently not registered, it is not possible to establish lists of overstayers.

The introduction of EES will:

- provide precise information on who is overstaying their authorised stay, which will support controls within the territory and allow to apprehend irregular migrants more efficiently;
- support the identification of irregular migrants; by storing biometrics in the EES on all persons not subject to the visa requirement, and taking into account that the biometrics of visa holders are stored in the VIS, Member States' authorities will be able to identify any undocumented irregular migrant found within the territory that crossed the external border legally; this will in turn facilitate the return process;
- allow for an evidence-based approach through the analysis generated by the system. In the case of visa policy for instance, the EES will provide precise data on whether there is problem with overstayers of a given nationality or not, which would be an important element when deciding whether to impose or lift visa obligations on a third country in question;

3. Reinforcing internal security and the fight against terrorism and serious crime.

Criminal activities such as trafficking in human beings, people smuggling or the smuggling of illicit goods involve numerous border crossings, which are facilitated by the absence of registration of the border crossings of the third country nationals concerned. Likewise, terrorist organisations and radicalised individuals can benefit from the absence of registration of border crossings. Controls of third country nationals at external borders involve identity checks and searches against various databases of known persons or groups posing a threat to public security that should be either apprehended or denied entry to the territory. However, if a third country national destroys his/her official documentation once inside the Schengen area, it can be very difficult for law enforcement authorities to identify that person in case he/she is suspected of a crime or is a victim of crime.

The introduction of EES will:

- support the reliable identification of terrorists, criminals as well as of suspects and victims;
- provide a record of travel histories of third country nationals including crime suspects. It would thus complement the information available in the Schengen Information System.

• Relevant developments since 2013

In preparing this revised proposal, the Commission also took account of relevant developments since 2013, which changed the political, legal and institutional environment compared to 2013, when the original Smart Borders proposals were submitted:

- The Visa Information System became fully operational. Its 'roll-out' to Member States consulates in all relevant third countries was concluded in November 2015. The biometric

verification of visa-holders against VIS at Schengen external borders is now compulsory. Law enforcement authorities increasingly use VIS for identification and investigation purposes.

- Visa liberalisation dialogues with countries in the Western Balkans and at the Eastern and South-Eastern borders of the EU were concluded or have been accelerated, which will lead to an increasing proportion of visa-exempt travellers to the EU. It is expected that this trend will continue in the coming years.
- The Internal Security Fund (ISF-B) was adopted, which earmarked € 791 million for the development of Smart Borders, to be used after the adoption of the relevant legal basis.
- The European Agenda on Migration⁷ identified "*border management*" as one of the "*four pillars to manage migration better*". Securing external borders and managing them more efficiently implies making better use of the opportunities offered by IT systems and technologies. Furthermore, at the Justice and Home Affairs and European Councils in December 2015, Member States emphasised the need to improve the controls at external borders through the use of new technologies.
- Rapid developments in the area of biometric technology opened up new possibilities for 'lighter' and 'faster' enrolment and verification of travellers, not only for fingerprints, but also for facial images.
- The Court judgment on the Data Retention Directive provided legal clarity on the conditions and safeguards that need to be respected for the storage and use of EES data.
- The December 2015 political agreement of the co-legislators on the reform of EU data protection rules will put in place a modern data protection framework across the EU. The General Data Protection Regulation and the Data Protection Directive will be formally adopted by the European Parliament and Council in the course of 2016.

- **Main elements of the revised smart borders package**

The scope of the new Entry Exit System includes border crossings by all third country nationals visiting the Schengen area for a short stay (maximum 90 days period in any period of 180 days), both visa-required and visa-exempt travellers, or eventually, on the basis of a touring visa⁸ (up to one year).

Family members of EU citizens enjoying the right of free movement or of third country nationals who enjoy the same rights of free movement equivalent to those of Union citizens and who do not yet have a residence card should be registered in the EES but are not subject to the short stay rule, and checks on this category shall be carried out in accordance with Directive 2004/38/EC⁹. Such

⁷ COM(2015) 240 final.

⁸ Should a touring visa be established in accordance with the Proposal submitted by the Commission for a Regulation of the European parliament and of the Council establishing a touring visa and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 562/2006 and (EC) No 767/2008 [COM(2014) 163 final]

⁹ Directive 2004/38/EC of the European Parliament and of the Council 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.

family members in possession of a residence card referred to in Directive 2004/38/EC are excluded from the EES.

The system will collect data and register entry and exit records with the view to both facilitating the border crossing of bona fide travellers, and better identifying overstayers. The EES will also record refusals of entry of third country nationals falling within its scope.

The main differences between this modified proposal and the 2013 proposals are:

- The architecture of the system: only one system is proposed, the Entry Exit System. The connection of the national border infrastructures to the EES central system will be done through a National Uniform Interface which will be identical for all Member States, and will allow the use of the existing national Entry Exit Systems. However, data from the central system cannot be copied into these existing national EES.

- Interoperability is ensured between the EES and VIS in order to achieve more efficiency and rapidity at border checks. To this effect, a connection will be established between the central systems of the EES and the VIS and direct access between them will be regulated for specific purposes. This will reduce the duplication of personal data processing in accordance with the 'privacy by design' principle.

- Biometric identifiers: while the 2013 EES proposals were relying on ten fingerprints, the revised EES proposals suggests a combination of four fingerprints and the facial image as biometric identifiers introduced from the start of operations of the EES. This choice will allow for sufficiently accurate verifications and identifications, considering the expected size of the EES, while keeping the amount of data to a reasonable level while at the same time speeding up border controls and enabling a wider use of self-service systems at border crossing points. The four fingerprints are used at enrolment to check if the third country national was already registered in the system while the facial image allows for a quick and reliable (automatic) verification at subsequent entry that the individual subject to the border control is the one already registered in the EES.

- Personal data protection: there is a significant reduction in the volume of personal data recorded in EES: 26 data items are to be recorded in EES instead of 36. The right of access, rectification and deletion of personal data are clearly defined and safeguarded. The European Data Protection Supervisor and the national data protection authorities will be in charge of supervision for data processing.

- Data retention period: The retention time for stored data is five years. The five year data retention period reduces the re-enrolment frequency and will be beneficial for all travellers, while allowing the border guard to perform the necessary risk analysis required by the Schengen Border Code before authorising a traveller to enter the Schengen area. For the border guard the systematic deletion of the EES record after 181 days as proposed in 2013 would have removed any trace of the third country national recent history of entries and exits from the Schengen area which is required for a risk analysis. It would be a regression of useful information compared to what the border guard currently uses: consulting stamps in a travel document gives in many cases information that stretches a period of several years. A longer data retention period is thus necessary to allow the border guard performing the necessary risk analysis requested by the Schengen Border Code before authorising a traveller entering the Schengen area. The processing of visa application in consular posts requires also analysing the travel history of the applicant to assess the use of previous visas and the respect of the conditions of stay. 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.

The longer data retention period will reduce the re-enrolment frequency and will be beneficial for all travellers as the average border crossing time will decrease as will do the waiting time at border crossing points. Even for a traveller entering only once in the Schengen area, the fact that other travellers being already registered in the EES will not have to re-enrol will reduce the waiting time at border.

A longer data retention period will also be necessary to allow for facilitation at border crossing by using process accelerators and self-service systems. Facilitation is dependent of the data registered in the system. A short data retention period would reduce the group of travellers that can benefit of such facilitation and thereby undermine the stated objective of EES to facilitate border crossing.

For non EU family members of EU citizens who fall within the scope of the present Regulation, each entry/exit record shall be kept for a maximum period of one year after the last exit. Their individual file should be kept for five years so as to enable the family member to benefit of the facilitation for border crossing.

For overstayers not yet found at the end of the data retention period, following a national decision, an alert based on the EES data can be created in the Schengen Information System, based upon a national decision, before deletion of the EES data.

- The facilitation of border crossings: the approach for facilitation is based on the implementation of self-service systems and e-gates, which will allow third country nationals to initiate the procedure for border clearance, to be completed by providing additional information to the border guard on request. The use of these accelerators (introduced in the proposal amending the Schengen Borders Code) is optional for Member States, open to most of the travellers and does not require the development of any new system.

- In addition there will be a harmonised legal basis (again introduced in the amendments to the Schengen Borders Code) for the establishment of national Registered Travellers Programmes by Member States, on a voluntary basis.

- Law enforcement access: from the start of operations, Member States' law enforcement authorities and Europol will have access to the EES, under strictly defined conditions. The EES will contain reliable data on entry and exit dates of third country nationals falling within the scope of the EES that can be of decisive importance in individual law enforcement files, to which access should be given in accordance with the purpose of the instrument and with respect for data protection rules.

