



Council of the
European Union

Brussels, 22 March 2017
(OR. en)

7223/17

**Interinstitutional File:
2016/0357 (COD)**

LIMITE

**FRONT 120
VISA 97
DAPIX 85
DATAPROTECT 35
CODEC 369
COMIX 194**

NOTE

From: Presidency
To: Working Party on Frontiers/Mixed Committee
(EU-Iceland/Liechtenstein/Norway/Switzerland)

No. prev. doc.: 6930/17 FRONT102 VISA 85 DAPIX 72 DATAPROTECT 28 CODEC 312
COMIX 165

Subject: Proposal for a Regulation of the European Parliament and of the Council
establishing a European Travel Information and Authorisation System
(ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399,
(EU) 2016/794 and (EU) 2016/1624

Delegations will find in the annex to this note compromise text proposals submitted by the Presidency on the above-mentioned subject.

Those Presidency text proposals cover Articles 30 to 82 (except Articles 41 and 67a).

Changes are highlighted in **bold underline** and ~~strikethrough~~ in relation to ST 14082/16.

2016/0357 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624

[Recitals to be examined at a later stage]

[Presidency compromise proposals on Articles 1-29 are included in ST 6930/17]

CHAPTER VI

Issuing, refusal, annulment or revocation of a travel authorisation

Article 30

Issuing of a travel authorisation

1. Where the examination of an application pursuant to the procedures laid down in Chapters III, IV and V indicates that there are no factual indications or reasonable grounds to conclude that the presence of the person on the territory of the Member States poses an **security**, irregular migration, ~~security~~ or public health risk, a travel authorisation shall be issued by the ETIAS Central System or the ETIAS National Unit of the responsible Member State.
 - 1a. The ETIAS National Unit of the responsible Member State may attach a recommendation for a thorough second line check to the travel authorisation it issues. This recommendation shall only be visible to the border guards and it shall indicate the reason for such recommendation. The recommendation may be removed by the border guard once the second line check has been carried out.**
2. A travel authorisation shall be valid for [five] years or until the end of validity of the travel document registered during application, whichever comes first, and shall be valid for the territory of the Member States.
3. A travel authorisation shall not confer an automatic right of entry **or stay**.

Article 31
Refusal of a travel authorisation

1. A travel authorisation shall be refused if the applicant:
 - (a) presents a travel document which is reported as lost, stolen or invalidated;
 - (b) poses an irregular migration risk;
 - (c) poses a security risk;
 - (d) poses a public health risk;
 - (e) is a person for whom an alert has been issued in the SIS for the purpose of refusing entry;
 - (f) fails to reply to a request for additional information or documentation within the deadlines referred to in Article 23.

A travel authorisation shall also be refused if there are reasonable doubts as to the authenticity of the data, the reliability of the statements made by the applicant, the supporting documents provided by the applicant or the veracity of their contents.

2. Applicants who have been refused a travel authorisation shall have the right to appeal. Appeals shall be conducted in the Member State that has taken the decision on the application and in accordance with the national law of that Member State. The ETIAS National Unit of the responsible Member State shall provide applicants with information regarding the procedure to be followed in the event of an appeal.

Article 32
Notification on the issuing or refusal of a travel authorisation

1. Where a travel authorisation has been issued, the applicant shall immediately receive a notification via the e-mail service, including:
 - (a) a clear indication that the travel authorisation has been issued and the travel authorisation application number;
 - (b) the commencement and expiry dates of the validity period of the travel authorisation;
 - (c) ~~where applicable, a reminder of the calculation of the duration of authorised short stay (90 days in any 180-day period), and of the rights derived from an issued travel authorisation pursuant to Article 30(3),~~ **as well as a reminder of the entry conditions as set out in Article 6 of Regulation (EU) N°2016/399 and of the calculation of the duration of authorised short stay (90 days in any 180-day period);** and

- (d) a link to the ETIAS public website containing information on the possibility for the applicant to **request the revocation** ~~ke~~ **of the travel authorisation and the possibility for the travel authorisation to be revoked if the conditions for issuing it are no longer met.**
2. Where a travel authorisation has been refused, the applicant shall immediately receive a notification via the e-mail service including:
- (a) a clear indication that the travel authorisation has been refused and the travel authorisation application number;
- (b) a reference to the authority **ETIAS National Unit** that refused the travel authorisation and its location;
- (c) the ground(s) for refusal of the travel authorisation, as laid down in Article 31(1);
- (d) information on the procedure to be followed for an appeal.

Article 33

Data to be added to the application file following the decision to issue or refuse a travel authorisation

- 1.** Where a decision has been taken to issue ~~or refuse~~ a travel authorisation, the ETIAS Central System or, where the decision has been taken following manual processing as provided for in Chapter IV, ~~relevant~~, the ETIAS National Units of the responsible Member State shall add the following data to the application file:
- (a) status information indicating that the travel authorisation has been issued ~~or refused~~;
- (b) ~~a reference to the authority that issued or refused the travel authorisation and its location;~~
- (c) place and date of the decision to issue ~~or refuse~~ the travel authorisation;
- (d) the commencement and expiry dates of the validity period of the travel authorisation;
- ~~(e) the ground(s) for refusal of the travel authorisation as laid down in Article 31(1);~~
- (f) any alert attached to the travel authorisation recommending a thorough second line check, as laid down in Article 30(1a).**

2. Where a decision has been taken to refuse a travel authorisation, the ETIAS National Unit of the responsible Member State shall add the following data to the application file:

- (a) status information indicating that the travel authorisation has been refused;**
- (b) a reference to the ETIAS National Unit that refused the travel authorisation and its location;**
- (c) place and date of the decision to refuse the travel authorisation;**
- (d) the ground(s) for refusal of the travel authorisation as laid down in Article 31(1).**

Article 34

Annulment of a travel authorisation

1. A travel authorisation shall be annulled where it becomes evident that the conditions for issuing it were not met at the time it was issued. The travel authorisation shall be annulled on the basis of one or more of the grounds for refusal of the travel authorisation laid down in Article 31(1).
2. Where a Member State is in possession of evidence that the conditions for issuing a travel authorisation were not met at the time it was issued, the ETIAS National Unit of that Member State shall annul the travel authorisation.
3. A person whose travel authorisation has been annulled shall have the right to appeal. Appeals shall be conducted in the Member State that has taken the decision on the annulment in accordance with the national law of that Member State.

Article 35

Revocation of a travel authorisation

1. A travel authorisation shall be revoked where it becomes evident that the conditions for issuing it are no longer met. The travel authorisation shall be revoked on the basis of one or more of the grounds for refusal of the travel authorisation laid down in Article 31(1).
2. Where a Member State is in possession of evidence that the conditions for issuing the travel authorisation are no longer met, the ETIAS National Unit of that Member State shall revoke the travel authorisation.
3. Without prejudice to paragraph 2, where a new refusal of entry alert or a travel document as lost, stolen or invalidated is reported in the SIS, the SIS shall inform the ETIAS Central System. The ETIAS Central System shall verify whether this new alert corresponds to a valid travel authorisation. Where this is the case, the ETIAS Central System shall transfer the application file to the ETIAS National Unit of the Member State having created the alert which shall revoke the travel authorisation.

