



Council of the  
European Union

Brussels, 29 May 2017  
(OR. en)

---

---

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

---

---

**9580/1/17  
REV 1**

**LIMITE**

**FRONT 240  
VISA 197  
DAPIX 205  
DATAPROTECT 104  
CODEC 904  
COMIX 378**

**NOTE**

---

<b>From:</b>	Presidency
<b>To:</b>	Permanent Representatives Committee/Mixed Committee
<b>Subject:</b>	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

---

**INTRODUCTION**

On 16 November 2016, the Commission adopted the above-mentioned proposal for a Regulation. This proposal establishes a European Travel Information and Authorisation System (ETIAS) allowing to gather information on visa exempt third country nationals in advance of their arrival at the EU external borders (land, air, and sea). The travel authorisation would only constitute an authorisation to travel to the Member States, but not a right of entry, as the decision to let a traveller enter the EU territory would still be taken by a border guard at the border-crossing point. The ETIAS proposal has been designed as an important building-block of the EU visa liberalisation policy. It aims at determining whether the presence of visa exempt travellers would pose a security, illegal immigration, or public health risk.

The Commission proposal was not accompanied by an impact assessment, but a feasibility study requested by the Commission was carried out from June until October 2016.

On 6 March 2017, the European Data Protection Supervisor submitted Opinion 3/2017 on the proposal (ST 7136/17). On 12 April 2017, the Article 29 Data Protection Working Party submitted a letter on the proposal (ST 8231/17).

The European Parliament is in the process of establishing its position on the proposal. Kinga GAL (EPP, HU) has been appointed rapporteur. The shadow rapporteurs are the following: Sylvie GUILLAUME (S&D, FR), Helga STEVENS (ECR, BE), Gérard DEPREZ (ALDE, BE), Marie-Christine VERGIAT (GUE/NGL, FR), Jan Philipp ALBRECHT (Verts/ALE, DE) and Lorenzo FONTANA (ENF, IT).

#### **PRESIDENCY COMPROMISE TEXT**

Three outstanding issues were specifically discussed at the meeting of the Permanent Representatives Committee/Mixed Committee on 24 May 2017, as outlined in ST 9349/17 and ST 9349/17 ADD1.

The Presidency proposal to require all third country nationals to hold a valid travel authorisation in case of airport transit (unless they require an airport transit visa or they are in possession of a valid visa) could be supported by a majority of delegations. Considering the security and practical reasons behind the Presidency compromise text, the Council Legal Service confirmed that this approach would be in line with the principle of proportionality. Article 81(5)(b) has been amended to specify that, when evaluating the ETIAS, the Commission should also evaluate the impact of the travel authorisation requirement for the purposes of airport transit, taking into account the objectives of the ETIAS as well as the economic impact of this requirement.

With regard to the possible inclusion of the purpose, means of subsistence and duration of the first intended stay among the fields to be filled in by the applicant, following the intervention by the Council Legal Service confirming that including this set of data would most probably violate the principle of proportionality, a very broad majority of delegations could support the Presidency text (i.e. not to include this set of data in the text).

As regards the nature of the assigned revenues (internal vs. external) emanating from the ETIAS fees, there was also a majority of Member States that could support the Presidency text which provides that the revenues generated by ETIAS constitute internal assigned revenues in accordance with Article 21(4) of the Financial Regulation. However, a number of scrutiny reservations were also entered. The Council Legal Service confirmed that the text was legally sound and that the reference to Article 21(4) of the Financial Regulation was sufficient.

The Schengen Associated Countries expressed some concerns in relation to the same issue, i.e. the fact that they would have to contribute financially to the operation and maintenance costs of ETIAS.

As several delegations pointed out that they still had some scrutiny reservations and needed some time to examine the note prepared by DG BUDG of the Commission, the Presidency indicated that this file would be on the agenda of the next meeting of the Permanent Representatives Committee/Mixed Committee.

Moreover, in order to alleviate the concerns of the Schengen Associated Countries as expressed above, recital 55a has been tabled by the Presidency. This recital makes clear that the operation and maintenance costs of ETIAS should not affect the contributions by the Schengen Associated Countries to the successor(s) of the Internal Security Fund (Borders and Visas) and the general budget of the Union, so that the costs and revenues would be neutral for the Schengen Associated Countries, in the same way that they should be neutral to the Member States in view of the fact that the costs should be covered by the revenue and the fee should be adjusted accordingly as necessary.

New text compared to document 9349/17 is indicated in **bold underline** and ~~double strikethrough~~.

## CONCLUSION

The Committee is therefore invited to examine and endorse the text as set out in the Annex to this note with a view to reaching a general approach at the JHA Council meeting on 8-9 June 2017.

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**

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

After consulting the European Data Protection Supervisor,

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

Having regard to the opinion of the Committee of the Regions<sup>2</sup>,

Acting in accordance with the ordinary legislative procedure,

Whereas:

---

<sup>1</sup> OJ C , , p. .

<sup>2</sup> OJ C , , p. .

- (1) The Communication of the Commission of 6 April 2016 entitled 'Stronger and Smarter Information Systems for Borders and Security'<sup>3</sup> outlined the need for the EU to strengthen and improve its IT systems, data architecture and information exchange in the area of border management, law enforcement and counter-terrorism. It emphasises the need to improve the interoperability of information systems. Importantly, it sets out possible options for maximising the benefits of existing information systems and, if necessary, developing new and complementary ones to address still existing information gaps.
- (2) Indeed, the Communication of 6 April 2016 identified a series of information gaps. Amongst them the fact that border authorities at external Schengen borders have no information on travellers exempt from the requirement of being in possession of a visa when crossing the external borders (the visa requirement). The Communication of 6 April 2016 announced that the Commission would launch a study on the feasibility of establishing a European Travel Information and Authorisation System (ETIAS), which was completed in November 2016. Such an automated system would determine the eligibility of visa-exempt third country nationals prior to their travel to the Schengen Area, and whether such travel poses a security, ~~or irregular~~ illegal immigration or public health risk.
- (3) The Communication of 14 September 2016 'Enhancing security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders'<sup>4</sup> confirms the priority of securing external borders and presents concrete initiatives to accelerate and broaden the EU response in continuing to strengthen the management of external borders.

---

<sup>3</sup> COM(2016) 205 final.

<sup>4</sup> COM(2016) 602 final.

- (4) It is necessary to specify the objectives of the ~~European Travel Information and Authorisation System (ETIAS)~~, to define its technical architecture, to set up the ETIAS Central Unit, the ETIAS National Units and the ETIAS Screening Board, to lay down rules concerning the operation and the use of the data to be entered into the system by the applicant, to establish rules on the issuing or refusal of the travel authorisations, to lay down the purposes for which the data are to be processed, to identify the authorities authorised to access the data and to ensure protection of personal data.
- (5) The ETIAS should apply to third country nationals who are exempt from the visa requirement of being in possession of a visa when crossing the external borders and to those who are exempt from the airport transit visa requirement.
- (6) It should also apply to third country nationals who are exempt from the visa requirement who are family members of a Union citizen to whom Directive 2004/38/EC<sup>5</sup> applies or of a national of a third country enjoying the right of free movement equivalent to that of Union citizens under an agreement between the Union and its Member States on the one hand and a third country on the other under Union law and who do not hold a residence card referred to under Directive 2004/38/EC or a residence permit pursuant to Regulation (EC) No 1030/2002. Article 21(1) of the Treaty on the Functioning of the European Union stipulates that every citizen of the Union shall have the right to move and reside freely within the territory of the Member States, subject to the limitations and conditions laid down in the Treaties and by the measures adopted to give them effect. The respective limitations and conditions are to be found in Directive 2004/38/EC on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States.

---

<sup>5</sup> Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC.

- (7) As confirmed by the Court of Justice of the European Union<sup>6</sup>, such family members have the right to enter the territory of the Member States and to obtain an entry visa for that purpose. Consequently, also family members exempted from the visa obligation should have the right to obtain a travel authorisation. Member States should grant such persons every facility to obtain the necessary travel authorisation which must be issued free of charge.
- (8) The right to obtain a travel authorisation is not unconditional as it can be denied to those family members who represent a risk to public policy, public security or public health pursuant to Directive 2004/38/EC. Against this background, family members can be required to provide their personal data related to their identification and their status only insofar these are relevant for assessment of the security threat they could represent. Similarly, examination of their travel authorisation applications should be made exclusively against the security concerns, and not those related to immigration risks.
- (9) The ETIAS should establish a travel authorisation for third country nationals exempt from the visa requirement to be in possession of a visa when crossing the external borders ('the visa requirement') and for those who are exempt from the airport transit visa requirement, enabling to determine whether their presence in the territory of the Member States does not pose an security, irregular illegal immigration, security or public health risk. Holding a valid travel authorisation should be a new entry condition for the territory of the Member States, however mere possession of a travel authorisation should not confer an automatic right of entry.
- (10) The ETIAS should contribute to a high level of security, to the prevention of irregular illegal immigration and to the protection of public health by providing an assessment of visitors prior to their arrival at the external borders crossing points.

---

<sup>6</sup> Judgment of the Court of 31 January 2006 in case C-503/03 Commission v Spain (Rec. 2006, p. I-1097).