The access to VIS data for law enforcement purpose has already proven its usefulness. Member States have reported cases of people who died violently and whose identification was only possible through accessing the VIS. Other cases reported are related to human being trafficking, terrorism or drug trafficking for which the access to VIS data allowed the investigators to make substantial progress.

- The costs: in the 2013 proposals, 1,1 billion EUR was set aside as an indicative amount for the development of an EES and an RTP. For the revised proposal, based on the preferred option of a single EES system including the law enforcement access, the amount needed has been estimated at EUR 480 million.

This revised proposal for a Regulation establishing an EES constitutes the core instrument for the legal framework of the EES. It also contains consequential amendments to existing EU legislation

(i.e. to Regulation (EU) No 1077/2011¹⁰, to Regulation (EC) No 767/2008¹¹ and to the Convention implementing the Schengen Agreement). This complementary proposal to amend the Schengen Borders Code as regards the use of the system as part of the border management process is presented in parallel with this proposal.

- **Existing provisions in the area of the proposal**

Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code).

Regulation of the European Parliament and of the Council (EC) No 1931/2006 laying down rules on local border traffic at the external land borders of the Member States and amending the provisions of the Schengen Convention.

Regulation of the European Parliament and of the Council (EC) No 767/2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation).

Regulation of the European Parliament and of the Council (EC) No 810/2009 establishing a Community Code on Visas.

Regulation of the European Parliament and of the Council (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

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.

2. CONSULTATION OF INTERESTED PARTIES AND IMPACT ASSESSMENT

- **Consultation of interested parties**

A detailed description of stakeholder consultation is included in the accompanying impact assessment in Annex 2. During 2015 the Commission carried out targeted consultations for the preparation of its revised Smart Borders proposals with the EDPS in a workshop on the preparation of the revised Smart Borders proposals of 20 March 2015, with civil society in a meeting of 5 May 2015, with carriers, transport, tourism and infrastructure operators in a meeting of 28 May 2015 and with the Fundamental Rights Agency in two meetings of 22 June and 23 July 2015. In addition, the Commission organised a meeting with law enforcement practitioners of the Member States on 9 July 2015 and two technical meetings with Member States' experts on 24 September 2015 and on 26 October 2015.

A public consultation, that took place from the 29 July to the 29 October 2015, collected the views of individuals, organisations, carriers and public authorities (the results of the public consultation are explained in detail in Annex 2 of the Impact Assessment).

¹⁰ Regulation of the European Parliament and of the Council (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

¹¹ Regulation of the European Parliament and of the Council (EC) No 767/2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation)

The LIBE Committee of the European Parliament organised an inter-parliamentary committee with national parliaments on Smart Borders on 23-24 February 2015.

- **Impact assessment**

A first impact assessment¹² was carried out in 2008 when preparing the Commission Communication on this subject and a second one was finalised in 2012¹³ in preparation of the 2013 proposals.

The third Impact Assessment was finalised in 2016. Taking into account the Technical Study, the report on the Pilot Project, the result of the consultation of interested parties and the discussions in the Council and the European Parliament, the impact assessment analysed key implementation options and suboptions for both the EES and the RTP. The preferred options resulting from the Impact Assessment are directly reflected in the main changes included in the current proposal as compared to the 2013 proposals (See point I "Main elements of the revised proposal")

The Regulatory Scrutiny Board (RSB) reviewed the draft impact assessment and delivered its positive opinion on 22 January 2016

3. LEGAL ELEMENTS OF THE PROPOSAL

- **Summary of the proposed actions**

The purposes, functionalities and responsibilities for the EES must be defined. Furthermore, a mandate needs to be given to the Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) to develop and operationally manage the system. A detailed explanation of the present revised proposal by article can be found in a separate Commission Staff Working Paper.

Consequential amendments to this proposal need to be adopted to Regulation (EU) No 1077/2011, Regulation (EC) No 767/2008 and the (Convention implementing the Schengen Agreement) as referred to under point 1.

- **Legal basis**

The present revised proposal uses Article 77(2)(b) and (d) of the Treaty on the Functioning of the European Union as the legal basis for this Regulation. Article 77(2)(b) and (d) is the appropriate legal basis for further specifying the measures on the crossing of the external borders of the Member States and developing standards and procedures to be followed by Member States in carrying out checks on persons at such borders. Article 77(2)(b) and (d) is the legal basis of the establishment of the EES. In addition, the revised proposal relies on Article 87(2)(a) as a legal basis to allow access for law enforcement purposes and Article 88(2)(a) to allow access by Europol, both under strict conditions Both these additional legal bases for the law enforcement and Europol access to EES data command the same ordinary legislative procedure which is applicable under Article 77(2)(b) and (d).

- **Subsidiarity principle**

¹² SEC (2008) 153.

¹³ SWD (2013) 47.

Under Article 77(2)(b) of the Treaty on the Functioning of the European Union, the Union has the power to adopt measures relating to the checks on persons and efficient monitoring of the crossing of external borders of the Member States. The current EU provisions on the crossing of the external borders of the Member States need to be modified to take into account that there are currently no reliable means to monitor the travel movements of third country nationals admitted for a short stay given the complexity and slowness of the current stamping obligation, which is insufficient for allowing Members States' authorities to assess the authorised stay at the border check of the traveller or at checks within the territory and the very limited value of national systems for such purposes in an area without internal border control.

The information on who has been refused entry into EU territory, on who is on EU territory and who complies with the maximum allowed short stay of 90 days within 180 days, on nationalities and groups (visa exempt/required) of travellers overstaying and to support random checks within the territory to detect irregularly staying persons should be available to increase the efficiency of migration management.

A common regime is needed in order to establish harmonised rules on the records of refusals of entry, cross border movements and monitoring of authorised short stays for the Schengen area as a whole.

Therefore, this objective of the proposal cannot be sufficiently achieved by the Member States.

A revision of the 2013 EES proposal is also required in order to allow law enforcement access to data in the EES for the purpose of the fight against terrorism and serious crime and ensure a high level of internal security. This objective cannot be sufficiently achieved by the Member States, since such an amendment can only be proposed by the Commission.

- **Proportionality principle**

Article 5 of the Treaty on the European Union states that action by the Union shall not go beyond what is necessary to achieve the objectives of the Treaty. The form chosen for this EU action must enable the proposal to achieve its objective and be implemented as effectively as possible. The proposed initiative constitutes a further development of the Schengen acquis in order to ensure that common rules at external borders are applied in the same way in all the Member States which have abolished controls at internal borders. It creates an instrument providing to the European Union information on how many third country nationals enter and leave the territory of the EU, which is indispensable for sustainable and evidence based policy making in the field of migration and visa. It also grants access to the EES to law enforcement authorities, which is a timely, accurate, secure and cost-efficient way to identify visa exempt nationals who are suspects (or victims) of terrorism or of a serious crime and to enable them to consult the travel history of both visa holder and visa exempt third country nationals who are suspects (or victims) of such crimes.

The proposal which conception is driven by the *privacy by design* principles is proportionate in terms of the right to protection of personal data in that it does not require the collection and storage of more data for a longer period than is absolutely necessary to allow the system to function and meet its objectives. In addition, all the safeguards and mechanisms required for the effective protection of the fundamental rights of travellers particularly the protection of their private life and personal data will be foreseen and implemented.

No further processes or harmonisation will be necessary at EU level to make the system work; thus the envisaged measure is proportionate in that it does not go beyond what is necessary in terms of action at EU level to meet the defined objectives.

The preferred option is also proportionate in terms of costs, taking into account the benefits the system will provide to all Member States in managing the common external border and progressing towards a common EU migration policy.

The proposal therefore complies with the proportionality principle.

- **Choice of instrument**

Proposed instruments: Regulation.

Other means would not be adequate for the following reason(s):

The present proposal will set up a centralised system through which Member States cooperate with each other, something which requires a common architecture and operating rules. Moreover it will lay down rules on border checks at the external borders and on access to the system including for the purpose of law enforcement which are uniform for all Member States. As a consequence, only a Regulation can be chosen as a legal instrument.

- **Fundamental rights**

The proposed Regulation has an impact on fundamental rights, notably on right to dignity (Article 1 of the Charter of Fundamental Rights of the EU); the prohibition of slavery and forced labour (Article 5 of the Charter); 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), right to asylum (Article 18 of the Charter) and protection in the event of removal, expulsion or extradition (Article 19 of the Charter), the right to non-discrimination (Article 21 of the Charter), the rights of the child (Article 24 of the Charter) and the right to an effective remedy (Article 47 of the Charter).

The prohibition of slavery and forced labour as well as the right to liberty and security are positively affected by the implementation of an EES. A better and more accurate identification (through the use of biometrics) of third country national crossing the external border of the Schengen area supports the detection of identity fraud, human being trafficking (particularly in the case of minors) and cross border criminality and thus contributes to improving the security of the citizens present in the Schengen area.