4. New elements introduced by ~~Europol~~ in the ETIAS watchlist shall be compared to the data of the application files in the ETIAS Central System. **The ETIAS Central System shall verify whether that new element corresponds to a valid travel authorisation.** Where **this is the case, the ETIAS Central System shall transfer the application file to the ETIAS National Unit of the Member State having entered the new element, or where Europol entered the new element, to** ~~the comparison results in a hit,~~ the ETIAS National Unit of the Member State of first entry as declared by the applicant in accordance with Article 15(2)(j). **That ETIAS National Unit** shall assess the security risk and, ~~it~~ shall revoke the travel authorisation **where it concludes that the conditions for granting it are no longer met.**
5. An applicant whose travel authorisation has been revoked shall have the right to appeal. Appeals shall be conducted in the Member State that has taken the decision on the revocation and in accordance with the national law of that Member State.
6. A travel authorisation may be revoked at the request of the applicant.

Article 36

Notification on the annulment or revocation of a travel authorisation

Where a travel authorisation has been annulled or revoked, the applicant shall immediately receive a notification via the e-mail service including:

- (a) a clear indication that the travel authorisation has been annulled or revoked and the travel authorisation application number;
- (b) a reference to the authority **ETIAS National Unit** that annulled or revoked the travel authorisation and its location;
- (c) the ground(s) for the annulment or revocation of the travel authorisation, as laid down in Article 31(1);
- (d) information on the procedure to be followed for an appeal.

Article 37

Data to be added to the application file following the annulment or revocation of a travel authorisation

1. Where a decision has been taken to annul or to revoke a travel authorisation, **the ETIAS National Unit that annulled or revoked** ~~the Member State responsible for the revocation or annulment~~ of the travel authorisation shall add the following data to the application file:
 - (a) status information indicating that the travel authorisation has been annulled or revoked;

- (b) a reference to the **ETIAS National Unit** authority that revoked or annulled the travel authorisation and its location;
 - (c) place and date of the decision **to annul or revoke the travel authorisation.**
2. The **ETIAS National Unit that annulled or revoked the travel authorisation shall also indicate in the** application file ~~shall also indicate~~ the ground(s) for annulment or revocation as laid down in Article 31(1) **or that the travel authorisation was revoked at the request of the applicant as referred to in Article 35(6).**

Article 38

Issuing of a travel authorisation with limited territorial validity on humanitarian grounds, for reasons of national interest or because of international obligations

1. A travel authorisation with limited territorial validity may be issued exceptionally, when the Member State concerned considers it necessary on humanitarian grounds, for reasons of national interest or because of international obligations notwithstanding the fact that, **following an application having been deemed admissible in accordance with Article 17,**
- (a) the manual assessment process pursuant to Article 22 is not yet completed or that
 - (b) a travel authorisation has been refused, annulled or revoked.

Where a travel authorisation with limited territorial validity has been issued in the circumstances referred to in point (a) of this paragraph, this shall not interrupt the manual assessment process on the application for a travel authorisation which does not have limited territorial validity.

2. For the purposes of paragraph 1, the applicant may **contact the ETIAS Central Unit indicating the Member State to which he or she intends to travel and that the purpose of his or her travel is based on** apply for a travel authorisation with limited territorial validity to the Member State to which he or she intends to travel. He or she and shall indicate the humanitarian grounds **or is linked to,** the reasons of national interest or the international obligations, **using a contact form as referred to in Article 14** in his or her application. **Where such contact form is received, the ETIAS Central Unit shall inform the ETIAS National Unit of the Member State to which the third country national intends to travel and shall record the information from the contact form in the application file.**¹

¹ An additional paragraph would be added to Article 14 as follows: "**6a. The public website and the mobile app for mobile devices shall enable the applicant to submit a contact form selecting from a predetermined list of options to indicate that the purpose of the intended stay relates to humanitarian grounds, reasons of national interest or international obligations.**"

3. The Member State to which the third country national intends to travel shall be the Member State responsible for deciding **decide** whether to issue or refuse a travel authorisation with limited territorial validity.
- 3a. The ETIAS National Unit of the Member State to which the third country national intends to travel may request additional information or documentation from the applicant. This request shall be notified through the email service referred to in Article 6(2)(f), to the contact email address recorded in the application file. The applicant shall provide the additional information or documentation directly to the ETIAS National Unit through the secure account service referred to in Article 6(2)(g).**
4. A travel authorisation with limited territorial validity shall be valid for the territory of the issuing Member State and for a maximum of 15 days **from the date on which the authorisation is issued. It may be exceptionally valid for the territory of more than one Member State, subject to the consent of each such Member State.**
5. Where a travel authorisation with **limited** territorial validity is issued, the following data shall be entered in the application file **by the ETIAS National Unit:**
- (a) status information indicating that the travel authorisation with limited territorial validity has been issued ~~or refused~~;
 - (b) the territory in which the travel authorisation holder is entitled to travel **and the duration of that travel authorisation;**
 - (c) the **ETIAS National Unit** authority of the Member State that issued the travel authorisation with **limited** territorial validity;
 - (d) a reference to the humanitarian grounds, the reasons of national interest or the international obligations.
- 6. Where a travel authorisation with limited territorial validity has been issued, the applicant shall immediately receive a notification via the e-mail service, including:**
- (a) **a clear indication that a travel authorisation with limited territorial validity has been issued and the travel authorisation application number;**
 - (b) **the commencement and expiry dates of the validity period of the travel authorisation with limited territorial validity, as well as the territory on which the holder of that authorisation is entitled to travel; and**
 - (c) **the rights derived from an issued travel authorisation pursuant to Article 30(3), as well as a reminder of the entry conditions as set out in Article 6 of Regulation (EU) N°2016/399 and of the calculation of the duration of authorised short stay (90 days in any 180-day period).**

Chapter VII

Use of ETIAS by carriers

Article 39

Access to data for verification by carriers²

1. In accordance with Article 26 of the Convention Implementing the Schengen Agreement carriers shall **send a query to** ~~consult~~ the ETIAS Central System in order to verify whether or not third country nationals subject to the travel authorisation requirement are in possession of a valid travel authorisation.
2. ~~As~~ Secure internet access to the carrier gateway, including the possibility to use mobile technical solutions, referred to in Article 6(2)(h) shall allow carriers to proceed with the **query consultation** referred to in paragraph 1 prior to the boarding of a passenger. For this purpose, the carrier shall **send the query to** ~~be permitted to consult~~ the ETIAS Central System using the data contained in the machine readable zone of the travel document.

The ETIAS Central System shall respond by indicating whether or not the person has a valid travel authorisation, **providing the carriers with an OK/NOT OK answer.** Carriers may store the information sent and the answer received.

3. An authentication scheme, reserved exclusively for carriers, shall be set up in order to allow access to the carrier gateway for the purposes of paragraph 2 to the duly authorised members of the carriers' staff. The authentication scheme shall be **adopted by the Commission by means of implementing acts in accordance with the examination procedure** referred to in **Article 79(2).**

Article 40

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

1. Where it is technically impossible to proceed with the ~~consultation~~ **query** referred to in Article 39(1), because of a failure of the ETIAS Information System or for other reasons beyond the carriers' control, the carriers shall be exempted of the obligation to verify the possession of a valid travel authorisation. In case of a failure of the ETIAS Information System, the ETIAS Central Unit shall notify the carriers. **In case of other reasons beyond the carriers' control, the carriers shall notify the ETIAS Central Unit.**

Penalties referred to in Article 26(2) of the Convention Implementing the Schengen Acquis shall not be imposed on carriers in the cases referred to in this paragraph.