- (11) ETIAS should contribute to the facilitation of border checks performed by border guards at the external borders crossing points and ensure a coordinated and harmonised assessment of third country nationals subject to the travel authorisation requirement who intend to travel to the Member States intending at visiting the Schengen area. In addition it should enable to better inform applicants of their eligibility to travel to the Member States ~~visit the Schengen area~~. Moreover, the ETIAS should also contribute to the facilitation of border checks by reducing the number of refusals of entry at the external borders.
- (12) The ETIAS should also support the objectives of the Schengen Information System (SIS) related to the alerts in respect of persons wanted for arrest or for surrender or extradition purposes, on missing persons, on persons sought to assist with a judicial procedure and on persons for discreet checks, [inquiry checks] or specific checks. For this purpose the ETIAS should ~~carry out an automated processing of~~ the application files against the relevant alerts in the SIS. This processing will be carried out for the purpose of supporting the SIS. ~~Accordingly, any hit resulting from this comparison should be stored in the SIS notified to the SIRENE Bureau concerned. Once and once this information is transferred to the SIRENE bureau, it should be dealt with in accordance with the relevant legislation relating to the SIS.~~
- (13) The ETIAS should consist of a large-scale information system, the ETIAS Information System, ~~a central team,~~ the ETIAS Central Unit and ~~national teams,~~ the ETIAS National Units.

- (14) The ETIAS Central Unit should be part of the European Border and Coast Guard Agency. The ETIAS Central Unit should be responsible for determining the verification parameters for ensuring the completeness of the application and the coherence of the data, for verifying, where the automated application process has reported a hit, travel authorisations' applications rejected from the automated process in order to determine whether the applicant's personal data corresponds to the personal data of the person having triggered that a hit, for launching the manual processing of the application, for launching the consultation process between the ETIAS National Units of the Member States involved, for establishing the specific risk indicators screening rules, and for carrying out regular audits on the processing of applications. The ETIAS Central Unit should work in 24/7 regime.
- (15) Each Member State should establish an ETIAS National Unit mainly responsible for the examination and decision on whether to issue or refuse a travel authorisation. The ETIAS National Units should cooperate among themselves and with Europol for the purpose of the assessment of the applications. The ETIAS National Unit should be provided with adequate resources for them to fulfil their tasks in accordance with the deadlines set out in this Regulation work in 24/7 regime.
- (16) To meet its objectives, the ETIAS should provide an online application form that the applicant should fill in with declarations relating to his or her identity, travel document, residence information, contact details, education and current occupation, his or her condition of family member to EU citizens or third country nationals benefiting from free movement not holding a residence card pursuant to Directive 2004/38/EC or a residence permit pursuant to Regulation (EC) No 1030/2002, if the applicant is minor, identity details of the responsible person and answers to a set of background questions (~~whether or not the applicant is subject to any disease with epidemic potential as defined by the International Health Regulations of the World Health Organisation or other infectious or contagious parasitic diseases, criminal records, presence in war zones, decision to return to borders/orders to leave territory~~). Access to the applicants' health data should only be allowed to determine whether they represent a threat to public health.

- (17) ETIAS should accept applications introduced on behalf of the applicant for situations where travellers are themselves not in a position to create an application, for whatever reason. In such cases, the application should be carried out by a third person authorised by the traveller or legally responsible for him/her provided this person's identity is included in the application form.
- (17a) Parameters for ensuring the completeness of the application and the coherence of the data should be established by the Central Unit to verify the admissibility of the application for travel authorisation. For instance, this verification should preclude the use of travel documents which will expire in less than six three months, have expired or were issued more than ten years before. This verification should occur before the applicant is invited to pay the fee.
- (18) In order to finalise the application, all applicants above the age of 12 ~~18~~ should be required to pay a fee. The payment should be managed by a bank or a financial intermediary. Data required for securing the electronic payment should only be provided to the bank or financial intermediary operating the financial transaction and are not part of the ETIAS data.
- (19) Most of the travel authorisations should be issued within minutes, however a reduced number could take longer, especially up to 72 hours for exceptional cases, where a request for additional information or documentation or an invitation to an interview is notified to the applicant ~~the procedure could last up to two weeks.~~

- (19a) The possibility for the ETIAS National Unit of the responsible Member State to invite an applicant to an interview should be envisaged for cases where it considers it necessary for the purposes of assessing the application. This should not be construed as a right of the applicant or an obligation on the ETIAS National Unit of the responsible Member State, but remains at the discretion of the latter, taking into account, inter alia, the presence or otherwise of a consulate of that Member State in the country of residence of the applicant. The communication between the ETIAS National Unit and the consulate should be organised by the Member State concerned taking into account security and data protection requirements, should that Member State decide to avail of itself of this possibility for the ETIAS National Unit to invite the applicant for an interview.
- (20) The personal data provided by the applicant should be processed by the ETIAS for the sole purposes of ~~verifying in advance the eligibility criteria laid down in Regulation (EU) 2016/399<sup>7</sup>~~ and assessing whether the applicant is likely to irregularly migrate, whether the entry of the applicant in the Union could pose a threat to security, illegal immigration or ~~to~~ public health in the Union.
- (21) The assessment of such risks cannot be carried out without processing the personal data listed in recital (16). Each item of personal data in the applications should be compared with the data present in a record, file or alert registered in an information system (the Schengen Information System (SIS), the Visa Information System (VIS), the Europol data, the Interpol Stolen and Lost Travel Document database (SLTD), [the Entry/Exit System (EES), the Eurodac, the European Criminal Records Information System (ECRIS)] and/or the Interpol Travel Documents Associated with Notices database (Interpol TDAWN)) or against the ETIAS watchlists, or against specific risk indicators. The categories of personal data that should be used for comparison should be limited to the categories of data present in the queried information systems, the ETIAS watchlist or the specific risk indicators.

---

<sup>7</sup> 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).

- (22) The comparison should take place by automated means. Whenever such comparison reveals that a correspondence (a 'hit') exists ~~with~~ between any of the personal data or combination thereof in the applications and that in a record, file or alert in the above information systems, ~~or with~~ the personal data in the ETIAS watchlist, or ~~with~~ the risk indicators, the application should be processed manually by ~~an operator in~~ the ETIAS National Unit of the responsible Member State ~~of declared first entry~~. The assessment performed by the ETIAS National Unit should lead to the decision to issue or not the travel authorisation.
- (23) The automated processing may result in the issuing of an authorisation. It is expected that the vast majority of applications will obtain a positive answer by automated means. No denial of a travel authorisation should be based only on the automated processing of personal data in the applications. For this reason, the applications for which a hit was generated should be assessed manually by ~~an operator in~~ an ETIAS National Unit.
- (24) Applicants who have been refused a travel authorisation should have the right to appeal. Appeals should be conducted in the Member State that has taken the decision on the application and in accordance with the national law of that Member State.
- (25) The screening rules should be used to analyse the application file by enabling a comparison between the data recorded in an application file ~~of the ETIAS Central System~~ and specific risk indicators corresponding to previously identified security, ~~irregular~~ illegal immigration or public health risk. The criteria used for defining the specific risk indicators should in no circumstances be based on a applicant's sex, race, ~~or~~ ethnic origin, ~~political opinions~~, religion or ~~philosophical beliefs~~, ~~trade union membership~~, ~~sexual life~~ disability, age or sexual orientation.

- (26) An ETIAS watchlist should be established for identifying connections between data in an ~~ETIAS~~ application file and information related to persons who are suspected of having committed or having taken part in a ~~an act of~~ serious criminal offence ~~crime~~ or a terrorism offence, or regarding whom there are factual indications or reasonable grounds to believe that they will commit ~~an act of~~ serious ~~crime~~ criminal offences or a terrorism offence. The ETIAS watchlist should be developed and hosted by Europol. Information should be entered into the watchlist by Europol, without prejudice to the relevant provisions ~~part of the data processed by Europol in accordance with Article 18(2)(a) of Regulation (EU) 2016/794 on international cooperation, and by Member States, and Europol's Integrated Data Management Concept implementing that Regulation.~~ When providing information to Europol, Member States should be able to determine the purpose or purposes for which it is to be processed, including the possibility to limit this processing to the ETIAS watchlist.
- (27) The continuous emergence of new forms of security threats, new patterns of ~~irregular~~ illegal immigration and public health threats requires effective responses and needs to be countered with modern means. Since these means entail the processing of important amounts of personal data, appropriate safeguards should be introduced to keep the interference with the right to protection of private life and to the right of protection of personal data limited to what is necessary in a democratic society.
- (28) Personal data in ETIAS should therefore be kept secure; access to it should be limited to strictly authorised personnel and in no circumstance ~~it~~ should it be used to reach decisions based on any form of discrimination. The personal data stored should be kept securely in eu-LISA's facilities in the Union.