Concerning the right to protection of personal data, the proposal contains safeguards as regards personal data, in particular access thereto, which should be strictly limited only to the purpose of this Regulation and to the therein designated competent authorities. Safeguards as regards personal data also include the right of access to or the right of correction or deletion of data. The limitation of the retention period of data referred to above in chapter 1 of this explanatory memorandum also contributes to the respect for personal data as a fundamental right.

The proposal provides for access to the EES for the prevention, detection or investigation of terrorist offences or other serious criminal offences for the purposes of identification of third country nationals crossing the external borders and for the purpose of accessing data on their travel history. As stipulated by Article 52(1) of the Charter, any limitation to the right to the protection of personal data must be appropriate for attaining the objective pursued and not going beyond what is necessary to achieve it. Article 8(2) of the European Convention of Human Rights also recognises

that interference by a public authority with a person's right to privacy may be justified as necessary in the interest of national security, public safety or the prevention of crime, as it is the case in the current proposal. The ECJ has also recognised¹⁴ that the fight against terrorism and serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques and hence, access to personal data granted for those specific purposes could be justified if considered necessary.

The proposal provides for access to the EES for the prevention, detection or investigation of terrorist offences or other serious criminal offences for the purposes of identification of third country nationals crossing the external borders and for the purpose of accessing data on their travel history. Access to the EES for identification purposes should only be possible where a prior search has been conducted in national databases without success and, in the case of searches with fingerprints where a prior search has been conducted in the automated fingerprint verification system under Decision 2008/615/JHA. Although data exist in the VIS on visa holders, neither data on visa exempt nationals or data on travel movements are available in any other EU database.

Access to EES data for law enforcement purposes may only be granted for the prevention, detection or investigation of criminal offences or other serious criminal offences as defined in Council Framework Decisions 2002/475/JHA on combatting terrorism and 2002/584/JHA on the European arrest warrant and only if it is necessary for a specific case. Moreover, designated law enforcement authorities may only request access to EES data if there are reasonable grounds to consider that such access will substantially contribute to the prevention, detection or investigation of the criminal offence in question. Such request are verified by a designated law enforcement authority in order to check whether the strict conditions for requesting access to the EES for law enforcement purposes are fulfilled.

Furthermore, the proposal also lays down strict data security measures to ensure the security of personal data processed and establishes supervision of the processing activities by independent public data protection authorities and documentation of all searches conducted. The proposal also states that the processing of all personal data carried out by law enforcement authorities on the EES once they have been extracted is subject to Council Framework Decision 2008/977/JHA.

The proposal establishes strict access rules to the EES system and the necessary safeguards. It also foresees the individuals' rights of access, correction, deletion and redress in particular the right to a judicial remedy and the supervision of processing operations by public independent authorities,. Therefore, the proposal fully complies with the Charter of Fundamental Rights of the European Union, in particular as regards the right to the protection of personal data, and is also in line with Article 16 TFEU which guarantees everyone the right to protection of personal data concerning them.

4. BUDGETARY IMPLICATIONS

In the 2013 EES proposal, reference was made to the Commission's proposal for the next multi-annual financial framework (MFF) which included a proposal of 4,6 billion EUR for the Internal security Fund (ISF) for the period 2014-2020. In the 2013 EES proposal, 1,1 billion EUR was set aside as an indicative amount for the development of an EES and an RTP assuming development costs would start from 2015. This amount was calculated on the basis of the development and

¹⁴ Judgement of the ECJ of 8 April 2014 in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd and Others EU:C:2014:238, paragraph 51.

operational management of two separate systems and on 3 years of development and 4 years of operations.

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 574/2000/EC (ISF Borders Regulation) provided in Article 5.5b) that EUR 791 million should be allocated for developing IT systems, based on existing and/or new IT systems, supporting the management of migration flows across the external borders. The amount of EUR 791 million corresponded to 3 years of development (2017-2019 inclusive) with already some preparatory activities in 2016 with operations starting in 2020.

Following the technical study and the Impact Assessment, the current proposal is based on the preferred option of a single EES system and the amount needed has been assessed as EUR 480 million which takes also into account the purpose of law enforcement access. Consequently, a proposal for the amendment of the ISF Borders Regulation is included in the present proposal to align it to the new reduced amount.

This financial support would cover not only the costs of central components for the entire MFF period (EUR 288 million – at EU level, both development and operational cost via indirect management) but also the costs for the integration of the existing national border infrastructures in Member States with the EES via the National Uniform Interfaces (NUI) (EUR 120 million - via direct management). Providing financial support for national integration costs would ensure that difficult economic circumstances at national level do not jeopardise or delay the projects. During the development phase (2017-2019) the Commission will spend a total amount of 52,7 mio € (via direct management) for the expenses related to the operations in the Member States.

Once the new system would be operational, future operational costs in the Member States could be supported by their national programmes in the framework of the ISF (shared management). An amount of EUR 20 million has been earmarked for this purpose within the overall envelope of EUR 480 million. This will include operational support for one year.

The cost model applied is explained in Annex 6 - Cost Model for EES System of the Impact Assessment.

5. ADDITIONAL INFORMATION

• Participation

This proposal builds upon the Schengen *acquis* in that it concerns the crossing of external borders. Therefore the following consequences in relation to the various protocols and agreements with associated countries have to be considered:

Denmark: In accordance with Articles 1 and 2 of the Protocol (no 22) on the position of Denmark, annexed to the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU), Denmark does not take part in the adoption by the Council of measures pursuant to Title V of part Three of the TFEU.

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.

United Kingdom and Ireland: In accordance with Articles 4 and 5 of the Protocol integrating the Schengen acquis into the framework of the European Union and Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland, and 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, the United Kingdom and Ireland do not take part in Regulation (EU) 2016/399 (Schengen Borders Code) nor in any other of the legal instruments which are commonly known as the "Schengen acquis", viz. the legal instruments organising and supporting the abolition of controls at internal borders and the flanking measures regarding the controls at external borders.

This Regulation constitutes a development of this acquis, and therefore, the United Kingdom and Ireland are not taking part in the adoption of this Regulation and are not bound by it or subject to its application.

In line with the judgment of the Court of Justice in case C-482/08, *United Kingdom v. Council*, ECLI:EU:C:2010:631, the circumstance that this Regulation has Articles 87(2)a) and Article 88(2)a) as legal bases alongside Article 77(2)b) and (d) TFEU does not affect the above conclusion, as the access for law enforcement purposes is ancillary to the establishment of the Entry/Exit System.

Iceland and Norway: The procedures laid down in the Association Agreement concluded by the Council and the Republic of Iceland and the Kingdom of Norway concerning the latter's association with the implementation, application and development of the Schengen acquis are applicable, since the present proposal builds on the Schengen acquis as defined in Annex A of this Agreement¹⁵.

Switzerland: This Regulation constitutes a development of the provisions of the Schengen *acquis*, as provided for by the Agreement between the European Union, the European Community and the Swiss Confederation on the latter's association with the implementation, application and development of the Schengen acquis¹⁶.

Liechtenstein: This Regulation constitutes a development of the provisions of the Schengen *acquis*, as provided for by 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 acquis¹⁷.

Croatia, Cyprus, Bulgaria and Romania: This Regulation establishing the EES replaces the obligation to stamp the passport of third country nationals. This provision was to be applied by the acceding Member States upon accession to the European Union.

¹⁵ OJ L 176, 10.7.1999, p. 36.

¹⁶ OJ L 53, 27.2.2008, p. 52.

¹⁷ OJ L 160, 18.6.2011, p. 19.

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), Article 87(2)(a) and Article 88(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 Committee¹,

Having regard to the opinion of the Committee of the Regions²,

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 Schengen area 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.

¹ OJ C , , p. .

² OJ C , , p. .

³ COM (2008) 69 final

- (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 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”*.
- (7) It is necessary to specify the objectives of the Entry/Exit System (EES) and its technical architecture, to lay down rules concerning its operation and use and to define responsibilities for the system, the categories of data to be entered into the system, the purposes for which the data are to be entered, the criteria for their entry, the authorities authorised to access the data and further rules on data processing and the protection of personal data.
- (8) The EES should apply to third country nationals admitted for a short stay to the Schengen area. It should also apply to third country nationals whose entry for a short stay has been refused.
- (9) The EES should have the objective of improving the management of external borders, preventing irregular immigration and facilitating 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 stay within the territory of the Member States.
- (10) To meet those objectives, the EES should process alphanumeric data and biometric data (fingerprints and facial image). 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 modus operandi of 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 third country national is not already enrolled under another identity or with another travel document) and to guarantee that sufficient data is available 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/EC⁴. The facial image of both visa exempt and visa holding third country nationals should be registered in the EES and it should be used as the main 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. Alternatively, that verification should be performed using fingerprints.
- (12) The EES should consist of a Central System, which will operate 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 VIS Central System and the 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.
- (13) Interoperability should be established between the EES and the VIS by way of a direct communication channel between the Central Systems to enable the border authorities using the EES to consult the VIS in order to retrieve visa-related data to create or update the individual file; to enable the border authorities to verify the validity of the visa and the identity of a visa holder by means of fingerprints directly against the VIS at the external borders 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 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 enable 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/EC of the European Parliament and of the Council⁵ should be amended accordingly.
- (14) 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.
- (15) Any processing of EES data should be proportionate to the objectives pursued and necessary for the performance of 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, 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.