2. The details of the fall-back procedures shall be laid down in an implementing act adopted in accordance with the examination procedure referred to in Article 79(2).

² A recital would be added as follows: **"In establishing the technical specifications for accessing the carrier gateway, the impact on passenger travel and carriers should be limited to the extent possible. For this purpose, the relevant integration with the Entry/Exit System should be considered."**

CHAPTER VIII

Use of ETIAS by border authorities at the external borders

*[Article 41
Access to data for verification at the external borders]*

[to be discussed later]

*Article 42
Fall-back procedures in case of technical impossibility to access data at the external borders or
failure of the ETIAS*

- 1.** Where it is technically impossible to proceed with the consultation referred to in Article 41(1), because of a failure of the ETIAS Information System, the Member State's authorities competent for carrying out checks at external border crossing points shall be notified by the ETIAS Central Unit.
2. Where it is technically impossible to perform the search referred to in Article 41(1) because of a failure of the national border infrastructure in a Member State, that Member State's competent authority shall notify eu-LISA, the ETIAS Central Unit and the Commission.
3. In both scenarios, the Member State's competent authorities for carrying out checks at external border crossing points shall follow their national contingency plans.

Chapter VIIIa

Use of ETIAS by immigration authorities

Article 42a³

Access to data by immigration authorities⁴

- 1. For the purpose of checking or verifying if the conditions for entry or stay on the territory of the Member States are fulfilled, the immigration authorities of the Member States shall have access to search the ETIAS Central System using the data contained in the machine readable zone of the travel document.**

- 2. The ETIAS Central System shall respond by indicating whether or not the person has a valid travel authorisation.**

In the case of minors, the immigration authorities shall also have access to the information relating to the traveller's parental authority or legal guardian referred to in Article 15(k).

³ A recital would be added as follows: "**Since the possession of a valid travel authorisation is a condition of entry and stay for certain categories of third country nationals, the immigration authorities of the Member States should be able to consult the ETIAS Central System to check the travel authorisation status of a traveller.**"

⁴ The definition, taken from the EES mandate, would read: 'immigration authorities' means the competent authorities assigned, in accordance with national law, to:

- (a) check within the territory of the Member States whether the conditions for entry to or of authorised stay in the territory of the Member States are fulfilled and/or
- (b) examine the conditions and take decisions related to the [...] residence of third country nationals on the territory of the Member States and where relevant provide advice in accordance with Regulation (EU) 377/2004 and/or;
- (c) facilitate the return of third country nationals to a third country of origin or transit.

CHAPTER IX

Procedure and conditions for access to the ETIAS Central System for law enforcement purposes

Article 43

Member States' designated ~~law enforcement~~ authorities

1. Member States shall designate the ~~law enforcement~~ authorities which are entitled to request consultation of data recorded in the ETIAS Central System in order to prevent, detect and investigate terrorist offences or other serious criminal offences.
2. At national level, each Member State shall keep a list of the **operational units** within the designated authorities that are authorised to request a consultation of data stored in the ETIAS Central System through the central access point(s).
3. **Each Member State shall designate a central access point which shall have access to the ETIAS Central System. The central access point shall ensure that the conditions to request access to the ETIAS Central System laid down in Article 45 are fulfilled.**

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

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

4. **Each Member State shall notify eu-LISA, the ETIAS Central Unit and the Commission of its designated authorities and central access point and may at any time amend or replace its notification.**
5. **Only duly empowered staff of the central access point(s) shall be authorised to access the ETIAS Central System in accordance with Articles 44 and 45.**

Article 44

Procedure for access to the ETIAS Central System for law enforcement purposes

1. The competent authorities **operational units referred to in article 43(2)** shall submit a reasoned electronic request for consultation of a specific set of data stored in the ETIAS Central System to the central access points referred to in Article ~~43(3) 8(2)(e-e)~~ **43(3)**. Where consultation of data referred to in Article 15(2)(i) and (4)(b) to (d) is sought, the reasoned electronic request shall include a justification of the necessity to consult those specific data.
2. ~~Each Member State shall ensure p~~**Prior to accessing ETIAS Central System, the central access point shall verify that according to its national law and procedural law a request for consultation undergoes an independent, efficient and timely verification** whether the conditions referred to in Article 45 are fulfilled, including whether any request for consultation of data referred to in Article 15(2)(i) and (4)(b) to (d) is justified.
3. If the conditions referred to in Article 45 are fulfilled, the central access point shall process the requests. The data stored in the ETIAS Central System accessed by the central access point shall be transmitted to the operational units referred to in Article 43(2) in such a way as to not compromise the security of the data.
4. ~~In an exceptional case of urgency, w~~**Where there is a need to immediately obtain personal data necessary for preventing a terrorist offence or an imminent danger associated with another the commission of a serious crime criminal offence** or for prosecuting its perpetrators, the central access point shall process the request immediately and without the independent verification provided in paragraph 2. An ex post independent verification shall take place without undue delay after the processing of the request, including whether an ~~exceptional~~ case of urgency actually existed.
5. Where an ex post ~~independent~~ verification determines that the consultation of and access to the data recorded in the ETIAS Central System were not justified, all the authorities that accessed and/or consulted such data shall erase the data originating from the ETIAS Central System and shall inform the central access point of the erasure.

Article 45

Conditions for access to data recorded in the ETIAS Central System by designated authorities of Member States

1. Designated authorities may request consultation of data stored in the ETIAS Central System if all the following conditions are met:
 - (a) the consultation is necessary for the purpose of the prevention, detection or investigation of a terrorist offences or another serious criminal offence;
 - (b) access for consultation is necessary in a specific case;

- (c) reasonable grounds exist to consider that the consultation of data stored in the ETIAS Central System 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 the category of third country nationals covered by this Regulation;
 - (d) prior consultation of ~~all relevant~~ national databases ~~and the Europol data~~ did not lead to the requested information.
2. Consultation of the ETIAS Central System shall be limited to searching with the following data recorded in the application file:
- (a) surname (family name); first name(s) (given names);
 - (b) other names (alias(es), artistic name(s), usual name(s));
 - (c) number of the travel document;
 - (d) home address;
 - (e) e-mail address; or phone number;
 - (f) IP address.
3. Consultation of the ETIAS Central System with the data listed under paragraph 2 may be combined with the following data in the application file to narrow down the search:
- (a) nationality or nationalities;
 - (b) sex;
 - (c) date of birth or age range.
4. Consultation of the ETIAS Central System shall, in the event of a hit with data recorded in an application file, give access to the data referred to in Article 15(2)(a) to (g) and (j) to (m) as recorded in that application file as well as to data entered in that application file in respect of the issuing, refusal, revocation or annulment of a travel authorisation in accordance with Articles 33 and 37. Access to the data referred to in Article 15(2)(i) and in (4) (b) to (d) as recorded in the application file shall only be given if consultation of that data was explicitly requested by the operating units in the reasoned electronic request submitted under Article 44(1) and approved by the independent verification. Consultation of the ETIAS Central System shall not give access to data concerning the education as referred to in Article 15(2)(h) or on whether or not the applicant may pose a public health risk as referred to in Article 15(4)(a).