- (29) Issued travel authorisations should be annulled or revoked as soon as it becomes evident that the conditions for issuing ~~it~~ them were not or are no longer met. In particular, when a new SIS alert is created for a refusal of entry or for a reported lost, ~~or~~ stolen or invalidated travel document, the SIS should inform the ETIAS which should verify whether this new alert corresponds to a valid travel authorisation. In such a case, the ETIAS National Unit of the responsible Member State having created the alert should be immediately informed by the ETIAS Central System and revoke the travel authorisation. Following a similar approach, new elements introduced in the ETIAS watchlist ~~shall~~ should be compared with the application files stored in the ETIAS in order to verify whether this new element corresponds to a valid travel authorisation. In such a case, the ETIAS National Unit of the responsible Member State of first entry that entered the new element, or the Member State of first intended stay or transit in the case of an element entered by Europol, should assess the hit and, where necessary, revoke the travel authorisation. Similarly, a refusal of entry on certain grounds in the Entry/Exit System should trigger a reassessment, and where necessary, the revocation of the travel authorisation. A possibility to revoke the travel authorisation at the request of the applicant should also be provided.
- (30) When, in exceptional circumstances, a Member State considers it necessary to allow a third country national to travel to its territory on humanitarian grounds, for reasons of national interest or because of international obligations, it should have the possibility to issue a travel authorisation with limited territorial and temporal validity. Considering the nature of the travel authorisation as an authorisation to travel to the territory of Member States for the purpose of a short stay or airport transit, reasons relating to international protection do not constitute humanitarian grounds in terms of issuance of travel authorisations with limited territorial validity. With regard to international obligations, this should include the obligations deriving from the EU Charter of Fundamental Rights and should in particular cover the cases referring to the right to a fair trial.

(31) Prior to boarding, air and sea carriers, as well as international carriers transporting groups overland by coach should have the obligation to verify ~~if travellers have all the travel documents required for entering the territory of the Member States pursuant to the Schengen Convention<sup>8</sup>. This should include~~ Such carriers should verifying that travellers are in possession of a valid travel authorisation. The ETIAS file itself should not be accessible to carriers. ~~A Secure internet~~ access to a carrier gateway, including the possibility to use ~~using~~ mobile technical solutions, should allow carriers to proceed with this consultation using travel document data.

(31a) 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.

(32) In order to comply with the revised conditions for entry, border guards should check whether the traveller is in possession of a valid travel authorisation. Therefore, during the standard border control process, the border guard should electronically read the travel document data. This operation should trigger a query to different databases as provided under the Schengen Border Code including a query to ETIAS which should provide the up-to-date travel authorisation status. ~~The full ETIAS file itself should not be accessible to the border guard for border controls, but~~ certain data in the ETIAS file should be accessible to the border guards with a view to assisting them in carrying out their tasks. If there is no valid travel authorisation, the border guard should refuse entry and should complete the border control process accordingly. If there is a valid travel authorisation, the decision to authorise or refuse entry should be taken by the border guard.

---

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

- (32a) Where the ETIAS National Unit of the responsible Member State considers that some elements of the application for a travel authorisation deserve further examination by the border guards, it may attach a flag to the travel authorisation it issues, recommending further or specific checks at the border crossing point. It should also be possible for a flag to be attached upon the request of a consulted Member State.
- (32b) The address for the first intended stay declared in the application being different from the address declared at entry should not lead to an automatic refusal of entry at the border by the border guards.
- (32c) 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. Immigration authorities of the Member States should have access to certain information stored in the ETIAS Central System, in particular for the purpose of returns. They should search the ETIAS Central System using the information which is contained in the machine readable zone of a travel document without necessarily using specific equipment for that purpose.
- (33) In the fight against terrorist offences and other serious criminal offences and given the globalisation of criminal networks, it is imperative that ~~law enforcement~~ designated authorities responsible for the prevention, detection or investigation of terrorist offences and other serious criminal offences ('designated authorities') have the necessary information to perform their tasks effectively. Access to data contained in the Visa Information System (VIS) for ~~law enforcement~~ such purpose has already proven effective in helping investigators to make substantial progress in cases related to human being trafficking, terrorism or drug trafficking. The Visa Information System does not contain data on visa-exempt third-country nationals.

(34) Access to the information contained in ETIAS is necessary to prevent, detect and investigate terrorist offences as referred to in Directive 2017/541(EU) Council Framework Decision 2002/475/JHA<sup>9</sup> or other serious criminal offences as referred to in Council Framework Decision 2002/584/JHA<sup>10</sup>. In a specific investigation and in order to establish evidence and information related to a person suspected of having committed a serious crime or a victim of a serious crime, ~~law enforcement~~ designated authorities may need access to the data generated by ETIAS. The data stored in ETIAS may also be necessary to identify the perpetrator of a terrorist offence or other serious criminal offences, especially when urgent action is needed. Access to the ETIAS 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 ETIAS. Therefore, the data in ETIAS should be retained and made available to the designated authorities of the Member States and the European Police Office ('Europol'), subject to the strict conditions set out in this Regulation in order for such access to be limited to what is strictly necessary for the prevention, detection and investigation of terrorist offences and other serious criminal offences in accordance with the requirements notably laid down in the jurisprudence of the Court, in particular in the Digital Rights Ireland case<sup>11</sup>.

---

<sup>9</sup> Directive (EU) 2017/541 of 15 March 2017 on combatting terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Directive 2005/671/JHA (OJ L 88, 31.03.2017, p. 6) of 13 June 2002 on combatting terrorism (OJ L 164, 22.6.2002 p.6).

<sup>10</sup> 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).

<sup>11</sup> Judgment of the Court (Grand Chamber) of 8 April 2014 in joined cases C-293/12 and C-594/12 Digital Rights Ireland Ltd, ECLI:EU:C:2014:238.

- (35) In particular, access to ETIAS data for the purpose of preventing, detecting or investigating terrorist offences or other serious criminal offences should only be granted following a reasoned request by the operating unit of the designated authority ~~competent authorities~~ giving reasons for its necessity. ~~Member States should ensure that any such request for access to data stored in ETIAS be the subject of a prior review by a court or by an authority providing guarantees of full independence and impartiality, and which is free from any direct or indirect external influence. However, in situations of extreme urgency, it can be crucial for the competent authorities~~ Where there is a need to immediately obtain immediately personal data necessary for preventing ~~the commission~~ a terrorist offence or an imminent danger associated with another of a serious criminal offence ~~crime~~ or so that its perpetrators can be prosecuted, ~~In such cases~~ it should be accepted that the verification as to whether the conditions were fulfilled ~~review of the personal data obtained from ETIAS~~ takes place as swiftly as possible after access to such data has been granted to the designated ~~competent~~ authorities.
- (36) It is therefore necessary to designate the ~~competent~~ authorities of the Member States 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.
- (37) ~~The ETIAS National Units should act as~~ The central access point(s) designated by each Member State ~~and~~ should verify that the conditions to request access to the ETIAS Central System are fulfilled in the concrete case at hand.
- (38) Europol is the hub for information exchange in the Union and it 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 ETIAS Central System within the framework of its tasks and in accordance with Regulation (EU) 2016/794<sup>12</sup> in specific cases where this is necessary for Europol to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences.

---

<sup>12</sup> OJ L 119, 4.5.2016, p. 132-149.

(39) To exclude systematic searches, the processing of data stored in the ETIAS Central System should take place only in specific cases and only 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 ETIAS 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. ~~The law enforcement authorities and Europol should only request access to the ETIAS if prior searches in all relevant national databases of the Member State and databases at Europol did not lead to the requested information.~~

(40) The personal data recorded in the ETIAS should be kept for no longer than is necessary for its purposes. In order for the ETIAS to function, it is necessary to keep the data related to applicants for the period of validity of the travel authorisation. In order to assess the security, ~~irregular~~ illegal immigration and public health risks posed by the applicants it is necessary to keep the personal data for five years from the last entry/exit record of the applicant stored in the EES. In fact, the ETIAS should rely on accurate preliminary assessments of the security, ~~public health and irregular~~ illegal immigration and public health risks, notably through the use of the screening rules. In order to constitute a reliable basis for the manual risk assessment by the Member States, and reduce to the minimum the occurrence of hits not corresponding to real risks ('false positives'), the hits resulting from screening rules based on statistics generated by ETIAS data itself need to be representative of a sufficiently broad population. This cannot be achieved exclusively on the basis of the data of the travel authorisations in their validity period. The retention period should start from the last entry/exit record of the applicant stored in the EES, since that constitutes the last actual use of the travel authorisation. A retention period of five years corresponds to the retention period of an ~~EES~~ entry/exit record with an entry authorisation granted on the basis of an ETIAS travel authorisation or a refusal of entry. This synchronisation of retention periods ensures that both the entry/exit record and the related travel authorisation are kept for the same duration and is an additional element ensuring the future interoperability between ETIAS and EES. This synchronisation of data retention periods is necessary to allow the competent authorities to perform the risk analysis requested by the Schengen Borders Code.

A decision to refuse, revoke or annul a travel authorisation could indicate a higher security, ~~or irregular~~ illegal immigration or public health risk posed by the applicant. Where such a decision has been issued, the 5 years retention period for the related data should start from ~~its~~ the date of that decision~~issuance~~, in order for ETIAS to be able to take accurately into account the higher risk possibly posed by the applicant concerned. After the expiry of such period, the personal data should be deleted.