⁴ Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS) (OJ L 213, 15.6.2004, p.5).

⁵ 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).

- (16) In the fight against terrorist offences and other serious criminal offences, it is imperative that law enforcement 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/JHA⁶ or other serious criminal offences as referred to in Council Framework Decision 2002/584/JHA⁷. 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 law enforcement 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 criminal intelligence 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 set out in this Regulation.
- (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 Council Decision 2009/371/JHA.⁸
- (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 should provide the law enforcement authorities of the Member States with a very valuable tool in preventing, detecting or investigating terrorist offences or other serious criminal offences, when for example the only evidence at a crime scene are latent fingerprints.

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

⁷ 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)

⁸ Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol) (OJ L 121, 15.5.2009, p. 37).

- (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 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 points should act independently of the designated authorities and should be responsible for ensuring, in an independent manner, strict compliance with the conditions for access as established in this Regulation. In exceptional cases of urgency, where early access is necessary to respond to a specific and actual threat related to terrorist offences or other serious criminal offences, the central access point should be able to process the request immediately and only carry out the verification afterwards.
- (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 with the national fingerprint databases of the Member State and with the automated fingerprinting identification systems of all other Member States under Council Decision 2008/615/JHA⁹ did not lead to the establishment of the identity of the data subject. Furthermore, access to the EES to consult the entry/exit records of a known person should be duly justified.
- (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 is necessary for the purposes of the EES. It is appropriate to keep the data related to third country nationals for a period of five 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. For third country nationals who are family members of a Union citizen to whom Directive 2004/38/EC¹⁰ applies

⁹ 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).

¹⁰ Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending

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 last exit.

- (26) A five year data retention period is necessary to allow the border guard performing the necessary risk analysis requested by the Schengen Borders Code before authorising a traveller entering the Schengen area. The processing of visa application in consular posts requires also analysing the travel history of the applicant to assess the use of previous visas and the respect of the conditions of stay. 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. The five year data retention period will reduce the re-enrolment frequency and will be beneficial for all travellers as the average border crossing time will decrease as will do the waiting time at border crossing points. Even for a traveller entering only once in the Schengen area, the fact that other travellers being already registered in the EES will not have to re-enrol will reduce the waiting time at border. This data retention period will also be necessary to allow for facilitation for the border crossing by using process accelerators and self-service systems. Such facilitation is dependent of the data registered in the system. A shorter data retention period would have a negative impact on the duration of border controls. A shorter data retention period would also reduce the group of travellers that can benefit of such facilitation and thereby undermine the stated objective of EES to facilitate border crossing.
- (27) The same retention period of five years would be necessary for data on persons 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 and for persons whose entry for a short stay {or on the basis of a touring visa} has been refused. The data should be deleted after the period of five years, unless there are grounds to delete it earlier.
- (28) 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 Council¹¹, 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.
- (29) Rules on the liability of the Member States in respect to damage arising from any breach of this Regulation should be laid down.

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).

¹¹ 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).

- (30) Directive 95/46/EC of the European Parliament and of the Council¹² 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 or verifying authorities of the Member States for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences.
- (31) The processing of personal data by the authorities of the Member States for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences pursuant to this Regulation should be subject to a standard of protection of personal data under their national law which complies with Council Framework Decision 2008/977/JHA¹³.
- (32) 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 assist the identification of a third country national in relation to his/her return and subject to strict conditions.
- (33) Regulation (EC) No 45/2001 of the European Parliament and the Council¹⁴ applies to the activities of the Union institutions or bodies when carrying out their tasks as responsible for the operational management of EES.
- (34) The independent supervisory authorities established in accordance with Article 28 of Directive 95/46/EC 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 25 of Council Framework Decision 2008/977/JHA should monitor the lawfulness of the processing of personal data for law enforcement purposes by the Member States, and the national supervisory authorities established in accordance with Article 33 of Decision 2009/371/JHA should monitor the lawfulness of data processing activities performed by Europol.
- (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 ...
- (37) The proposal establishes strict access rules to the EES system and the necessary safeguards. It also sets out the individuals' rights of access, correction, deletion and redress, in particular the right to a judicial remedy and the supervision of processing operations by public independent

¹² Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

¹³ Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (OJ L 350, 30.12.2008, p. 60).

¹⁴ 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).

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).

- (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 Council¹⁵.
- (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 Entry/Exit System, Article 20(2) of the Convention implementing the Schengen Agreement should be amended as it is incompatible with Article 77(2)(a) and (c) of the Treaty on Functioning of the European Union due to the fact that the common policy on visas cannot be based on the existence or non-existence of bilateral visa waiver agreements concluded by Member States and the authorised length of stay of third country nationals should not depend on the number and content of such bilateral agreements. Furthermore the Entry/Exit system could not take into account of and calculate the authorised length of stay of visa free third country nationals benefitting from such agreements and they should be eliminated.
- (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 Council¹⁶. 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.

¹⁵ Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

¹⁶ 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).

- (43) This Regulation establishing the EES replaces the obligation to stamp passports of third country nationals which is applicable by all acceding Member States. Stays in Member States which are not yet fully applying the Schengen *acquis* in accordance with their respective Acts of Accession should not be taken into account in the calculation of the duration of the authorised stay in the Schengen area. Such Member States should register in the EES the stay of third country nationals but the automated calculator in the system should not compute it as part of the authorised length of stay.
- (44) This Regulation is without prejudice to the application of Directive 2004/38/EC.
- (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/EC¹⁷; 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/EC¹⁸; 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 latter's association with the implementation, application and development of the Schengen *acquis*¹⁹ which fall within the area referred to in Article 1, point A of Council Decision 1999/437/EC²⁰.
- (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

¹⁷ 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).

¹⁸ 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).

¹⁹ OJ L 176, 10.7.1999, p. 36.

²⁰ 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).

with the implementation, application and development of the Schengen *acquis*²¹ 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/EC²² and with Article 3 of Council Decision 2008/149/JHA²³.

- (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 Confederation's association with the implementation, application and development of the Schengen *acquis*²⁴ 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/EU²⁵ and with Article 3 of Council Decision 2011/349/EU.²⁶
- (51) This Regulation constitutes an act 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,

²¹ OJ L 53, 27.2.2008, p. 52.

²² 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)

²³ 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)

²⁴ OJ L 160, 18.6.2011, p. 21.

²⁵ 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). .

²⁶ 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).

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 external borders of the Member States, for the calculation of the duration of their stay, and for the generation of alerts to Member States when authorised periods for stay have 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 {or on the basis of a touring visa} has been refused as well as the authority of the Member State which refused the entry and the reasons for the refusal.
2. This Regulation also lays down in its Chapter IV the conditions under which Member States' designated law enforcement authorities and the European Police Office (Europol) may obtain access for consultation of the EES for the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences.

Article 2

Scope

1. This Regulation applies to third country nationals admitted for a short stay {or on the basis of a touring visa} in the territory of the Member States subject to border checks in accordance with Regulation (EU) 2016/399 when crossing the external borders of the Member States. When entering and exiting the territory of the Member States, it applies to 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 under Union law and who do not hold a residence card referred to under Directive 2004/38/EC.
2. This Regulation also applies to third country nationals whose entry for a short stay {or on the basis of a touring visa} 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) family members of a Union citizen to whom Directive 2004/38/EC applies who hold a residence card pursuant to that Directive;
 - (b) family members of third country nationals enjoying the right of free movement under Union law who hold a residence card pursuant to Directive 2004/38/EC;
 - (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;

- (d) holders of long-stay visas;
- (e) nationals of Andorra, Monaco and San Marino;
- (f) persons or categories of persons exempt from or benefiting from facilitation of border crossing as referred to in Article 6a (3)(d),(e) and (f) of Regulation (EU) 2016/399.

This Regulation does not apply to family members 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 stay and the generation of alerts to Member States when authorised periods for stay have expired do not apply to 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 under Union law and who do not hold a residence card referred to under Directive 2004/38/EC.