Article 46

Procedure and conditions for access to data recorded in the ETIAS Central System by Europol

1. For the purposes of Article 1(2), Europol may request consultation of data stored in the ETIAS Central System and submit a reasoned electronic request for consultation of a specific set of data stored in the ETIAS Central System to the ETIAS Central Unit. **Where consultation of data referred to in Article 15(2)(i) and (4)(b) to (d) is sought, the reasoned electronic request shall include a justification of the necessity to consult those specific data.**
2. The reasoned request shall contain evidence that the following conditions are met:
 - (a) the consultation is necessary to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences falling under Europol's mandate;
 - (b) the consultation is necessary in a specific case;
 - (c) the consultation shall be limited to searching with data referred to in Article 45(2);
 - (d) 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;
 - (e) prior consultation of the database at Europol did not lead to the requested information.
3. Europol requests for consultation of data stored in the ETIAS Central System shall be subject to prior verification by the EDPS, where appropriate in accordance with the procedure of Article 44 of Regulation (EU) 2016/794, which shall examine in an efficient and timely manner whether the request fulfils all conditions of paragraph 2.
4. Consultation of the ETIAS Central System shall, in the event of a hit with data stored in an application file, give access to the data referred to in Article 15(2)(a) to (g) and (j) to (m) as well as to the data entered in the application file in respect to the issuing, refusal, revocation or annulment of a travel authorisation in accordance with Articles 33 and 37. Access to the data referred to in Article 15(2)(i) and in (4)(b) to (d) as stored in the application file shall only be given if consultation of that data was explicitly requested by Europol. **Consultation of the ETIAS Central System shall not give access to data concerning the education as referred to in Article 15(2)(h) or on whether or not the applicant may pose a public health risk as referred to in Article 15(4)(a).**
5. Where the EDPS has approved the request, the ETIAS Central Unit shall process the request for consultation of data stored in the ETIAS Central System **and shall transmit the data accessed to Europol in such a way as to not compromise the security of the data.**

CHAPTER X

Retention and amendment of the data

Article 47 *Data retention*

1. Each application file shall be stored in the ETIAS Central System for:
 - (a) the period of validity of the travel authorisation;
 - (b) [five years from the last entry record of the applicant stored in the EES; or]
 - (c) five years from the last decision to refuse, revoke or annul the travel authorisation in accordance with Articles 31, 34 and 35.
2. Upon expiry of its retention period the application file shall automatically be erased from the ETIAS Central System.

Article 48 *Amendment of data and advance data deletion*

1. The ETIAS Central Unit and the ETIAS National Units shall have the obligation to update the data stored in the ETIAS Central System and ensure that it is correct. The ETIAS Central Unit and the ETIAS National Units shall not have the right to modify data entered in the application form directly by the applicant pursuant to Article 15(2), **(3)** or (4).
2. Where the ETIAS Central Unit has evidence that data recorded in the ETIAS Central System by the ETIAS Central system are factually inaccurate or that data were processed in the ETIAS Central System in contravention of this Regulation, it shall check the data concerned and, if necessary, amend or erase them without delay from the ETIAS Central System.
3. Where the responsible Member State has evidence that data recorded in the ETIAS Central System are factually inaccurate or that data were processed in the ETIAS Central System in contravention of this Regulation, its ETIAS National Unit shall check the data concerned and, if necessary, amend or erase them without delay from the ETIAS Central System.
4. If a Member State different from the responsible Member State has evidence to suggest that data stored in the ETIAS Central System are factually inaccurate or that data were processed in the ETIAS Central System in contravention of this Regulation, it shall contact the ETIAS Central Unit or the ETIAS National Unit of the responsible Member State within a time limit of 14 days. The ETIAS Central Unit or the competent ETIAS National Unit shall check the accuracy of the data and the lawfulness of its processing within a time limit of one month and, if necessary, amend or erase the data from the ETIAS Central System without delay.

5. Where a third country national has acquired the nationality of a Member State or has fallen under the scope of Article 2(2)(a) to (e), the authorities of that Member State shall verify whether that person has a valid travel authorisation and, where relevant, shall delete the application file without delay from the ETIAS Central System. The authority responsible for deleting the application file shall be the:
- (a) the ETIAS National Unit of the Member State that issued the travel document as referred to in Article 2(2)(a);
 - (b) the ETIAS National Unit of the Member State the nationality of which he or she has acquired;
 - (c) the ETIAS National Unit of the Member State that issued the residence permit or card;
 - (d) the ETIAS National Unit of the Member State that issued the long-stay visa.
6. Where a third country national has fallen under the scope of Article 2(2)(f) to (h), he or she shall inform the competent authorities of the Member State he or she next enters of this change. That Member State shall contact the ETIAS Central Unit within a time limit of 14 days. The ETIAS Central Unit shall check the accuracy of the data within a time limit of one month and, if necessary erase the application file and the data contained within from the ETIAS Central System without delay. The individual shall have access to an effective judicial remedy to ensure the data is deleted.

CHAPTER XI

Data protection

Article 49 *Data Protection*

1. Regulation (EC) No 45/2001 shall apply to the processing of personal data by the European Border and Coast Guard Agency and eu-LISA.
2. [Regulation 2016/679] shall apply to the processing of personal data by the ETIAS National Units.
3. [Directive (EU) 2016/680] shall apply to the processing **of personal data** by Member States designated authorities for the purposes of Article 1(2).
4. Regulation (EU) 2016/794 shall apply to the processing of personal data by Europol pursuant to Articles ~~25~~ 24 and 46.

Article 50 *Data controller*

1. The European Border and Coast Guard Agency is to be considered a data controller in accordance with Article 2(~~ed~~) of Regulation (EC) No 45/2001 in relation to the processing of personal data in the ETIAS Central System.
2. In relation to the processing of personal data in the ETIAS Central System by a Member State, the ETIAS National Unit is to be considered as controller in accordance with Article 4(7) of [Regulation (EU) 2016/679] ~~which~~ **and** shall have central responsibility for the processing of personal data in **the** ETIAS Central System by this Member State.

Article 51 *Data processor*

1. eu-LISA is to be considered a data processor in accordance with Article 2(d) of Regulation (EC) No 45/2001 in relation to the processing of personal data in the ETIAS Information System.
2. eu-LISA shall ensure that the ETIAS Information System is operated in accordance with this Regulation.

Article 52
Security of processing

1. ~~Both~~ eu-LISA, **the ETIAS Central Unit** and the ETIAS National Units shall ensure the security of processing of personal data takes place pursuant to the application of this Regulation. eu-LISA, **the ETIAS Central Unit** and the ETIAS National Units shall cooperate on **data** security related tasks.
2. Without prejudice to Article 22 of Regulation (EC) No 45/2001, eu-LISA shall take the necessary measures to ensure the security of the Central System, the Communication Infrastructure between the Central System and the National Uniform Interface, the public website and mobile app, the email service, the secure account service, the carrier gateway, the web service and the software enabling to process the applications;
3. Without prejudice to Article 22 of Regulation (EC) No 45/2001 and Articles 32 and 34 of [Regulation (EU) 2016/679], ~~both~~ eu-LISA, **the ETIAS Central Unit** and the ETIAS National Units shall 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 the secure website that carries out operations in accordance with the purposes of the ETIAS;
 - (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 recorded personal data;
 - (e) prevent the unauthorised processing of data in the ETIAS Central System and any unauthorised modification or deletion of data processed in the ETIAS Central System;
 - (f) ensure that persons authorised to access the ETIAS Information System 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 ETIAS Information System create profiles describing the functions and responsibilities of persons who are authorised to access the data and make their profiles available to the supervisory authorities;
 - (h) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment;

- (i) ensure that it is possible to verify and establish what data has been processed in the ETIAS Information System, 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 ETIAS Central System 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.
4. 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 this Article.