- (41) Precise rules should be laid down as regards the responsibilities of the Agency for the operational management of large-scale information systems in the area of freedom, security and justice (eu-LISA) for the designing, development and technical management of the ETIAS Information System, the responsibilities of the European ~~Coast and Border~~ and Coast Guard Agency, the responsibilities of the Member States and the responsibilities of Europol.
- (42) Regulation (EC) No 45/2001 of the European Parliament and the Council<sup>13</sup> applies to the activities of eu-LISA and the European ~~Coast and Border~~ and Coast Guard Agency when carrying out the tasks entrusted to them in this Regulation.
- (43) [Regulation (EU) 2016/679]<sup>14</sup> applies to the processing of personal data by the Member States' authorities in application of this Regulation unless such processing falls within the scope of [Directive (EU) 2016/680] ~~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.~~
- (44) [Directive (EU) 2016/680]<sup>15</sup> applies to the processing of personal data by the designated 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 [Directive (EU) 2016/680].~~

---

<sup>13</sup> 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).

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

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

- (45) The independent supervisory authorities established in accordance with [Regulation (EU) 2016/679] should monitor the lawfulness of the processing of personal data by the Member States, whilst the European Data Protection Supervisor as established by Regulation (EC) No 45/2001 should monitor the activities of the Union institutions and bodies in relation to the processing of personal data. The European Data Protection Supervisor and the supervisory authorities should cooperate with each other in the monitoring of the ETIAS.
- (46) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 6 March 2017.
- (47) Strict access rules to the ETIAS Central System and the necessary safeguards should be established. It is also necessary to provide for 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.

- (48) In order to assess the security, ~~irregular~~ illegal immigration or public health risk which could be posed by a traveller, interoperability between the ETIAS Information System and other EU information systems consulted by ETIAS such as the Entry/Exit System (EES), the Visa Information System (VIS), the Europol data, the Schengen Information System (SIS), the Eurodac and the European Criminal Records Information System (ECRIS) should have to be established including for the purpose of implementing this Regulation. ~~However this interoperability can only be fully ensured once the proposals to establish the EES<sup>16</sup>, the ECRIS<sup>17</sup> and the recast proposal of the Eurodac Regulation<sup>18</sup> have been adopted.~~
- (49) ~~The effective monitoring of the application of this Regulation requires evaluation at regular intervals. The Member States should lay down rules on the penalties applicable to infringements of the provisions of this Regulation and ensure that they are implemented. Member States should take the necessary measures to ensure that the penalties applicable to infringements of the provisions of this Regulation are dissuasive, effective and proportionate and that they are implemented.~~
- (50) In order to establish the technical measures needed for the application of this Regulation, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission:

---

<sup>16</sup> 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) COM(2016) 194 final.

<sup>17</sup> Proposal for a Directive of the European Parliament and of the Council amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA.

<sup>18</sup> Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast) COM(2016) 272 final.

- to adopt a predetermined list of answers concerning the questions on the level and field of education, the current occupation and the job title to be indicated in the application for a travel authorisation,
- to specify the content and format of questions relating to diseases, convictions for criminal offences, stays in war or conflict zones and decisions to leave the territory or return decisions which can be put to an applicant for a travel authorisation,
- to specify the content and format of ~~the~~ additional questions ~~which can be put to an~~ the applicant having replied affirmatively to one of the questions relating to diseases, convictions for criminal offences, stays in war or conflict zones and decisions to leave the territory or return decisions, and to set out the predetermined list of answers thereto for a travel authorisation,
- to lay down the payment methods and process for the travel authorisation fee and the changes to the amount of that fee taking into account any increase in the costs of the ETIAS the technological developments and their availability and to amend the amount of the fee,
- to lay down the content and format of a predetermined list of options when the applicant is requested to provide additional information or documentation,
- ~~— to regularly identify specific risks relating to further specify the security, irregular illegal immigration or public health risks to be used for the establishment of the risk indicators in order to ensure adaptation in view of the continuous emergence of new risks and patterns,~~
- to extend the duration of the transitional period of grace during which no travel authorisations is required, as well as of to extend the duration of the period of grace during which ~~no~~ a travel authorisations is required but in which border guards will allow third country nationals not in possession of the travel authorisation exceptionally to enter subject to certain conditions.

~~—— to further specify the security, irregular migration or public health risks to be used for the establishment of the risk indicators.~~

- (51) It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

- (52) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to adopt detailed rules on the conditions for operation of the public website and the mobile app for mobile devices and on the data protection and security rules applicable to the public website and the mobile app for mobile devices, to regularly identify specific risks relating to security, illegal immigration or public health to be used for the establishment of the risk indicators in order to ensure adaptation in view of the continuous emergence of new risks and patterns, to establish the technical specifications of the ETIAS watchlist, to adopt as well as an authentication scheme reserved exclusively to carriers and to specify the details of the fall-back procedures to be followed in the case of technical impossibility to access data by carriers ETIAS, to adopt model contingency plans in case of technical impossibility to access data at the external borders or failure of the ETIAS, to adopt a model security plan and a model business continuity and disaster recovery plan in relation to security of processing of personal data, to lay down and develop a mechanism, procedures and interpretation of data quality compliance, to draw up a common leaflet to inform travellers, to adopt detailed rules on the operation of the central repository and the data protection and security rules applicable to the repository, and to make available to Member States a technical solution in order to facilitate the collection of certain data. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council<sup>19</sup>.
- (53) The establishment of a ETIAS 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.

---

<sup>19</sup> 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).

- (54) ~~The projected costs for the development of the ETIAS Information System and for the establishment of the ETIAS Central Unit and the ETIAS National Units are lower than the remaining amount on the budget earmarked for Smart Borders in Regulation (EU) No 515/2014 of the European Parliament and the Council<sup>20</sup>. Accordingly, this Regulation, pursuant to Article 5(5)(b) of Regulation (EU) No 515/2014, should, re-allocate the amount currently attributed for developing IT systems supporting the management of migration flows across the external borders. The operational and maintenance costs of the ETIAS Information System, the ETIAS Central Unit and of the ETIAS National Units should be covered entirely by the revenues generated by the fees. The fee should therefore be adapted as necessary, having regard to the costs.~~
- (55) The revenue generated by the payment of travel authorisation fees should be assigned to cover the recurring operational and maintenance costs of the ETIAS Information System, of the ETIAS Central Unit and of the ETIAS National Units. In view of the specific character of the system, it is appropriate to treat the revenue as ~~external~~ internal assigned revenue.
- (55a) The costs relating to the operation and maintenance of the ETIAS should not affect the contributions of the Schengen Associated Countries to the successor(s) to the Internal Security Fund (Borders and Visas) or to the general budget of the European Union and should therefore not be taken into account for the purpose of calculating those contributions.**
- (56) This Regulation is without prejudice to the application of Directive 2004/38/EC.
- (57) 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.

---

<sup>20</sup> 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).

- (58) This Regulation constitutes a development of the provisions of the Schengen *acquis* in which the United Kingdom does not take part, in accordance with Council Decision 2000/365/EC<sup>21</sup>; 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.
- (59) This Regulation constitutes a development of the provisions of the Schengen *acquis* in which Ireland does not take part, in accordance with Council Decision 2002/192/EC<sup>22</sup>; Ireland is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.
- (60) As regards Iceland and Norway, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latter's association with the implementation, application and development of the Schengen *acquis*<sup>23</sup> which fall within the area referred to in Article 1, point A of Council Decision 1999/437/EC<sup>24</sup>.
- (61) As regards Switzerland, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*<sup>25</sup> which fall within the area referred to in Article 1, point A of Council Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/146/EC<sup>26</sup> and with Article 3 of Council Decision 2008/149/JHA<sup>27</sup>.

---

<sup>21</sup> 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).

<sup>22</sup> Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen *acquis* (OJ L 64, 7.3.2002, p. 20).

<sup>23</sup> OJ L 176, 10.7.1999, p. 36.

<sup>24</sup> Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis* (OJ L 176, 10.7.1999, p. 31).

<sup>25</sup> OJ L 53, 27.2.2008, p. 52.

<sup>26</sup> Council Decision 2008/146/EC of 28 January 2008 on the conclusion, on behalf of the European Community, of the Agreement between the European Union, the European

(62) As regards Liechtenstein, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*<sup>28</sup> which fall within the area referred to in Article 1, point A of Council Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU<sup>29</sup> and with Article 3 of Council Decision 2011/349/EU.<sup>30</sup>

~~(63) 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.~~

---

Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L 53, 27.2.2008, p. 1).

<sup>27</sup> Council Decision 2008/149/JHA of 28 January 2008 on the conclusion on behalf of the European Union of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L 53, 27.2.2008, p. 50).

<sup>28</sup> OJ L 160, 18.6.2011, p. 21.

<sup>29</sup> Council Decision 2011/350/EU of 7 March 2011 on the conclusion, on behalf of the European Union, of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*, relating to the abolition of checks at internal borders and movement of persons (OJ L 160, 18.6.2011, p. 19).

<sup>30</sup> Council Decision 2011/349/EU of 7 March 2011 on the conclusion on behalf of the European Union of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* relating in particular to judicial cooperation in criminal matters and police cooperation (OJ L 160, 18.6.2011, p. 1).

- (64) In order to have this Regulation fit into the existing legal framework and reflect the changes for the European Border and Coast ~~and Border~~ Guard Agency and ~~Europol~~ the Regulations (EU) No 515/2014, (EU) 2016/399, ~~(EU) 2016/794~~ and (EU) 2016/1624 should be amended accordingly.