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;
 - (2) 'border authorities' mean the competent authorities assigned, in accordance with national law, to carry out checks on persons at the external border crossing points in accordance with Regulation (EU) 2016/399;
 - (3) 'immigration authorities' mean the competent authorities assigned, in accordance with national law, to examine the conditions and take decisions related to the stay of third country nationals on the territory of the Member States;
 - (4) 'visa authorities' mean the competent authorities, including the central visa authorities and the authorities responsible for issuing visas at the external border, which are responsible in each Member State for examining visa applications, for taking decisions on visa applications and for taking decisions on whether to annul, revoke or extend visas,
 - (5) 'third country national' means any person who is not a citizen of the Union within the meaning of Article 20 of the Treaty, 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;
- (8) 'short stay visa' means an authorisation issued by a Member State with a view to an intended stay on the territory of the Member States of a duration of no more than 90 days in any 180 day period;
- (9) 'touring visa' means an authorisation issued by a Member State with a view to an intended stay in the territory of two or more Member States for a duration of more than 90 days in any 180 day period, provided that the applicant does not intend to stay for more than 90 days in any 180 day period in the territory of the same Member State;
- (10) 'carriers' mean any natural or legal person whose profession it is to provide transport of persons;
- (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 fingerprints of the index, middle finger, ring finger and little finger from the right hand, where present, and otherwise from the left hand, or a latent fingerprint;
- (16) 'facial image' means digital images of the face with sufficient image resolution and quality to be used in automated biometric matching;
- (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 a 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) 'Frontex' means the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union established by Regulation (EC) No 2007/2004;
- (21) 'supervisory authority' means the supervisory authorities established in accordance with Article 28 of Directive 95/46/EC;

- (22) 'national supervisory authority' as regards law enforcement purposes means the supervisory authorities established in accordance with Article 25 of Council Framework Decision 2008/977/JHA;
 - (23) 'national supervisory body' means the supervisory bodies established in accordance with Article 33 of Decision 2009/371/JHA;
 - (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;
 - (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;
- 2. The terms defined in Article 2 of Directive 95/46/EC shall have the same meaning in this Regulation in so far as personal data are processed by the authorities of Member States for the purpose laid down in Article 5 of this Regulation.
 - 3. The terms defined in Article 2 of Framework Decision 2008/977/JHA 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.

Article 4 *Set-up of the EES*

The Agency for the operational management of large-scale information systems in the area of freedom, security and justice ('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.

Article 5 *Purpose of the EES*

By recording, storing and providing access to Member States to the date, time and place of the entry and exit and refusals of entry of third country nationals at external borders, the EES shall:

- (a) 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 {or on the basis of a touring visa};

- (b) assist in the identification of any person who does not, or does no longer fulfil the conditions for entry to or stay on the territory of the Member States;
- (c) allow to identify and detect overstayers (also within the territory) and enable competent national authorities of the Member States to take appropriate measures including to increase the possibilities for return
- (d) allow to electronically check refusals of entry in the EES;
- (e) free up border control resources from performing checks that can be automated and enable better focus on the assessment of third country nationals;
- (f) enable consulates to have access to information on the lawful use of previous visas;
- (g) inform third country nationals of the duration of their authorised stay;
- (h) gather statistics on the entries and exits, refusals of entry and overstays of third country nationals to improve the assessment of the risk of overstays and to support evidence-based Union migration policy making;
- (i) combat identity fraud;
- (j) contribute to the prevention, detection and investigation of terrorist offences or of other serious criminal offences;
- (k) enable identifying and apprehending terrorist, criminal suspects as well as of victims crossing the external borders;
- (l) enable generating information on travel histories of terrorist, criminal suspects as well as of victims for investigations related to terrorism or serious crime.

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;
 - (c) a Secure Communication Channel between the EES Central System and the VIS Central System;
 - (d) a Communication Infrastructure between the Central System and the National Uniform Interfaces.

2. The EES Central System shall be hosted by eu-LISA in its two 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/EC²⁷, 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. A separate virtual private network dedicated to the EES shall be established in addition to the existing private virtual network of the VIS to ensure the logical separation of VIS and EES data.

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 (EC) No 767/2008²⁸ provide for it.
2. The interoperability requirement 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 individual file of a visa holder in the EES in accordance with Article 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 EES 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 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 pursuant to Article 21 of this Regulation and Article 18(2) of Regulation (EC) No 767/2008;
 - (d) verify at the external borders 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 cannot be verified against the EES, verify at the external borders 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.

²⁷ Commission Decision 2008/602/EC of 17 June 2008 laying down the physical architecture and requirements of the national interfaces and of the communication infrastructure between the Central VIS and the national interfaces for the development phase (OJ L 194, 23.7.2008, p. 3).

²⁸

3. The interoperability requirement shall enable the visa authorities using the VIS to consult the EES from the VIS in order to:
 - (a) examine visa applications and adopt decisions relating to those applications in accordance with Article 22 of this Regulation and Article 15(4) of Regulation (EC) No 767/2008;
 - (b) update the visa related data in the EES 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.

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, including border, visa and immigration authorities. 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.

Within three months after the EES has started operations in accordance with Article 60, a consolidated list of those authorities shall be published in *the Official Journal of the European Union*. Where there are amendments thereto, eu-LISA shall publish an updated consolidated list once a year.

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 in using the EES, it does not discriminate against third country nationals on the grounds of sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation and that it fully respects human dignity and the integrity of the person. Particular attention shall be paid to the specific situation of children, the elderly and persons with a disability. In particular, when retaining 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 authorised duration of stay in accordance with Article 6(1) of Regulation (EU) 2016/399 for third country nationals registered in the EES admitted for a short stay {or on the basis of a touring visa}.

The calculator shall not apply to 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 under Union law and who do not hold a residence card referred to under Directive 2004/38/EC.

2. The automated calculator shall:
 - (a) inform the competent authorities of the authorised length of stay on entry and whether the number of authorised entries of the single or double entry visas have been previously used;
 - (b) identify third country nationals upon exit who have overstayed.
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 {or the touring visa}, in accordance with Article 8(9) of Regulation (EU) 2016/399.
4. Stays in Member States which are not yet fully applying the Schengen *acquis* in accordance with their respective Acts of Accession shall not be taken into account in the calculation of the duration of the authorised stay in the Schengen area. Those Member States shall register the stays of third country nationals in the EES. The automated calculator in the system shall not however compute stays in Member States which are not yet fully applying the Schengen *acquis* as part of the authorised length of stay.

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 length of stay and identify records for which the maximum stay allowance has been exceeded.
2. 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.

Article 12

Web service

1. In order to enable third country nationals to verify at any moment the remaining authorised length of stay, a secure internet access to a web service hosted by eu-LISA in its two 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 dates. On that basis, the web service shall provide them with an OK/NOT OK answer. 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 data.

2. Carriers may use the secure internet access to the web service referred to in paragraph 1 to verify whether or not third country nationals holding a single or double entry visa have already used the visa. The carrier shall provide the data listed in Article 14(1)(d). 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.
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 border 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 their identity. Where a third country national uses a self-service system for pre-enrolment of data or for the performance of border checks [should this self-service system not be defined or explained?] , 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, enter an entry/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) shall be added to the individual file and the data referred to in Article 17(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 travel document which differs from the one which was previously registered, the data referred under Article 14(1)(f) shall also be updated if the facial image recorded in the chip of the new travel document can be extracted electronically.
3. Where it is necessary to create or update the individual file data of a visa holder, the border authorities may retrieve and import the data provided for in Article 14(1) (d), (e) and (g) directly from the VIS in accordance with 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, 15 and 16 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 that needs to be updated. The data shall be

confirmed by the border guard 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(1)(d), (e) and (g) may be retrieved and imported directly 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. Where it is necessary to create an individual file or to update the facial image referred to in Article 14(1)(f), the facial image can only be extracted electronically from the electronic Machine Readable Travel Documents (eMRTD) and inserted into the individual file where it has been verified that the facial image recorded in the chip of the eMRTD corresponds to the live facial image of the concerned third country national.

Article 14 *Personal data for visa holders*

1. The border authority shall create the individual file of the visa holding third country national by entering the following data:
 - (a) surname (family name); first name(s) (given names); date of birth; nationality or nationalities; sex;
 - (b) type, number 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) the short stay visa sticker number, including the three letter code of the issuing Member State, the type of visa, the date of end of maximum duration of the stay as authorised by the visa which needs to be updated at each entry and the date of expiry of the validity of the visa, if applicable;
 - (e) at the first entry on the basis of the short stay visa, the number of entries and the authorised period of stay as indicated on the visa sticker;
 - (f) the facial image, where possible extracted electronically from the eMRTD, and where this is not possible, taken live;
 - (g) the visa sticker number of the touring visa, the type of visa and the date of expiry of the validity of the visa, if applicable.