Article 53
Self-monitoring

The European Border and Coast Guard Agency, Europol and Member States shall ensure that each authority entitled to access the ETIAS Information System takes the measures necessary to comply with this Regulation and cooperates, where necessary, with the supervisory authority.

Article 54
Right of information, access, correction and erasure

1. Without prejudice to the right of information in Articles 11 and 12 of Regulation (EC) 45/2001, applicants whose data are stored in the ETIAS Central System shall be informed, at the time their data are collected, on the procedures for exercising the rights under Articles 13, 14, 15 and 16 of Regulation (EC) 45/2001 and on the contact details of the data protection officer of the European Border and Coast Guard Agency, of the European Data Protection Supervisor and of the national supervisory authority of the responsible Member State.
2. In order to exercise their rights under Articles 13, 14, 15 and 16 of Regulation (EC) 45/2001 and Article 15, 16, 17 and 18 of [Regulation (EU) 2016/679] any applicant shall have the right to address him or herself to the ETIAS Central Unit or to the ETIAS National Unit responsible for the application, who shall examine and reply to the request.

Where following an examination it is found that the data stored in the ETIAS Central System are factually inaccurate or have been recorded unlawfully, the ETIAS Central Unit or the ETIAS National Unit of the responsible Member State for the application shall correct or delete these data in the ETIAS Central System.

Where a travel authorisation is amended by the ETIAS Central Unit or an ETIAS National Unit during its validity period, the ETIAS Central System shall carry out the automated processing laid down in Article 18 to determine whether the amended application file triggers a hit pursuant to Article 18(2) to (5). Where the automated processing does not report any hit, the ETIAS Central System shall issue an amended travel authorisation with the same validity of the original and notify the applicant. Where the automated processing reports one or several hit(s), the ETIAS National Unit of the Member State **responsible of first entry as declared by the applicant in accordance with Article 15(2)(j)** shall assess the **security**, irregular migration, ~~security~~ or public health risk and shall decide whether to issue an amended travel authorisation or, where it concludes that the conditions for granting the travel authorisation are no longer met, revoke the travel authorisation.

3. Where the ETIAS Central Unit or the ETIAS National Unit of the Member State responsible for the application **does** not agree that data stored in the ETIAS Central System are factually inaccurate or have been recorded unlawfully, the ETIAS Central Unit or the ETIAS National Unit of the Member State responsible for the application 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.
4. This decision shall also provide the person concerned with information explaining the possibility to challenge the decision taken in respect of the request referred **to** in paragraph 2 and where relevant, information on how to bring an action or a complaint before the competent authorities or courts and any assistance, including from the competent national supervisory authorities.
5. Any request made pursuant to paragraph 2 shall contain the necessary information to identify the person concerned. That information shall be used exclusively to enable the exercise of the rights referred to in paragraph 2 and shall be erased immediately afterwards.
6. The ETIAS Central Unit or the ETIAS National Unit of the Member State responsible for the application shall keep a record in the form of a written document that a request referred to in paragraph 2 was made and how it was addressed and shall make that document available to competent data protection national supervisory authorities without delay.

Article 55

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

1. Personal data stored in the ETIAS Central System shall not be transferred or made available to a third country, to an international organisation or any private party with the exception of transfers to Interpol for the purpose of carrying out the automated processing referred to in Article 18(2)(b) and (m). Transfers of personal data to Interpol are subject to the provisions of Article 9 of Regulation 45/2001.

2. Personal data accessed from the ETIAS Central System by a Member State or by **Europol** for the purposes referred to in Article 1(2) 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.

Article 56

Supervision by the national supervisory authority

1. The supervisory authority or authorities designated pursuant to Article 51 of [Regulation 2016/679] shall ensure that an audit of the data processing operations by the ETIAS National Units is carried out in accordance with relevant international auditing standards at least every four years.
2. Member States shall ensure that their supervisory authority has sufficient resources to fulfil the tasks entrusted to it under this Regulation.
3. 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 their responsibilities as laid down in this Regulation. Each Member State shall grant the supervisory authorities access to their records and allow them access at all times to all their ETIAS related premises.

Article 57

Supervision by the European Data Protection Supervisor

The European Data Protection Supervisor shall ensure that an audit of eu-LISA's and the ETIAS Central Unit 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 Member States. eu-LISA and the European Border and Coast Guard Agency shall be given an opportunity to make comments before their reports are adopted.

Article 58

Cooperation between national supervisory authorities and the European Data Protection Supervisor

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

2. In cases referred to under paragraph 1, the European Data Protection Supervisor and the national supervisory authorities competent for data protection supervision may, each acting within the scope of their respective competences, exchange relevant information, assist each other in carrying out audits and inspections, examine difficulties over the interpretation or application of this Regulation, study problems related to 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 as part of the Board established by [Regulation (EU) 2016/679]. The costs of these meetings shall be borne by the Board established by [Regulation (EU) 2016/679]. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary.
4. A joint report of activities shall be sent to the European Parliament, the Council, the Commission, the European Border and Coast Guard Agency 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 59
Keeping of records

1. eu-LISA shall keep records of all data processing operations performed within the ETIAS Information System. Those records shall show the purpose of the access, the date and time of each operation, the data used for the automated processing of the applications, the hits found while carrying out the automated processing laid down in Article 18, the data used for verification of the identity regarding the ETIAS Central System or other information systems and databases, the results of the verification process referred to in Article 20 and the staff having performed it.
2. The ETIAS Central Unit shall keep records of the staff duly authorised to perform the identity verifications.
3. The ETIAS National Unit of the responsible Member State shall keep records in the ETIAS Information System of all data processing operations while carrying out the assessment referred to in Article 22. Those records shall show the date and time of each operation, the data used for interrogation of other information systems and databases, the data linked to the hit received, the staff having performed the risk assessment and the justification behind the decision to issue, refuse, revoke or annul a travel authorisation.

In addition, the ETIAS National Unit of the responsible Member State shall keep records of the staff duly authorised to enter or retrieve the data.

4. eu-LISA shall keep records of all data processing operations within the ETIAS Information System concerning the access by carriers to the gateway, ~~and the access by~~ **border guards** ~~the competent authorities for carrying out checks at external border crossing points~~ **and access by immigration authorities** referred to in Article 39, ~~and 41~~ **and 42**. Those records shall show the date and time of each operation, the data used for launching the search, the data transmitted by the ETIAS Central System and the name of the authorised staff of the carriers, **border guards and immigration authorities** ~~or of the competent authority~~ entering and retrieving the data.

In addition, the carriers and the competent authorities shall keep records of the staff duly authorised to enter and retrieve the data.

5. Such records may be used only for the data protection monitoring of the admissibility of data processing as well as to ensure data security and integrity. Those records shall be protected by appropriate measures against unauthorised access and deleted one year after the retention period referred to in Article 47 has expired, if they are not required for monitoring procedures which have already begun.

eu-LISA and the ETIAS National Units shall make available those records to the European Data Protection Supervisor and, respectively, to the competent supervisory authorities on request.