HAVE ADOPTED THIS REGULATION:

# CHAPTER I

## General provisions

### *Article 1* *Subject matter*

1. This Regulation establishes a 'European Travel Information and Authorisation System' (ETIAS) for third country nationals exempt from the requirement to be in possession of a visa when crossing the external borders ('the visa requirement') or when in airport transit enabling to ~~determine~~ assess whether their presence in the territory of the Member States ~~does not~~ would pose an security, irregular illegal immigration, security or public health risk. For this purpose a travel authorisation and the conditions and procedures to issue or refuse it are introduced.
2. This Regulation lays down the conditions under which Member States' ~~law enforcement~~ designated authorities and the European Union Agency for Law Enforcement Cooperation ~~Police Office~~ (Europol) may consult data stored in the ETIAS Central System for the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences falling under their competence.

### *Article 2* *Scope*

1. This Regulation applies to the following categories of third country nationals ~~exempt from the visa requirement~~:
  - (a) nationals of third countries listed in Annex II to Council Regulation (EC) No 539/2001<sup>31</sup> who are exempt from the visa requirement for ~~airports transits or~~ intended stays in the territory of the Member States of a duration of no more than 90 days in any 180 day period;

---

<sup>31</sup> OJ L 81, 21.3.2001, p. 1.

- (aa) nationals of third countries who are not required to hold an airport transit visa, for the purpose of transit through the international transit areas of one or more Member States' airports of the Member States, unless they are in possession of a valid visa;
- (b) refugees and stateless persons where the third country in which they reside and which issued their travel document is one of the third countries listed in Annex II to Regulation (EC) No 539/2001 and persons who are exempted from the visa requirement pursuant to Article 4(2)(b) of that Regulation (EC) No 539/2001 for intended stays in the territory of the Member States of a duration of no more than 90 days in any 180 day period;
- (c) third country nationals who are exempt from the visa requirement and who fulfil the following conditions:
  - i) they 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 equivalent to that of Union citizens under an agreement between the Union and its Member States on the one hand and a third country on the other;
  - ii) they do not hold a residence card referred to under Directive 2004/38/EC or a residence permit pursuant to Regulation (EC) No 1030/2002.

2. This Regulation does not apply to:

- (a) refugees or stateless persons or other persons who do not hold the nationality of any country who reside in a Member State and who are holders of a travel document issued by that Member State;
- (b) third country nationals who are members of the family of a Union citizen to whom Directive 2004/38/EC applies and who hold a residence card pursuant to that Directive;

- (c) third country nationals who are members of the family of a nationals of a third country enjoying the right of free movement under Union law equivalent to that of Union citizens under an agreement between the Union and its Member States on the one hand and a third country on the other and who hold a residence card pursuant to Directive 2004/38/EC or a residence permit pursuant to Regulation 1030/2002
- (d) holders of residence permits referred to in point 16 of Article 2 of Regulation (EU) 2016/399 of the European Parliament and of the Council<sup>32</sup> ~~other than those covered by points (b) and (c) of this paragraph;~~
- (e) holders of uniform visas ~~or~~
- (ea) holders of national long-stay visas;
- (f) nationals of Andorra, Monaco and San Marino and holders of a passport issued by the Vatican State;
- (g) the nationals of third countries ~~listed in Annex I and II to Regulation (EC) No 539/2001~~ who are holders of a local border traffic permit issued by the Member States pursuant to Regulation (EC) No 1931/2006<sup>33</sup> when these holders exercise their right within the context of the Local Border Traffic regime;
- (h) persons or categories of persons referred to in Article 4(1)(a) to (f) ~~and (3)~~ of Regulation (EC) No 539/2001.
- (i) persons who have been subjected to a visa requirement pursuant to Article 4(3) of Regulation (EC) No 539/2001.

---

<sup>32</sup> Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ L 077 23.3.2016, p. 1).

<sup>33</sup> OJ L 405, 30.12.2006, p. 1.

*Article 3*  
*Definitions*

1. For the purposes of this Regulation, the following definitions apply:
- (a) 'external borders' mean external borders as defined in Article 2(2) of Regulation (EU) 2016/399;
  - (b) 'border checks' means border checks as defined in Article 2(11) of Regulation (EU) 2016/399;
  - (ba) 'second line check' means a second line check as defined in Article 2(13) of Regulation (EU) 2016/399;
  - (c) 'border guard' means border guard as defined in Article 2(14) of Regulation (EU) 2016/399;
  - (d) 'travel authorisation' means a decision issued in accordance with this Regulation indicating that ~~there are~~ no factual indications or reasonable grounds have been identified to conclude **consider** that the presence of the person on the territory of the Member States ~~will pose a security, irregular illegal immigration, security or public health risk~~ and which is a requirement for third country nationals referred to in Article 2 to fulfil the entry condition laid down in Article 6(1)(b) of Regulation (EU) 2016/399.
  - (da) 'security risk' means a risk of a threat to public policy, internal security or international relations obligations of any of the Member States;
  - (db) 'illegal immigration risk' means the risk of a third country national not fulfilling the conditions of entry and stay as set out in Article 6 of Regulation (EU) 2016/399 of the European Parliament and of the Council<sup>34</sup>.

---

<sup>34</sup> Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ L 077 23.3.2016, p. 1).

- (e) 'public health risk' means any disease with epidemic potential as defined by the International Health Regulations of the World Health Organization and other infectious diseases or contagious parasitic diseases if they are the subject of protection provisions applying to nationals of the Member States ~~threat to public health as defined in Article 2(21) of Regulation (EU) 2016/399;~~
- (f) 'applicant' means any third country national referred to in Article 2 who has lodged an application for a travel authorisation;
- (g) '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;
- (h) 'short stay' means stays in the territory of the Member States within the meaning of Article 6(1) of Regulation (EU) 2016/399;
- (i) '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;
- (j) 'mobile app for mobile devices' means a software application designed to run on mobile devices such as smartphones and tablet computers;
- (k) 'hit' means the existence of a correspondence established by comparing the personal data recorded in an application file of the ETIAS Central System with the personal data stored in a record, file or alert registered in an information system queried by the ETIAS Central System, in the ETIAS watchlist or with the specific risk indicators referred to in Article 28;
- (l) 'terrorist offences' mean the offences which correspond or are equivalent to those referred to in ~~Articles 1 to 4 of~~ Directive (EU) 2017/541 ~~Framework Decision 2002/475/JHA;~~

- (m) '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;
- (n) 'Europol data' means personal data provided to Europol for the purpose referred to in Article 18(2)(a) of Regulation (EU) 2016/794;
- ~~(o) 'carrier' means any natural or legal person whose profession it is to provide passenger transport of persons ;~~
- (o) 'minor' means a third country national or a stateless person below the age of 18 years;
- (p) 'consulate' means a Member State's diplomatic mission or a Member State's consular post authorised to issue visas and headed by a career consular officer as defined by the Vienna Convention on Consular Relations of 24 April 1963;
- (q) 'designated authorities' means authorities which are responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences and designated by Member States pursuant to Article 43;
- (r) 'immigration authorities' mean 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.

2. The definitions set out in Article 2 of Regulation (EC) 45/2001 shall apply in so far as personal data are processed by the European Border and Coast Guard Agency and eu-LISA
3. The definitions set out in Article 4 of [Regulation (EU) 2016/679] shall apply in so far as personal data are processed by the authorities of Member States.
4. The definitions set out in Article 3 of [Directive (EU) 2016/680] shall apply in so far as personal data are processed by the authorities of the Member States for ~~law enforcement~~ the purposes of prevention, detection or investigation of terrorist offences or of other serious criminal offences.

*Article 4*  
*Objectives of the ETIAS*

By supporting the competent authorities of the Member States, the ETIAS shall ~~will~~:

- (a) contribute to a high level of security by providing for a thorough security risk assessment of applicants, prior to their arrival at the external borders crossing points, in order to determine whether there are factual indications or reasonable grounds to conclude that the presence of the person on the territory of the Member States poses a security risk;
- (b) contribute to the prevention of ~~irregular~~ illegal immigration by providing for an ~~irregular~~ illegal immigration risk assessment of applicants prior to their arrival at the external borders crossing points;
- (c) contribute to the protection of public health by providing for an assessment of whether the applicant poses a public health risk within the meaning of Article 3(1)(e) prior to their arrival at the external borders crossing points;
- (d) enhance the effectiveness of border checks;

- (e) support the objectives of the Schengen Information System (SIS) related to the alerts in respect of persons wanted for arrest or for surrender or extradition purposes, on missing persons, on persons sought to assist with a judicial procedure and on persons for discreet checks [inquiry checks] or specific checks;
- (f) contribute to the prevention, detection and investigation of terrorist offences or of other serious criminal offences.

*Article 5*  
*General structure of ETIAS*

The ETIAS consists of:

- (a) the ETIAS Information System as referred to in Article 6;
- (b) the ETIAS Central Unit as referred to in Article 7;
- (c) the ETIAS National Units as referred to in Article 8.