2. On each entry of the visa holding third country national, 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;
3. On each exit, the following data shall be entered in the entry/exit record linked to the individual file of that visa holding third country national:
 - (a) date and time of the exit;
 - (b) the border crossing point of the exit.
4. Where there is no exit data immediately following the date of expiry of the authorised length of stay, the entry/exit record shall be identified with a mark or flag by the system and the data of the visa holding third country national identified as an overstayer shall be entered into the list referred to in Article 11.
5. In order to create the individual file of a visa holding third country national the data provided for in paragraph 1 (d), (e) and (g) may be retrieved and imported directly from the VIS by the border authority in accordance with Article 18a of Regulation (EC) No 767/2008.

Article 15

Personal data for third country nationals exempt from the visa obligation

1. For third country nationals exempt from the visa obligation, the border authority shall enter into their individual file the data provided for in Article 14(1)(a), (b), (c) and (f). In addition it shall enter into that individual file the four fingerprint of the index, middle-finger, ring-finger and little finger from the right hand, and where this is not possible the same fingers from the left hand, in accordance with the specifications for the resolution and use of fingerprints adopted by the Commission in accordance with Article 61(2). For third country nationals exempt from the visa obligation, Articles 14(2) to 14(4) shall apply.
2. Children under the age of 12 shall be exempt from the requirement to give fingerprints for legal reasons.
3. Persons for whom fingerprinting is physically impossible shall be exempt from the requirement to give fingerprints for factual reasons.

However, where the physical impossibility is of a temporary nature, the person shall be required to give the fingerprints at the subsequent entry. The border authorities shall be entitled to request further clarification on the grounds for the temporary impossibility to provide fingerprints.

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 for legal or factual reasons pursuant to paragraphs 2 or 3, the specific data field shall be marked as 'not applicable'. The system shall allow a distinction to be made between the cases where fingerprints are not required to be provided for legal reasons and the cases where they cannot be provided for factual reasons.

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 the data required pursuant to Article 14(1) in the case of visa holding third country nationals and the data required pursuant to Article 15(1) in the case of visa exempt third country nationals.
2. In order to create the individual file of visa holder third country nationals, the data provided for in Article 14 (1) (d), (e) and (g) may be retrieved and imported directly from the VIS into the EES by the competent border authority in accordance with Article 18a of Regulation (EC) No 767/2008.
3. For both visa holding 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.
4. Where a previous file already exists in the EES the data provided for in paragraph 2 shall be added to the existing file.

Article 17

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

1. Where a decision has been taken to revoke or annul an authorisation to 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 individual file:
 - (a) the status information indicating that the authorisation to 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 to 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 to stay or the visa or to extend the duration of the authorised stay or the visa;
 - (d) the new visa sticker number including the three letter code of the issuing country;
 - (e) the period of the extension of the authorised duration of stay;
 - (f) the new expiry date of the authorisation to stay or the visa.
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 of the authorisation to stay, which shall be:
 - (a) the grounds on which the person is being expelled;
 - (b) any other decision taken by the competent authorities of the Member State, in accordance with national legislation, resulting in the removal or departure of the third country national who does not fulfil or no longer fulfils the conditions for the entry into or for the 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 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 is not registered in the EES or the entry/exit record does not contain an exit date following the date of expiry of the authorised length of stay, the competent authorities may presume that the third country national does not fulfil or no longer fulfils the conditions relating to duration of stay in the territory of the Member States.

In that case Article 12 of Regulation (EU) 2016/399 shall apply and if that presumption is rebutted by proof that the third country national concerned has respected the conditions relating to the condition of short stay, 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

In the event of technical impossibility in entering 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. If this is not possible, the data shall be temporarily stored locally. 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 can be carried out at any time and for any of their border crossing points.

Article 20

Transitional period and transitional measures

1. For a period of six months after the EES has started operations, in order to verify at entry that the third country national has not exceeded the number of entries authorised by the single or double entry visa and to verify at entry and at exit that third country nationals entering for a short stay have not exceeded the length of the maximum authorised stay, 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 and has not yet exited it before the EES has started operations, an individual file shall be created and the date of that entry as stamped in the passport shall be entered in the entry/exit record in accordance with Article 14(2) when the third country national exits. 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 external borders

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 control tasks.
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).

In addition, for third country nationals who are subject to a visa requirement to cross the external borders, the border authorities may launch a search in the VIS directly from the EES using the same alphanumeric data for the purposes of carrying out the consultation of the VIS for verification at external borders in accordance with Article 18 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). Where the technology is not available at the border crossing for the use of live facial image, 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 visa holding third country nationals, 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 competent authority shall be given access to consult the data of the individual file of that third country national and the entry/exit 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 to cross the external borders, 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 competent 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 to cross the external borders 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 competent 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 is not subject to the application of Regulation (EC) No 767/2008 in accordance with its Act of Accession, the border authorities shall consult the VIS in accordance with point(a) or (b) 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 external borders of a Member State which is subject to the application of Regulation (EC) No 767/2008.

CHAPTER III

Entry of data and use of the EES by other authorities

Article 22

Use of the EES for examining and deciding on visa applications

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 Council²⁹
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 visa sticker number, including the three letter code of the issuing Member State referred to in Article 14(1)(d);
 - (c) the biometric data as referred to in Articles 14(1)(f) and 15.
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 linked to it.

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 data referred to in Article 14(1)(a), (b), (c) and (f).
3. If the search with the data set out in paragraph 2 indicates that data on the third country national are recorded in the EES, the competent authority shall be given access to consult the data of the individual file of that third country national and the entry/exit records linked to it.

²⁹ 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)

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 whether the conditions for entry to or stay on the territory of the Member States are fulfilled, the authorities of the Member States competent to carry out checks within the territory of the Member States as to whether the conditions for entry to, stay or residence on the territory of the Member States are fulfilled, shall have access to search with the data referred to in Article 14(1)(a), (b) and (c).

If the search indicates that data on the third country national are recorded in the EES, the competent authorities shall compare the live facial image of the third country national with the facial image referred to in Article 14(1)(f). Where the technology is not available for the use of live facial imaging, the competent authorities shall proceed with the verification of fingerprints of visa exempt third country nationals in the EES and of visa holding third country nationals 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 competent authority shall be given access to consult the data of the individual file of that person and the entry/exit record(s) linked to it.
3. Where the search with the data set out in paragraph 2 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 border authorities shall have access to data for identification in accordance with Article 25.

Article 25
Access to data for identification

1. 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 to, for stay or for residence on the territory of the Member States, the competent authorities for carrying out checks at external border crossing points in accordance with Regulation (EU) 2016/399 or within the territory of the Member States as to whether the conditions for entry to, stay or residence on the territory of the Member States are fulfilled shall have access to search with the biometric data of that third country national referred to in Articles 14(1)(f) and 15(1).

Where the search with the data referred to in Articles 14(1)(f) and 15(1) 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 external borders, 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 and the facial image has failed, the search shall be carried out with the data referred to in Article 14(1)(a) or (b) or in both.

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

CHAPTER IV:

Procedure and conditions for access to the EES for law enforcement purposes

Article 26

Member States' designated law enforcement authorities

1. Member States shall designate the law enforcement 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 in a declaration to eu-LISA and the Commission its designated authorities and may at any time amend or replace its declaration with another declaration. The declarations shall be published in the *Official Journal of the European Union*.
3. Each Member State shall designate a central access point which shall have access to the EES. The central access point shall be an authority of the Member State which is responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences. 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 independently 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.

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 in a declaration to eu-LISA and the Commission their central access point(s) and may at any time amend or replace its declaration with another declaration. The declarations shall be published in the *Official Journal of the European Union*.
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 an authority which is authorised to request access to the EES through its designated central access point in order to prevent, detect and investigate terrorist offences or other serious criminal offences. The designated authority shall be an operating unit of Europol.
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 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 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 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 26(5) in such a way as to not compromise the security of the data.
2. In an exceptional 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 an exceptional case of urgency actually existed. The ex post verification shall take place without undue delay 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, thus making a search of the database proportionate if there is an overriding public security concern;
 - (b) access for consultation is necessary in a specific case;
 - (c) reasonable grounds exist to consider that the consultation of the EES data may substantially contribute to the prevention, detection or investigation of any of the

criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category covered by this Regulation;

2. The access to the EES as a criminal identification 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 without success;
 - (b) in the case of searches with fingerprints, a prior search has been conducted without success in the automated fingerprint verification system of the other Member States under Decision 2008/615/JHA where comparisons of fingerprints are technically available.

However, that prior search does not have to be conducted 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. Those reasonable grounds shall be included in the electronic request for comparison with EES data sent by the designated authority to the central access point(s).