Article 60

Keeping of records, logs and documentation for requests for consultation of data for law enforcement access

1. eu-LISA shall keep records of all data processing operations performed within the ETIAS Central System concerning the access by central access points for the purposes of Article 1(2). Those records shall show the date and time of each operation, the data used for launching the search, the data transmitted by the ETIAS Central System and the name of the authorised staff of the central access points entering and retrieving the data.
2. In addition, each Member State and Europol shall keep records of all data processing operations within the ETIAS Central System resulting from requests to consult ~~of~~ or access to data stored in the ETIAS Central System for the purposes laid down in Article 1(2). The records shall include logs and documentation of all data processing operations.
3. The records shall show:
 - (a) the exact purpose of the request for consultation of or access to data stored in the ETIAS Central System, including the terrorist offence or other serious criminal offence concerned and, for Europol, the exact purpose of the request for consultation;
 - (b) the decision taken with regard to the admissibility of the request;

- (c) the national file reference;
- (d) the date and exact time of the request for access made by the ~~National~~ **Central** Access Point to the ETIAS Central System;
- (e) where applicable, the use of the urgent procedure referred to in Article 44(4) and the ~~decision taken with regard to~~ **outcome of** the ex-post verification;
- (f) which of **the** data or set of data referred to in Article 45(2) and (3) have been used for consultation;
- (g) in accordance with national rules or with Regulation (EU) 2016/794, the identifying mark of the official who carried out the search and of the official who ordered the search or supply.

4. The records referred to in paragraphs 1 and 2 shall be used only to check the admissibility of the request, monitor the lawfulness of data processing and to ensure data integrity and security. Only records containing non-personal data may be used for the monitoring and evaluation referred to in Article 81. The European Data Protection Supervisor and the competent supervisory authorities responsible for monitoring the lawfulness of the data processing and data integrity and security shall have access to those records at their request for the purpose of fulfilling their duties. The authority responsible for checking the admissibility of the request shall also have access to those records for this purpose. Other than for such purposes, personal data, as well as the records of the consultation requests of data stored in the ETIAS Central System 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.

CHAPTER XII

Public awareness

Article 61 *Information to the general public*

The ETIAS Central Unit shall provide the general public with all relevant information in relation to the application for a travel authorisation, in particular:

- (a) the criteria, conditions and procedures for applying for a travel authorisation;
- (b) information concerning the website and the mobile application for a ~~web~~ **mobile devices** where the application can be launched;
- (c) the deadlines for deciding on an application provided for in Article 27;
- (d) that decisions on applications must be notified to the applicant, that such decisions must state, where relevant, the ~~reasons~~ **grounds** for refusal on which they are based and that applicants whose applications are refused have a right to appeal, with information regarding the procedure to be followed in the event of an appeal, including the competent authority, as well as the time limit for lodging an appeal;
- (e) that mere possession of a travel authorisation does not confer an automatic right of entry and that the holders of a travel authorisation are requested to present proof that they fulfil the entry conditions at the external border, as provided for in Article 6 of Regulation (EU) 2016/399.

Article 62 *Information campaign*

The Commission shall, in cooperation with the ETIAS Central Unit, and the Member States, accompany the start of the ETIAS operation with an information campaign, to inform third country nationals falling within the scope of this Regulation of ~~their travel authorisation~~ **of the** requirement **for them** to be in possession of a valid travel authorisation for crossing the external borders.

CHAPTER XIII

Responsibilities

Article 63

Responsibilities of eu-LISA during the designing and development phase

1. The ETIAS Information System shall be hosted by eu-LISA in its technical sites and shall provide the functionalities laid down in this Regulation in accordance with the conditions of security, availability, quality and speed pursuant to paragraph 3.
2. The infrastructures supporting the public website, the mobile app and the carrier gateway shall be hosted in eu-LISA' sites or in Commission sites. These infrastructures shall be geographically distributed to provide the functionalities laid down in this Regulation in accordance with the conditions of security, availability, quality and speed laid down in **Article 64(1) paragraph 3**.
3. eu-LISA shall be responsible for the development of the ETIAS Information System, for any development required for establishing interoperability between the ETIAS Central System and the information systems referred to in Article 10.

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 **National** Uniform Interfaces, 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 [EES], SIS, [Eurodac], [ECRIS] or VIS deriving from the establishment of interoperability with the ETIAS.

eu-LISA shall develop and implement the Central System, the National Uniform Interfaces, 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 15(2) and (4), Article 16(4), Article 28(5), Article 39(3), Article 40(2) and Article 72(1) and (4).

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

4. 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 six members appointed by eu-LISA's Management Board from among its members or its alternates, the Chair of the ETIAS-EES Advisory Group referred to in Article 80, a member representing eu-LISA appointed by its Executive Director, a member representing the European Border and Coast Guard Agency appointed by its Executive Director and one member appointed by the Commission. The members appointed by eu-LISA's Management Board shall be elected only from those Member States which are fully bound under Union law by the legislative instruments governing the development, establishment operation and use of all the large-scale IT systems managed by eu-LISA and which will participate in the ETIAS. The Programme Management Board will meet once a month. It shall ensure the adequate management of the design and development phase of the ETIAS. 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.
5. 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 a~~ Member State **which is 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.

The EES-ETIAS Advisory Group referred to in Article 80 shall meet regularly until the start of operations of the ETIAS. 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.

Article 64

Responsibilities of eu-LISA following the entry into operations of the ETIAS

1. Following the entry into operations of the ETIAS, eu-LISA shall be responsible for the technical management of the 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 technical management of the Communication Infrastructure between the Central system and the National Uniform Interfaces as well as for the public website, the mobile app for mobile devices, the email service, the secure account service, the carrier gateway, the web service and the software to process the applications, as referred to in Article 6.

Technical management of the ETIAS shall consist of all the tasks necessary to keep the ETIAS Information System 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 technical quality, in particular as regards the response time for interrogation of the central database in accordance with the technical specifications.

2. 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 data stored in the ETIAS Central System. This obligation shall also apply after such staff leave office or employment or after the termination of their activities.
3. eu-LISA shall also perform tasks related to providing training on the technical use of the ETIAS Information System.

Article 65

Responsibilities of the European Coast and Border Guard Agency

1. The European Coast and Border Guard Agency shall be responsible for:
 - (a) the setting up and operation of the ETIAS Central Unit;
 - (b) the automated processing of applications;
 - (c) the screening rules.
2. Before being authorised to process data recorded in the ETIAS Central System, the staff of the ETIAS Central Unit having a right to access the ETIAS Central System shall be given appropriate training about data security and data protection rules, in particular on relevant fundamental rights.

Article 66
Responsibilities of Member States

1. Each Member State shall be responsible for:
 - (a) the connection to the National Uniform Interface;
 - (b) the organisation, management, operation and maintenance of the ETIAS National Units for the examination of and decision on **applications for** travel authorisations' ~~applications **where** rejected during the automated processing~~ **reported a hit** of applications;
 - (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 ETIAS Information System in accordance with this Regulation and to establish and regularly update a list of such staff and their profiles;
 - (e) the set up and operation of the ETIAS National Units.
2. Each Member State shall use automated processes for querying the ETIAS Central System at the external border.
3. Before being authorised to process data recorded in the ETIAS Central System, the staff of the ETIAS National Units having a right to access the ETIAS Information System shall be given appropriate training about data security and data protection rules, in particular on relevant fundamental rights.