*Article 6*  
*Set up and technical architecture of the ETIAS Information System*

1. The Agency for the operational management of large-scale information systems in the area of freedom, security and justice ('eu-LISA') shall develop the ETIAS Information System and ensure its technical management.
2. The ETIAS Information System 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 Central System to connect to the national border infrastructures in Member States;

- (c) a secure Communication Infrastructure between the Central System and the National Uniform Interfaces;
- (d) a secure Communication Infrastructure between the ETIAS Central System and the information systems referred to in Article 10;
- (e) a public website and a mobile app for mobile devices;
- (f) an email service;
- (g) a secure account service enabling applicants to provide additional information and/or documentation, if necessary;
- (h) a carrier gateway;
- (i) a secure web service enabling communication between the Central System, on the one hand and the public website, the mobile app, the email service, the secured account service, the carrier gateway, the payment intermediary and the international systems (Interpol systems/databases), on the other hand;
- (j) a software enabling the ETIAS Central Unit and the ETIAS National Units to process the applications and to manage the consultations with other ETIAS National Units referred to in Article 24 and with Europol referred to in Article 25;
- (k) a central repository of data for the purposes of reporting and statistics.

3. [The Central System, the National Uniform Interfaces, the web service, the carrier gateway and the Communication Infrastructure of the ETIAS shall share and re-use as much as technically possible the hardware and software components of respectively the EES Central System, the EES National Uniform Interfaces, the EES web service, the EES carrier gateway and the EES Communication Infrastructure.]

*Article 7*  
*Set up of the ETIAS Central Unit*

1. An ETIAS Central Unit is hereby established within the European Border and Coast Guard Agency.
2. The ETIAS Central Unit working in 24/7 regime shall be in charge of:
  - (a) ~~ensuring that the data stored in the applications files and in the ETIAS Central System is correct~~determining the verification parameters for ensuring that the application is complete and that the data provided is coherent and
  - (aa) ensuring that the data they enter in the applications files is up to date in accordance with the relevant provisions of Articles 48 and 54;
  - (b) ~~verifying, in cases where the automated application process has reported a hit, travel authorisations applications rejected from the automated process in order to determine~~ whether the applicant personal data corresponds to the personal data of the person having triggered a that hit in one of the consulted information systems/databases or the specific risk indicators referred to in Article 28, and where confirmed or where doubts remain, launching the manual processing of the application, as referred to in Article 22;
  - (c) defining, testing, implementing, evaluating and revising the specific risk indicators as referred to in Article 28 after consultation of the ETIAS Screening Board;
  - (d) carrying out regular audits on the processing of applications and on the implementation of the provisions of Article 28 including regularly assessing their impact on fundamental rights, in particular with regard to privacy and personal data protection.

*Article 8*  
*Set up of the ETIAS National Units*

1. Each Member State shall designate a competent authority as the ETIAS National Unit.
2. The ETIAS National Units shall be responsible for:
  - (a) ensuring that the data they enter in the application files is correctly filled in and that the data stored in the applications files and in the ETIAS Central System is correct and up to date in accordance with the relevant provisions of Articles 48 and 54;
  - (b) examining and deciding on ~~travel authorisations'~~ applications for travel authorisation where rejected by the automated application process reported a hit, and the manual processing of the application has been launched by the ETIAS Central Unit and carrying out the manual risk assessment referred to in Article 22;
  - (ba) deciding to issue travel authorisation with limited territorial validity as referred to in Article 38;
  - (c) ensuring coordination ~~between~~ with other ETIAS National Units and Europol concerning the consultation requests referred to in Articles 24 and 25;
  - (d) providing applicants with information regarding the procedure to be followed in the event of an appeal in accordance with Article 31(2);
  - ~~(e) acting as central access point for the consultation of the ETIAS Central System for the purpose laid down in Article 1(2) and in accordance with Article 44;~~
  - (f) annuling and revoking a travel authorisation, as referred to in Articles 34 and 35.
3. Member States shall provide the ETIAS National Units with adequate resources for them to fulfil their tasks in accordance with the deadlines set out in this Regulation 24/7 regime.

*Article 9*  
*The ETIAS Screening Board*

1. An ETIAS Screening Board with an advisory function is hereby established within the European Border and Coast Guard Agency. It shall be composed of a representative of each ETIAS National Unit, the European Border and Coast Guard Agency and Europol.
2. The ETIAS Screening Board shall be consulted ~~on~~:
  - (a) by the ETIAS Central Unit, on the definition, evaluation and revision of the specific risk indicators referred to in Article 28;
  - (b) by Europol, on the implementation of the ETIAS watchlist referred to in Article 29.
3. For the purpose referred to in paragraph 2 4, the ETIAS Screening Board shall issue opinions, guidelines, recommendations and best practices.
4. The ETIAS Screening Board shall meet whenever necessary, and at least twice a year. The costs and servicing of its meetings shall be borne by the European Border and Coast Guard Agency.
5. The ETIAS Screening Board shall adopt rules of procedure at its first meeting by a simple majority of its members.

*Article 10*  
*Interoperability with other EU information systems*

Interoperability between the ETIAS Information System and other EU information systems ~~consulted by ETIAS such as [the Entry/Exit System (EES)], the Visa Information System (VIS), the Europol data, the Schengen Information System (SIS), [the Eurodac] and [the European Criminal Records Information System (ECRIS)]~~ shall be established for the purpose of implementing this Regulation and, in particular including to enable the verification carrying out the risk assessment referred to in Article 18.

*Article 11*  
*Access to data stored in the ETIAS*

1. Access to the ETIAS Information System shall be reserved exclusively to duly authorised staff of the ETIAS Central Unit and of the ETIAS National Units.
2. Access by border guards to the ETIAS Central System in accordance with Article 41 shall be limited to searching the ETIAS Central System to obtain the travel authorisation status of a traveller present at an external border crossing point, and to certain data as referred to in Article 41(2).

Where additional verifications are needed for the purpose of a thorough second line check, access to the ETIAS Central System by the border guards shall be extended to the data provided for in Article 41(3)(4).

3. Access by carriers to the ETIAS Central System ~~by~~ in accordance with Article 39, shall be limited to searching the ETIAS Central System to obtain the travel authorisation status of a traveller.
4. Access by immigration authorities to the ETIAS Central System shall be limited to obtain the travel authorisation status of a traveller present on the territory of the Member State for the purposes of verifying whether the conditions of entry and stay are fulfilled, and to certain data as referred to in Article 42a.
5. Each Member State shall designate the competent national authorities, including the ETIAS National Units, as well as the border guards competent for carrying out border checks and immigration authorities for the purposes of this Regulation. Each Member State referred to in paragraphs 1, 2 and 4 and shall communicate a list of these authorities to eu-LISA without delay. That list shall specify for which purpose the duly authorised staff of each authority shall have access to the data in the ETIAS in accordance with paragraphs 1, 2 and ~~to~~ 4.

*Article 12*  
*Non-discrimination*

Processing of personal data within the ETIAS *Information System* by any user shall not result in discrimination against third country nationals notably on the grounds of sex, race, ~~racial~~ or ethnic origin, religion or belief, disability, age or sexual orientation. It shall fully respect human dignity and integrity. ~~Particular attention shall be paid to children, the elderly and persons with a disability.~~

## CHAPTER II

### Application

#### *Article 13*

##### *Practical arrangements for lodging an application*

1. Applicants shall lodge an application by filling in the online application form via the dedicated public website or via the mobile app for ~~web~~ mobile devices sufficiently in advance of any intended travel.
  - 1a.  Holders of a valid travel authorisation may lodge an application for a new travel authorisation as from 91 days before the expiry date of the valid travel authorisation.  
91 days before the expiry of the travel authorisation, the ETIAS Central System shall automatically inform ~~notify~~ the holder of that travel authorisation via the email service about the expiry date and the possibility to lodge an application for a new travel authorisation.
  - 1b. All communications with the applicant for the purpose of his or her application for a travel authorisation shall be done by email sent to the email address provided by the applicant in the application form as referred to in Article 15(2)(g).
2. Applications may be lodged by the applicant or by a person or a commercial intermediary authorised by the applicant to lodge the application in his or her behalf.

#### *Article 14*

##### *The public website and mobile app for mobile devices*

1. The public website and the mobile app for mobile devices shall enable third country nationals subject to the travel authorisation requirement to launch a travel authorisation application, to provide the data required in the application form in accordance with Article 15 and to pay the travel authorisation fee.

2. The public website and the mobile app for mobile devices shall make the application form widely available and easily accessible to applicants free of charge.
3. The public website and the mobile app for mobile devices shall be available in all the official languages of the Member States.
4. Where the official language(s) of the countries listed in Annex II of Council Regulation (EC) No 539/2001 do not correspond to the languages referred to in paragraph 3, factsheets with information concerning the content and the use of the public website and the mobile app for mobile devices and explanatory information shall be made available by eu-LISA on the public website and on the mobile app for mobile devices in at least one of the official languages of the countries referred to. Where any such country has more than one official language, such factsheets shall only be necessary if none of those languages correspond to the languages referred to in paragraph 3.
5. The public website and the mobile app for mobile devices shall inform applicants of the languages which may be used when filling in the application form.
6. The public website and the mobile app for mobile devices shall provide the applicant with an account service enabling applicants to provide additional information and/or documentation, where required.
  - 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.
  - 6b. The public website shall contain the information referred to in Article 61.
7. The Commission shall adopt detailed rules on the conditions for operation of the public website and the mobile app for mobile devices, and on the data protection and security rules applicable to the public website and the mobile app for mobile devices. Those implementing measures shall be adopted in accordance with the examination procedure referred to in Article 79(2).