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 provided the searches carried out in accordance with points(a) and (b) of the first subparagraph did not lead to the verification of the identity of the data subject.

3. The access to the EES as a criminal intelligence tool to consult the travel history or the periods of stay in the Schengen area 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 and where there is a duly justified need to consult the entry/exit records of the person concerned.
4. Consultation of the EES for identification shall be limited to searching in the application file with any of the following EES data:
 - (a) Fingerprints (including latents) of visa exempt third country nationals;
 - (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) and Article 15(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 or in the entry/exit records:
 - (a) Surname(s) (family name); first name(s) (given names); date of birth, nationality or nationalities and 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 latents);
- (e) Facial image;
- (f) Date and time of entry, entry authoriser authority 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 and the entry/exit records including data entered in respect of revocation or extension of authorisation to 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, thus making a search of the database proportionate if there is an overriding public security concern;
 - (b) the consultation is necessary in a specific case;
 - (c) reasonable grounds exist to consider that the consultation may substantially contribute to the prevention, detection or investigation of any of the criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category covered by this Regulation.
2. The conditions laid down in Article 29 (2) 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 paragraph 1 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 for five 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 for five years and one day following the date of the last exit record if there is no entry record within five 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 authorised period of 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 to paragraphs (2) and (3), the entry/exit record(s) generated by third country nationals in their condition of 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 under Union law and who do not hold a residence card referred to under Directive 2004/38/EC, shall be stored in the EES for a maximum of one year after the last exit record.
5. Upon expiry of the retention period referred to in paragraphs 1 and 2 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 correcting or deleting such data.
- 2 If the Member State responsible has evidence to suggest that data recorded in the EES are factually inaccurate or that data were processed in the EES in contravention of this Regulation, it shall check the data concerned and, if necessary, amend 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 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, amend or erase them from the EES without delay 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 14 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 the Member State responsible or a Member State other than the Member State responsible has evidence to suggest that visa-related data recorded in the EES are factually inaccurate 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 amend 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 correct or delete them immediately from the VIS and inform the Member State responsible or the Member State to which the request has been made which shall, if necessary, amend or delete them from the EES without delay and, where applicable, from the list of identified overstayers referred to in Article 11.
5. The data of identified persons referred to in Article 11 shall be deleted without delay from the list referred to in that Article and shall be corrected 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 authorised duration of stay due to unforeseeable and serious events, that he or she has acquired a legal right to stay or in case of errors. The third country national shall have access to an effective judicial remedy to ensure the data is amended.
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 records linked to it in accordance with Articles 14 and 15 shall be deleted without delay from the EES as well as, where applicable, from the list of identified persons referred to in Article 11:
 - (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.

Where a third country national has acquired the nationality of Andorra, Monaco or San Marino 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.

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, and the Communication Infrastructure, in particular measures for:

- (a) the specifications for the resolution and use of fingerprints for biometric verification and identification in the EES;
- (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;
- (g) the specifications and conditions for the web-service referred to in Article 12;
- (h) the common leaflet referred to Article 44(3);
- (i) the specifications and conditions for the website referred to in Article 44(3);
- (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).

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 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, 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 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.

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 eight members appointed by eu-LISA's Management Board from among its members, the Chair of the EES Advisory Group referred to in Article 62 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 once a month. 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 the Member State holding the Presidency, provided it 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 or, if

this requirement is not met, by the Member State which shall next hold the Presidency and which meets that requirement.

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. It shall meet at least once a month 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, at all times the best available technology, subject to a cost-benefit analysis. eu-LISA shall also be responsible for the operational management of the Communication Infrastructure between the Central system and the National Uniform Interfaces and for the web-service referred to in Article 12.

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*

1. Each Member State shall be responsible for:
 - (a) the integration of the existing national border infrastructure 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 excepted points (j), (k) and (l);
 - (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 and Europol shall connect their respective central access points referred to in Article 26 and 27 to the National Uniform Interface.
- 3. Each Member State shall use automated procedures for processing the data.
- 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.

Article 36
Responsibility for the use of data

- 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 2(d) of Directive 95/46/EC 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 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 files and national entry exit system in full respect of Union Law.
2. The data shall not be kept in the national files or national entry/exit systems longer than it is 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) and (c) and Article 15(1) may be transferred or made available to a third country or to an international organisation listed in the Annex in individual cases, if necessary in order to prove the identity of third country nationals for the purpose of return, only where the following conditions are satisfied:
 - (a) the Commission has adopted a decision on the adequate protection of personal data in that third country in accordance with Article 25(6) of Directive 95/46/EC, or a readmission agreement is in force between the Community and that third country, or Article 26(1)(d) of Directive 95/46/EC applies;
 - (b) the third country or international organisation agrees to use the data only for the purpose for which they were provided;
 - (c) the data are transferred or made available in accordance with the relevant provisions of Union law, in particular readmission agreements, and the national law of the Member State which transferred or made the data available, including the legal provisions relevant to data security and data protection;
 - (d) the Member State which entered the data in the EES has given its consent.
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 within the meaning of Article 2(b) of Framework Decision 2008/977/JHA.

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 border infrastructure, adopt the necessary measures, including a security plan and a business continuity and disaster recovery plan, in order to:
 - (a) physically protect data, including by making contingency plans for the protection of critical infrastructure;
 - (b) deny unauthorised persons access to 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;
 - (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 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 national supervisory authorities referred to in Article 49 and to the national supervisory authorities referred to in Article 52(2) without delay at their request;
 - (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;

- (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.

Article 40 *Liability*

- 1. Any person or Member State that has suffered damage as a result of an unlawful processing operation or any act incompatible with this Regulation shall be entitled to receive compensation from the Member State which is responsible for the damage suffered. That Member State shall be exempted from its liability, in whole or in part, if it proves that it is not responsible for the event 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 records*

- 1. eu-LISA shall keep records of all data processing operations within the EES. Those records 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. In addition, each Member State shall keep records of the staff duly authorised to enter or retrieve the data.
- 2. For the consultations listed in Article 7, a record 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 records of the concerned data processing operations are kept when the competent authorities launch a data processing operation directly from one system to the other..
- 3. Such records may be used only for the data protection monitoring of the admissibility of data processing as well as to ensure data security. Those records shall be protected by appropriate measures against unauthorised access and deleted one year after the retention period referred to in Article 31 has expired, if they are not 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 authority.

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, including administrative and criminal penalties in accordance with national law, that are effective, proportionate and dissuasive.

CHAPTER VII
Rights and supervision on data protection

Article 44
Right of information

1. Without prejudice to the right of information in Article 10 of Directive 95/46/EC, third country nationals whose data are recorded in the EES shall be informed by the Member State responsible in writing 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 to have their fingerprints taken;
 - (c) the obligation on all third country nationals subject to registration in the EES to have their facial image recorded;
 - (d) that the collection of the data is mandatory for the examination of entry conditions;
 - (e) the right of access to data relating to them, the right to request that inaccurate data relating to them be corrected or that unlawfully processed data relating to them be deleted, including the right to receive information on the procedures for exercising those rights and contact details of the national supervisory authorities, or of the European Data Protection Supervisor if applicable, which shall hear claims concerning the protection of personal data.
2. The information provided in paragraph 1 of this Article shall be provided at the time when the individual file of the person concerned is being created in accordance with Articles 14, 15 or 16.
3. A common leaflet and a website containing at least 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). The leaflet and the content of the website

shall be clear and simple and available in a linguistic version the person concerned understands or is reasonably supposed to understand.

The leaflet and the website 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 national supervisory authorities, as well as contact details of the office of the controller and national supervisory authorities.

Article 45 *Information campaign*

The Commission shall, in cooperation with the national supervisory authorities and the European Data Protection Supervisor, accompany the start of the EES operation with an information campaign informing the public about the objectives, the data stored, the authorities having access and the rights of persons.

Article 46 *Right of access, correction and deletion*

1. Without prejudice to Article 12 of Directive 95/46/EC any third country national shall have the right to obtain the data relating to him or her recorded in the EES and of the Member State which transmitted it to the EES.
2. If a request for correction or deletion 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 one 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 14 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 one month.
3. In the event that data recorded in the EES are factually inaccurate or have been recorded unlawfully, the Member State responsible or, where applicable, the Member State to which the request has been made shall correct or delete the 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 correct or delete data relating to him.