Article 67
Responsibilities of Europol

1. Europol shall ensure processing of the queries referred to in Article 18(2)(j) and (4) and accordingly adapting its information system.
2. Europol shall be responsible for the establishment of the ETIAS watchlist pursuant to Article 29.
3. Europol shall be responsible for providing an opinion following a consultation request pursuant to Article ~~25~~ 26.

CHAPTER XIV

Amendments to other Union instruments

[Article 67a

Amendments to Regulation (EU) No 1077/2011

[to be discussed later]

Article 68

Amendments to Regulation (EU) 515/2014

Regulation (EU) 515/2014 is amended as follows:

In Article 6, the following paragraph 3bis is inserted:

“3bis. During the development phase Member States shall receive an additional allocation of 96,5 million EUR to their basic allocation and shall entirely devote this funding to ETIAS to ensure its quick and effective development in accordance with the implementation of the ETIAS Central System, as foreseen in [Regulation establishing a European Travel Information and Authorisation System (ETIAS)].”

Article 69

Amendments to Regulation (EU) 2016/399

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

1. Article 6 is amended as follows:

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

"(b) they are in a possession of a valid visa if required pursuant to Council Regulation (EC) No 539/2001 or of a valid travel authorisation if required pursuant to [Regulation establishing a European Travel Information and Authorisation system], except where they hold a valid residence permit or a valid long stay visa;"

2. In Article 8, paragraph 3 is amended as follows:

(a) in point (a), subpoint (i) is replaced by the following:

"(i) verification that the third-country national is in possession of a document which is valid for crossing the border and which has not expired, and that the document is accompanied, where applicable, by the requisite visa, travel authorisation or residence permit."

(b) the following point (bb) is inserted:

"(bb) if the third country national holds a travel authorisation referred to in Article 6(1)(b) the thorough checks on entry shall also comprise the verification of the authenticity, validity and status of the travel authorisation and, if applicable, of the identity of the holder of the travel authorisation, by querying the ETIAS in accordance with Article 41 of [Regulation establishing a European Travel Information and Authorisation System (ETIAS)]"

3. In Annex V part B in the reasons for refusal, point (C) is replaced by the following:

"(C) has no valid visa, travel authorisation or residence permit."

*Article 70
Amendments to Regulation (EU) 2016/794*

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

1. (1) In Article 4 paragraph 1, the following point (n) is added:

"(n) ~~establish, manage and update~~ **host** the ETIAS watchlist referred to in Article 29 of [Regulation establishing a European Travel Information and Authorisation System (ETIAS)] in accordance with Article 18(2)(a)."

2. Article 21 is amended as follows:

(a) the title is replaced by the following:

"Article 21

Access by Eurojust, OLAF and, **only for purposes of ETIAS, by** the European Borders and Coast Guard Agency ~~only for purposes of ETIAS~~ to information stored by Europol"

(b) the following paragraph 1a is inserted:

"Europol shall take all appropriate measures to enable the European Borders and Coast Guard Agency, within its mandate and for the purposes of Regulation [Regulation establishing a European Travel Information and Authorisation System (ETIAS)], to have indirect access on the basis of a hit/no hit system to information provided for the purposes of point (a) of Article 18(2) without prejudice to any restrictions indicated by the Member State, Union body, third country or international organisation providing the information in question, in accordance with Article 19(2).

In the case of a hit, Europol shall initiate the procedure by which the information that generated the hit may be shared, in accordance with the decision of the provider of the information to Europol, and only to the extent that the data generating the hit are necessary for the performance of the European Borders and Coast Guard Agency tasks related to ETIAS.

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

Article 71
Amendments to Regulation (EU) 2016/1624

Regulation (EU) 2016/1624 is amended as follows:

1. In Article 8 paragraph 1, the following point (qq) is inserted:

"(qq) fulfil the tasks and obligations entrusted to the European ~~Coast~~ **Border** and **Coast** ~~Border~~ Guard Agency referred to in [Regulation establishing a European Travel Information and Authorisation System (ETIAS)] and ensure the **setting up and operation** ~~creation and management~~ of the ETIAS Central Unit in accordance with Article 7 of [Regulation establishing a European Travel Information and Authorisation System (ETIAS)]."

2. In Chapter II, the following Section 5 is added:

"Section 5
The ETIAS

Article 33a
Creation of the ETIAS Central Unit

1. An ETIAS Central Unit is hereby established.
2. The European Border and Coast Guard Agency shall ensure the creation and management of an ETIAS Central Unit pursuant to Article 7 of [Regulation establishing a European Travel Information and Authorisation System (ETIAS)]."

CHAPTER XV

Final provisions

Article 72

Transitional period and transitional measures

1. For a period of six months from the date ETIAS commences operations, the utilisation of ETIAS shall be optional and the requirement to be in possession of a valid travel authorisation shall not apply. The Commission may adopt a delegated act in accordance with Article 78 to extend that period for a maximum of a further six months.
2. During ~~this six month~~ **the period referred to in paragraph 1**, the border guards shall inform third country nationals subject to the travel authorisation requirement crossing the external borders of the requirement to have a valid travel authorisation from the expiry of the six month period. For this purpose, the border guards shall distribute a common leaflet to this category of travellers.
3. The common leaflet shall be drawn up and set up by the Commission. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 79(2) and shall contain at a minimum the information referred to in Article 61. The leaflet shall be clear and simple and available in a language version the person concerned understands or is reasonably assumed to understand.
4. A period of grace ~~of six months may~~ **shall apply** ~~be established~~ following the end of the period defined in paragraph 1. During such period, the requirement to be in possession of a valid travel authorisation shall apply. During the period of grace the border guards shall exceptionally allow third country nationals subject to the travel authorisation requirement who are not in possession of a travel authorisation to cross the external borders where they fulfil all the remaining conditions of Article 6(1) of Regulation (EU) 2016/399 provided that they cross the external borders of the Member States for the first time since the end of the period referred to in paragraph 1 ~~of this Article~~. Border guards shall **inform** ~~notify~~ the third country nationals subject to the travel authorisation requirement of the requirement to be in possession of a valid travel authorisation in accordance with Article 6(1)(b) of Regulation (EU) 2016/399. **The Commission may adopt a delegated act in accordance with Article 78 to extend that period for a maximum of a further six months.**
5. ~~The Commission shall adopt delegated acts on the duration of the period of grace referred to in paragraph 4. That period shall not exceed twelve months from the end of the period defined in paragraph 1.~~

Article 73
Use of data for reporting and statistics

1. The duly authorised staff of the competent authorities of Member States, the Commission, eu-LISA and the ETIAS Central Unit 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) nationalities, sex and **age** ~~date of birth~~ of the applicant;
 - (c) the country of residence;
 - (d) education;
 - (e) current occupation (~~domain~~), job title;
 - (f) the type of the travel document and three letter code of the issuing country;
 - (g) the type of travel authorisation and, for travel authorisation with limited territorial validity, a reference to the Member State(s) issuing the travel authorisation with limited territorial validity;
 - (h) the validity period of the travel authorisation;
 - (i) the reasons for refusing, revoking or annulling a travel authorisation.