*Article 15*  
*Application form and personal data of the applicant*

1. Each applicant shall submit a completed application form including a declaration of authenticity, completeness and reliability of the data submitted and a declaration of veracity and reliability of the statements made. Each applicant shall also state that he or she has understood the conditions for entry as referred to in Article 6 of Regulation (EU) 2016/399 of the European Parliament and of the Council<sup>35</sup> and that he or she may be requested to provide the relevant supporting documents at each entry. Minors shall submit an application form ~~electronically~~ signed by a person exercising permanent or temporary parental authority or legal guardianship.
  
2. The applicant shall provide the following personal data in the application form:
  - (a) surname (family name), first name(s) (given name(s)), surname at birth; date of birth, place of birth, country of birth, sex, current nationality, first name(s) of the parents of the applicant;
  - (b) other names (alias(es), artistic name(s), usual name(s)), if any;
  - (c) other nationalities (if any);
  - (d) type, number and country of issuance of the travel document;
  - (e) the date of issuance and the date of expiry of the validity of the travel document;
  - (f) the applicant's home address or, if not available, his or her city and country of residence;

---

<sup>35</sup> Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ L 077 23.3.2016, p. 1).

- (g) e-mail address and, if any, phone and mobile phone numbers;
- (h) education (level and field);
- (i) current occupation, job title and employer; for students, name of educational establishment;
- (j) address for the first intended stay or, in the case of transit if no stay is intended,  
Member State of first intended transit entry;
- ~~(ja) purpose of first intended stay;~~
- ~~(jb) means of subsistence for the first intended stay and for the return trip;~~
- ~~(jc) duration of the first intended stay;~~
- (k) for minors, surname and first name(s), home address, email address and phone number of the applicant's parental authority or legal guardian;
- (l) where he or she claims the status of family member referred to in Article 2(1)(c):
  - i) their status of family member;
  - ii) the surname, first name(s), date of birth, place of birth, country of birth, current nationality, home address, e-mail address and phone number of the family member with whom the applicant has family ties;
  - iii) their family ties with that family member in accordance with Article 2(2) of Directive 2004/38/EC;
- (m) in the case of applications filled in by a person other than the applicant, the surname, first name(s), name of firm, organization if applicable, e-mail address, mailing address, phone number; relationship to the applicant and an ~~electronically~~ signed representative declaration.
- ~~(n) in the case where an applicant is a minor, whether the applicant's parental authority or legal guardian is subject to an alert in the SIS.~~

3. The applicant shall choose the level and field of education, the current occupation and the job title and the purpose of the first intended stay from a predetermined list. The Commission shall be empowered to adopt delegated acts in accordance with Article 78 to lay down these predetermined lists.
4. In addition, the applicant shall provide answers to the following questions:
- (a) whether the applicant is subject to any disease with epidemic potential as defined by the International Health Regulations of the World Health Organisation or other infectious or contagious parasitic diseases if such diseases are the subject of protection provisions applying to nationals of the Member States;
  - (b) whether he or she has ~~ever~~ been convicted of any criminal offence listed in the Annex over the previous ~~twenty~~ ten years and in the case of terrorist offences, over the previous twenty years, when and in which ~~any~~ country;
  - (c) whether he or she has stayed ~~regarding any stay~~ in a specific war or conflict zone over the ~~last~~ previous ten years and the reasons for the stay;
  - (d) whether he or she has been the subject of ~~regarding~~ any decision requiring him or her to leave the territory of a Member State or of any other country or whether he or she was subject to any return decision issued over the ~~last~~ previous ten years.
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 78 specifying the content and format of ~~those~~ the questions referred to in paragraph 4.

6. ~~The applicant shall provide answers to those questions.~~ Where the applicant answers affirmatively to any of the questions referred to in paragraph 4, he or she shall be required to provide answers to additional questions on the application form by selecting from a predetermined list of ~~aimed at collecting further information via providing answers to a predetermined list of questions.~~ The Commission shall be empowered to adopt delegated acts in accordance with Article 78 to lay down the content and format of those additional questions and the predetermined list of answers to those questions.
7. The data referred to in paragraphs 2 and 4 shall be introduced by the applicant in Latin alphabet characters ~~with~~ diacritics.
8. On submission of the application form, the ETIAS *Information System* shall collect the IP address from which the application form was submitted.

*Article 16*  
*Travel authorisation fee*

1. A travel authorisation fee of EUR 5 shall be paid by the applicant for each application.
2. The travel authorisation fee shall be waived for children under 12 ~~eighteen~~ years of age at the time of the application.
3. The travel authorisation fee shall be charged in euro.
4. The Commission shall be empowered to adopt delegated acts in accordance with Article 78 on the payment methods and process for the travel authorisation fee and on changes to the amount of that fee which shall take into account any increase in the costs referred to in Article 74.

## CHAPTER III

### Creation of the application file and examination of the application by the ETIAS Central System

#### *Article 17*

#### *Admissibility and creation of the application file*

1. The ETIAS *Central System* shall automatically verify whether, following submission of an application:
  - (a) all the fields of the application form are filled in and contain all the items referred to in Article 15(2) and (4),
  - (b) the travel authorisation fee has been collected.
2. When the application is deemed admissible pursuant to paragraph 1, the ETIAS Central System shall automatically create an application file without delay and assign it an application number.
3. Upon creation of the application file, the ETIAS Central System shall record and store the following data:
  - (a) the application number;
  - (b) status information, indicating that a travel authorisation has been requested;
  - (c) the personal data referred to in Article 15(2), ~~and (4)~~ and (6) including the three letter code of the country issuing the travel document;
  - (d) the data referred to in Article 15(~~8~~5);
  - (e) the date and the time the application form was submitted as well as a reference to the successful payment of the travel authorisation fee and the unique reference number of the payment.

4. Upon creation of the application file, the ETIAS Central System shall determine whether the applicant already has another application file in the ETIAS Central System by comparing the data referred to in Article 15(2)(a) with the personal data of the application files stored in the ETIAS Central System. In such a case, the ETIAS Central System shall link the new application file to any previous existing application file created for the same applicant.
5. Upon creation of the application file, the applicant shall immediately receive a notification via the email service:
  - (a) status information, acknowledging the submission of an application for travel authorisation; and
  - (b) the application number.

*Article 18*  
*Automated processing*

1. The application files shall be automatically processed by the ETIAS Central System to identify hit(s). The ETIAS Central System shall examine each application file individually.
2. The ETIAS Central System shall compare the relevant data referred to in Article 15(2)(a),(b), (c), (d),(f),(g), (ja) except in case of transit, (m) and (8) to the data present in a record, file or alert registered in the ETIAS Central System, the Schengen Information System (SIS), [the Entry/Exit System (EES)], the Visa Information System (VIS), [the Eurodac], [the European Criminal Records Information System (ECRIS)], the Europol data, the Interpol Stolen and Lost Travel Document database (SLTD), and the Interpol Travel Documents Associated with Notices database (Interpol TDAWN).

In particular, the ETIAS Central System shall verify:

- (a) whether the travel document used for the application corresponds to a travel document reported lost, stolen or invalidated in the SIS;

- (b) whether the travel document used for the application corresponds to a travel document reported lost, stolen or invalidated in the SLTD;
- (c) whether the applicant is subject to a refusal of entry alert recorded in the SIS;
- (d) whether the applicant is subject to an alert in respect of persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant or wanted for arrest for extradition purposes in the SIS;
- (e) whether the applicant and the travel document correspond to a refused, revoked or annulled ~~application for~~ travel authorisation in the ETIAS Central System;
- (f) whether the data provided in the application concerning the travel document correspond to another application for travel authorisation associated with different identity data referred to in Article 15(2)(a) in the ETIAS Central System;
- (g) [whether the applicant is currently reported as overstayer, whether he has been reported as overstayer in the past through consultation of the EES;]
- (h) [whether the applicant was refused entry through consultation of the EES;]
- (i) whether the applicant has been subject to a decision to refuse, revoke or annul a short stay visa recorded in the VIS;
- (j) whether the data provided in the application corresponds to data recorded in the Europol data;
- (k) [whether the applicant was subject to a return decision or a removal order issued following the withdrawal or rejection of the application for ~~internal~~ international protection in the Eurodac;]

- (l) [whether the applicant corresponds to a person whose data is recorded in the ECRIS;]<sup>36</sup>
- (m) whether the travel document used for the application corresponds to a travel document recorded in a file in the Interpol TDAWN;
- (n) in the case where an applicant is a minor, whether the applicant's parental authority or legal guardian:
- i) is subject to an alert in respect of persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant or wanted for arrest for extradition purposes in the SIS;
- ii) is subject to a refusal of entry alert recorded in the SIS.
3. The ETIAS Central System shall verify whether the applicant has replied affirmatively to any of the questions listed in Article 15(4) and whether the applicant has not provided a home address but only his city and country of residence, as referred to in Article 15(2)(f).
4. The ETIAS Central System shall compare the relevant data referred to in Article 15(2)(a), (b), ~~(c)~~, (d), (f), (g), (i), ~~(ja) except in case of transit~~, (k), (m) and (8) to the data present in the ETIAS watchlist referred to in Article 29.
5. The ETIAS Central System shall compare the relevant data referred to in Article 15(2)(a), ~~(c)~~, (f), (h), and (i), ~~(ja), (jb) and (jc)~~ and the specific risk indicators referred to in Article 28.
6. The ETIAS Central System shall add a reference to any hit obtained pursuant to paragraphs (2) to (5) to the application file.