In the event that visa-related data recorded in the EES are factually incorrect 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 the Member State to which the request was made, shall contact the authorities of the Member State responsible for entering these data in the VIS within a time limit of 14 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 which shall, if necessary, amend or erase them 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 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 correct or delete data relating to him.
5. The Member State responsible or, where applicable, the Member State to which the request has been made shall also provide the person concerned with information explaining the steps which he can take if he does not accept the explanation for the decision pursuant to paragraph 5. 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, including from the supervisory authorities, that is available in accordance with the laws, regulations and procedures of that Member State.
6. Any request made pursuant to paragraphs 1 and 2 shall contain the necessary information to identify the person concerned, including fingerprints. 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 requests data relating to him in accordance with paragraph 2, the competent authority 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 national supervisory authorities without delay.

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(3), (4) and (5).
2. In each Member State, the supervisory authority shall, upon request, assist and advise the person concerned in exercising his right to correct or delete data relating to him in accordance with Article 28(4) of Directive 95/46/EC.

In order to achieve those aims, the supervisory authority of the Member State responsible which transmitted the data and the supervisory authorities of the Member States to which the request has been made shall cooperate with each other.

Article 48

Remedies

1. In each Member State any person shall have the right to bring an action or a complaint before the competent authorities or courts of that Member State which refused the right of access to or the right of correction or deletion of data relating to him, provided for in Article 46.

2. The assistance of the supervisory authorities shall remain available throughout the proceedings.

Article 49

Supervision by the national supervisory authority

1. Each Member State shall ensure that the national supervisory authority or authorities designated pursuant to Article 28(1) of Directive 95/46/EC shall monitor the lawfulness of the processing of personal data referred to in Articles 13 to 19 by the Member State concerned, including their transmission to and from the EES.
2. The supervisory authority shall ensure that an audit of the data processing operations in the National System is carried out in accordance with relevant international auditing standards at least every four years.
3. Member States shall ensure that their supervisory authority has sufficient resources to fulfil the tasks entrusted to it under this Regulation.
4. In relation to the processing of personal data in the EES, each Member State shall designate the authority which is to be considered as controller in accordance with Article 2(d) of Directive 95/46/EC and which shall have central responsibility for the processing of data by this Member State. Each Member State shall communicate the details of this authority to the Commission.
5. Each Member State shall supply any information requested by the supervisory authorities and shall, in particular, provide them with information on the activities carried out in accordance with Articles 35, 36(1) and 39. Each Member State shall grant the supervisory authorities access to their records pursuant to Article 30 and allow them 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 ensure that the personal data processing activities of eu-LISA concerning the EES are carried out in accordance with this Regulation.
2. The European Data Protection Supervisor shall ensure that an audit of the Agency's personal data processing activities is carried out in accordance with relevant international auditing standards at least every four years. A report of that audit shall be sent to the European Parliament, the Council, eu-LISA, the Commission and the national 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 records referred to in Article 41 and allow him access to all its premises at any time.

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

1. The national supervisory authorities and the European Data Protection Supervisor shall actively cooperate within the framework of their responsibilities and shall ensure coordinated supervision of the EES and the National Systems.
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 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. The costs of these meetings shall be borne by the European Data Protection Supervisor. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary.
4. A joint report of activities shall be sent to the European Parliament, the Council, the Commission and eu-LISA every two years. That report shall include a chapter of each Member State prepared by the supervisory authority of that Member State.

Article 52
Protection of personal data for law enforcement access

1. Each Member State shall ensure that the provisions adopted under national law implementing Framework Decision 2008/977/JHA are also applicable to the access to EES by its national authorities in line with Article 1(2).
2. The monitoring of the lawfulness of the access to personal data by the Member States for the purposes listed in Article 1(2) of this Regulation, including their transmission to and from the EES, shall be carried out by the national supervisory authorities designated pursuant to Framework Decision 2008/977/JHA.
3. The processing of personal data by Europol shall be carried out in accordance with Decision 2009/371/JHA and shall be supervised by an independent external data protection supervisor. Articles 30, 31 and 32 of that Decision shall be applicable to the processing of personal data by Europol pursuant to this Regulation. The independent external data protection supervisor shall ensure that the rights of the third country national are not infringed.
4. Personal data accessed in the EES for the purposes laid down in Article 1(2) 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 national data protection authorities and the European Data Protection Supervisor to monitor the compliance of data processing with Union 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 for the purposes laid down in Article 1(2) 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:
 - (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 National Access Point to the Central System;
 - (f) 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;
 - (g) the data used for comparison;
 - (h) in accordance with national rules or with Decision 2009/371/JHA, 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 containing non-personal data may be used for the monitoring and evaluation referred to in Article 64. The competent national supervisory authorities 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 those 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 an alien’s stay in its territory in exceptional circumstances’.

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

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

(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 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] *."

* Regulation No XXX of the European Parliament and the Council establishing an Entry/Exit System (EES) to register entry and exit 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]

(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 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 (EC) No 767/2008³⁰ provide for it.

2. The interoperability requirement 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;

30

- (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 requirement 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 individual file of a visa holder in the EES in accordance with Articles 13, 14 and 16 of [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 at the external borders 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 at the external borders 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 cannot be verified against the EES, verify at the external borders 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.

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 external border crossing points

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 external border crossing points in accordance with Regulation (EU) 2016/399 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) or Article 21(4) of [Regulation establishing an Entry/Exit System (EES)], the competent border authority may launch a search in the VIS directly from the EES using the data referred to in point (a) of paragraph 1.

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 territorially valid for the border crossing, the competent border control authority 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 border control authority 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 border authority shall be given access to consult the 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 border authority 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) the technology is not available at the border crossing point for the use of live facial image and therefore the identity of the visa holder cannot be verified against the 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, for the first time after the creation of the individual file, that person intends to cross the external borders of a Member State in which this Regulation is applicable.

The border authorities 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 the individual file of a visa holder into the EES

1. Solely for the purpose of creating or updating the individual file of a visa holder in the EES in accordance with Article 13(2) and Articles 14 and 16 of [Regulation establishing an Entry/Exit System (EES)], the competent border authority 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(1)(d), (e) and (g) 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 10 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:

- (a) 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)];
- (b) for third country nationals exempt from the visa obligation who had their individual file created in the EES by a Member State in which this Regulation is not applicable, when, for the first time after the creation of the individual file, the person intends to cross the external borders of a Member State in which this Regulation is applicable.

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 border authority 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 border authority may launch a search in the VIS directly from the EES using the alphanumeric data foreseen under paragraph 2.

4. If the search with the data listed in paragraph 2 indicates that data on the person are recorded on the VIS, the competent border authority 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.

5. 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 border authority shall verify the fingerprints of the person against the fingerprints recorded in the VIS. The competent border control 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.

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 border authority may launch from the EES the identification referred to in Article 20 of this Regulation."

(8) In Article 20, 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 external border crossing points in accordance with Regulation (EU) 2016/399 or within the territory of the Member States as to whether the conditions for entry to, stay or residence on the territory of the Member States are fulfilled, shall have access to 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, eu-LISA and Frontex shall have access to consult the following data, solely for the purposes of reporting and statistics without allowing for individual identification:
 - (a) status information;
 - (b) nationality, gender and date 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 short stay visa, {or the touring 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) and the border crossing point at which entry was refused.
2. For the purpose of paragraph 1, eu-LISA shall establish, implement and host a central repository 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 improve the assessment of the risk of overstay, 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 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 the form of quarterly statistics for that year. The statistics shall contain a breakdown of data for each Member State.
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 and the National Uniform Interface 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 systems (space, implementation, electricity, cooling);
- (c) operation of national systems (operators and support contracts);
- (d) customisation of existing border control 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 and the costs for their connection to the National Uniform Interface shall be borne by each Member State.
4. Each Member State and Europol shall set up and maintain at their expense the technical infrastructure necessary to implement Article 5(2) 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 eu-LISA of the competent authorities referred to in Article 8 which have access to enter, amend, delete, consult or search data.
3. Member States shall notify the Commission 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 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. Commission shall make the information notified pursuant to paragraph 1 available to the Member States and the public by a constantly updated public website.

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).
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 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.

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.

Article 63
Training

eu-LISA shall perform tasks related to providing training on the technical use of the EES.

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. 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 an examination of results achieved against objectives and the impact on fundamental rights, and assessing the continuing validity of the underlying rationale, the application of the Regulation, the security of the EES and any implications on future operations, and shall make any necessary recommendations. The Commission shall transmit the evaluation report to the European Parliament and the Council.
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) - the exact purpose of the consultation (whether for identification or for entry/exit records) including the type of terrorist or serious criminal offence;
 - (b) - reasonable grounds given for the substantiated suspicion that the suspect, perpetrator or victim is covered by this Regulation;
 - (c) - the reasonable grounds given not to conduct 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 which have ended in successful identifications;
 - (f) - the need and use made of the exceptional case of urgency including those cases where that urgency was not accepted by the ex post verification carried out by the central access point.

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

Done at Brussels,

For the European Parliament
The President

For the Council
The President