2. For the purpose of paragraph 1, eu-LISA shall establish, implement and host a central repository 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 to improve the assessment of the **security**, irregular migration, ~~security~~ and **public** health risks, to enhance the efficiency of border checks, to help the ETIAS Central Unit **and the ETIAS National Units** processing the travel authorisation 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-**ng** 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 79(2).

3. The procedures put in place by eu-LISA to monitor the development and the functioning of the ETIAS Information System referred to in Article 81(1) shall include the possibility to produce regular statistics for ensuring that monitoring.
4. Every quarter, eu-LISA shall publish statistics on the ETIAS Information System showing in particular the number and nationality of applicants whose travel authorisation was refused, including the grounds for refusal, and of third country nationals whose travel authorisation ~~were~~ **was** annulled or revoked.
5. At the end of each year, statistical data shall be compiled in the form of quarterly statistics for that year.
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 74
Costs

The costs incurred in connection with the development of the ETIAS Information System, the integration of the existing national border infrastructure and the connection to the National Uniform Interface as well as ~~the~~ **by hosting of** the National Uniform Interface ~~and~~; the set-up of the ETIAS Central and National Units ~~and the operation of the ETIAS~~ shall be borne by the general budget of the Union.

The costs of the operation of the ETIAS shall also be borne by the general budget of the Union. This shall include the operation and maintenance costs of the ETIAS Information System, including of the National Uniform Interface; the operation costs of the ETIAS Central Unit and the costs of staff and ICT of the ETIAS National Units.

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 checks;
- (e) design, development, implementation, operation and maintenance of national communication networks;

Article 75
Revenues

The revenues generated by the ETIAS shall constitute external assigned revenue in accordance with Article 21(4) of Regulation (EU, EURATOM) No 966/2012.

Article 76
Notifications

1. Member States shall notify the Commission of the authority which is to be considered as controller referred to in Article 50.
2. The ETIAS Central Unit and the Member States shall notify eu-LISA of the ~~competent~~ authorities referred to in Article 11 which have access to the ETIAS Information System.

A consolidated list of those authorities shall be published in the *Official Journal of the European Union* within a period of three months from the date on which ETIAS commenced operations in accordance with Article 77. Where there are amendments to the list, eu-LISA shall publish an updated consolidated list once a year.

3. Member States shall notify the Commission of their designated authorities **and central access points** referred to in Article 43 and shall notify without delay any amendments thereto.
4. eu-LISA shall notify the Commission of the successful completion of the test referred to in Article 77(1)(b).
5. The 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 77
Start of operations

1. The Commission shall determine the date from which the ETIAS is to start operations, after the following conditions are met:
 - (a) the measures referred to in Article 15(3) and (4), Article 16(4), Article 28(3), Article 39(3), Article 40(2), Article 72(1) and (5) and Article 73(2) have been adopted;
 - (b) eu-LISA has declared the successful completion of a comprehensive test of the ETIAS;

- (c) eu-LISA and the ETIAS Central Unit have validated the technical and legal arrangements to collect and transmit the data referred to in Article 15 to the ETIAS Central System and have notified them to the Commission;
 - (d) the Member States and the ETIAS Central Unit have notified to the Commission the data concerning the various authorities referred to in Article 76(1) and (3).
2. The test of the ETIAS referred to in point (b) of paragraph 1 shall be conducted by eu-LISA in cooperation with the Member States and the ETIAS Central Unit.
 3. 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.
 4. The Commission decision referred to in paragraph 1 shall be published in the *Official Journal of the European Union*.
 5. The Member States and the ETIAS Central Unit shall start using the ETIAS from the date determined by the Commission in accordance with paragraph 1.

Article 78
Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The power to adopt delegated acts referred to in Article 15(3), **(5)** and **(46)**, Article 16(4), Article 28(3) and Article 72(1) and (5) shall be conferred on the Commission for an indeterminate period of time⁵ from [*the date of entry into force of this Regulation*].
3. The delegation of power referred to in Article 15(3), **(5)** and **(46)**, Article 16(4), Article 28(3) and Article 72(1) and (5) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

3a. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016.

⁵ The delegation of power proposed by the Commission in Article 78(2) is for an indeterminate period of time, which corresponds to option 1 of the duration standard clauses set out in the appendix of "Better Law-Making" Interinstitutional Agreement (see page 13):

<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:123:FULL&from=EN>

However, two other options are possible :

- delegation for a determined period with a tacit extension for periods of an identical duration and a Commission's report in respect of the delegation of power not later than nine months before the end of original period (option 2) and

- delegation for a determined period without a tacit extension (option 3).

The Council often opts for a delegation of five years with a tacit extension (option 2).

The Presidency wishes to have the delegations' views on the preferred option.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
5. A delegated act adopted pursuant to Article 15(~~32~~), (~~5~~) and (~~46~~), Article 16(4), Article 28(3) and Article 72(1) and (~~54~~) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of [two months] of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by [two months] at the initiative of the European Parliament or of the Council.

Article 79
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. **Where the Committee delivers no opinion, the Commission shall not adopt the draft implementing act and the third subparagraph of Article 5(4) of Regulation (EU) No 182/2011 shall apply**

Article 80
Advisory group

The eu-LISA EES Advisory Group responsibilities shall be extended to ETIAS. This EES-ETIAS Advisory Group shall provide eu-LISA with the expertise related to the ETIAS in particular in the context of the preparation of its annual work programme and its annual activity report.

Article 81
Monitoring and evaluation

1. eu-LISA shall ensure that procedures are in place to monitor the development of the ETIAS Information System in light of objectives relating to planning and costs and to monitor the functioning of the ETIAS 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 ETIAS Information System, 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 **National** Uniform Interfaces and the Communication Infrastructure between the Central System and the **National** 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 ETIAS Information System.
4. ~~For the first time~~ Two years after the start of operations of the ETIAS 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 ETIAS Information System, including the security thereof.
5. Three years after the start of operations of the ETIAS and every four years thereafter, the Commission shall evaluate ETIAS and shall make any necessary recommendations to the European Parliament and the Council. This evaluation shall include:
 - (a) the results achieved by the ETIAS having regard to its objectives, mandate and tasks;
 - (b) the impact, effectiveness and efficiency of the ETIAS performance and its working practices in relation to its objectives, mandate and tasks;
 - (c) the rules of the automated application processor used for the purpose of risk assessment;
 - (d) the possible need to modify the mandate of the ETIAS Central Unit;
 - (e) the financial implications of any such modification;
 - (f) the impact on fundamental rights.

The Commission shall transmit the evaluation report to the European Parliament and the Council.

6. The Member States and Europol shall provide eu-LISA, the ETIAS Central Unit and the Commission with the information necessary to draft the reports referred to in paragraphs 4 and 5. This information shall not jeopardise working methods or include information that reveals sources, staff members or investigations of the designated authorities.
7. eu-LISA and the ETIAS Central Unit shall provide the Commission with the information necessary to produce the 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 data stored in the ETIAS Central System for law enforcement purposes containing information and statistics on:
 - (a) the exact purpose of the consultation 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 number of requests for access to the ETIAS Central System for law enforcement purposes;
- (d) the number and type of cases which have ended in **positive hits** ~~successful identifications~~;
- (e) the need and use made of the ~~exceptional case of~~ urgency **procedure** 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 82
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