---

<sup>36</sup> This wording will need to be adapted to specify that a hit will only be triggered in relation to terrorism and other serious criminal offences depending on the relevant proposal on ECRIS.

~~7. For the purposes of Article 4(e), the ETIAS Central System shall allow the comparison of the relevant data referred to in Article 15(2)(a),(b) and (d) to the data present in the SIS in order to determine whether the applicant is subject to one of the following alerts:~~

~~(a) an alert in respect of persons wanted for arrest for surrender purposes or extradition purposes;~~

~~(b) an alert in respect of missing persons;~~

~~(c) an alert in respect of persons sought to assist with a judicial procedure;~~

~~(d) an alert on persons and objects for discreet checks or specific checks.~~

~~Any hit resulting from this comparison shall be stored in the SIS.~~

8. Where the data recorded in the application file corresponds to the data triggering a hit pursuant to paragraphs 2 and 4, the ETIAS Central System shall identify, where relevant, the Member State(s) that entered or supplied the data having triggered the hit(s) and shall record this in the application file.

9. Following any hit pursuant to paragraphs (2)(j) and (4) and where no Member State had supplied the data having triggered the hit, the ETIAS Central System shall identify whether Europol entered the data and shall record this in the application file.

#### *Article 19*

#### *Results of the automated processing*

1. Where the automated processing laid down in Article 18(2) to (5) does not report any hit, the ETIAS Central System shall automatically issue a travel authorisation in accordance with Article 30 and shall ~~immediately~~ notify the applicant in accordance with Article 32.

1a. Where the automated processing laid down in Article 18(2) to (5) reports one or several hit(s), the application shall be assessed in accordance with the procedure laid down in Article 20.

2. ~~Where the automated processing laid down in Article 18(2) to (5) reports one or several hit(s),~~ Where the verification process laid down in Article 20 certifies that the data recorded in the application file corresponds to the data triggering a hit during the automated processing pursuant to Article 18(2) to (5) or where doubts remain concerning the identity of the applicant, the application shall be assessed in accordance with the procedure laid down in Article 22.
- 2a. Where the automated processing laid down in Article 18(3) reports that the applicant has replied affirmatively to any of the questions listed in Article 15(4), and if there is no other hit, the application shall be sent to the ETIAS National Unit of the responsible Member State for manual processing as set out in Article 22.
3. ~~Where the automated processing laid down in Article 18(2) to (5) is inconclusive because the ETIAS Central System is not in a position to certify that the data recorded in the application file correspond to the data triggering a hit, the application shall be assessed in accordance with the procedure laid down in Article 20.~~

#### *Article 20*

##### *Verification by the ETIAS Central Unit*

1. Where the automated processing pursuant to Article 18(2) to (5) reports one or several hit(s) the ETIAS Central System shall automatically consult the ETIAS Central Unit.
2. The ETIAS Central Unit shall have access to the application file and the linked application file(s), if any, as well as to all the hits triggered during the automated processing pursuant to Article 18(2) to (5) and to the information identified by the ETIAS Central System according to Article 18(8) and (9).
3. The ETIAS Central Unit shall verify whether the data recorded in the application file corresponds to the data present in one of the consulted information systems/databases, the ETIAS watchlist referred to in Article 29 or the specific risk indicators referred to in Article 28.

4. Where the data do not correspond, and no other hit has been reported during the automated processing pursuant to Article 18(2) to (5), the ETIAS Central Unit shall delete the false hit from the application file and the ETIAS Central System shall automatically issue a travel authorisation in accordance with Article 30.
5. Where the data correspond to or where doubts remain concerning the identity of the applicant, the application shall be assessed in accordance with the procedure laid down in Article 22.
6. The ETIAS Central Unit shall complete the manual examination within a maximum of 12 hours from receipt of the application file.

*Article 20a*

*Support of the objectives of the Schengen Information System*

1. For the purposes of Article 4(e), the ETIAS Central System shall compare the data referred to in Article 15(2)(a),(b) and (d) to the data present in the SIS in order to determine whether the applicant is subject to one of the following alerts:
  - (a) an alert on missing persons;
  - (b) an alert on persons sought to assist with a judicial procedure;
  - (c) an alert on persons for discreet checks, [inquiry checks] or specific checks.

2. Where the comparison referred to in paragraph 1 reports one or several hit(s) or where the applicant is subject to a SIS alert in respect of persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant or wanted for arrest for extradition purposes in accordance with Article 18(2)(d), the ETIAS Central System shall send an automated notification to the ETIAS Central Unit which shall verify whether the applicant personal data corresponds to the personal data contained in the alert having triggered that hit and upon confirmation, the ETIAS Central System shall send an automated notification to the SIRENE Bureau of the Member State that issued the alert. The ETIAS Central System shall also send an automated notification to the SIRENE Bureau of the Member State that issued an alert having triggered a hit against the SIS during the automated processing referred to in Article 18(a), (c) and (d), where, following verification by the ETIAS Central Unit as referred to in Article 20, such alert led to manual processing of the application in accordance with Article 22.
3. The notification provided to the SIRENE Bureau of the Member State that issued the alert shall contain the following data:
- (a) surname(s), first name(s) and, if any, alias;
  - (b) place and date of birth;
  - (c) sex;
  - (d) nationality(ies);
  - (e) address of the first intended stay or, in case of transit, Member State of first intended transit ~~entry~~;

- (f) travel authorisation status information, indicating whether a travel authorisation has been issued, refused or whether the application is subject to a manual assessment pursuant to Article 22;
- (g) a reference to the hit(s) obtained in accordance with paragraphs 1 and 2, including the date and time of the hit.

4. The ETIAS Central System shall add a reference to any hit obtained pursuant to paragraph (1) to the application file.

#### *Article 21*

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

1. For third country nationals referred to in Article 2(1)(c), the travel authorisation as defined in Article 3(d) shall be understood as a decision issued in accordance with this Regulation indicating 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 a security or public health risk in accordance with Directive 2004/38/EC.
2. When a third country national referred to in Article 2(1)(c) applies for a travel authorisation, the following specific rules shall apply:
  - (a) ~~the applicant shall provide the additional personal data referred to in Article 15(2)(1);~~
  - (b) the applicant shall not reply to the question referred to in Article 15(4)(d);
  - (c) the fee referred to in Article 16 shall be waived.

3. [When processing an application for a travel authorisation for a third country national referred to in Article 2(1)(c), the ETIAS Central Systems shall not verify whether:
- (a) the applicant is currently reported as an overstayer, or whether he or she has been reported as an overstayer in the past through consultation of the EES as referred to in Article 18(2)(g);
  - (b) the applicant corresponds to a person whose data is recorded in the Eurodac as referred to in Article 18(2)(~~j~~)(k).]

The specific risk indicators based on ~~irregular~~ illegal immigration risks determined pursuant to Article 28(~~2~~) shall not apply.

4. An application for a travel authorisation shall not be refused on the ground of an ~~irregular~~ illegal immigration risk as referred to in Article 31(1)(~~c~~)(b).
5. The following rules shall also apply:
- (a) in the notification laid down in Article 32(1) the applicant shall receive information regarding the fact that he or she needs to be able to prove when crossing the external border his or her status as family member of a citizen exercising the right of free movement as referred to in Article 15(2)(1), which shall also include a reminder that the family member of a citizen exercising the right of free movement who is in possession of a travel authorisation only has a right to enter if the family member accompanies or joins the citizen exercising its right of free movement;
  - (b) an appeal as referred to in Article 32 shall be made in accordance with Directive 2004/38/EC;

- (c) the retention period of the application file referred to in Article 47(1) shall be:
- i) the period of validity of the travel authorisation;
  - ii) [one year from the last entry record of the applicant stored in the EES, where that period of one year ends on a later date than the period of validity of the travel authorisation; or]
  - iii) five years from the last decision to refuse, revoke or annul the travel authorisation in accordance with Articles 31, 34 and 35.

## CHAPTER IV

### Examination of the application by the ETIAS National Units

#### *Article 21a* *Responsible Member State*

1. The Member State responsible for the manual processing of applications as referred to in Article 22 (the 'responsible Member State') shall be identified by the ETIAS Central System as follows:
  - (a) Where only one Member State is identified as having entered or supplied the data that triggered the hit pursuant to Article 18, that Member State shall be the responsible Member State.
  - (b) Where several Member States are identified as having entered or supplied the data that triggered the hits pursuant to Article 18, the Member State that has entered or supplied the most recent data corresponding to points (a) or (c) of Article 18(2), shall be the responsible Member State.
  - (c) Where several Member States are identified as having entered or supplied the data that triggered the hits pursuant to Article 18, but none of that data corresponds to points (a) and (c) of Article 18(2), the responsible Member State shall be the one that entered **or supplied** the most recent data.
  - (d) For the purposes of paragraphs (a) ~~to~~ and (c), hits triggered by data not entered or supplied by a Member State shall not be taken into account in order to identify the responsible Member State. Where the manual processing of an application is not triggered by data entered or supplied by a Member State, the responsible Member State shall be the Member State of first ~~entry~~ intended stay or, in case of transit if ~~no stay is intended~~, the Member State of first intended transit as declared by the applicant in accordance with Article 15(2)(j).
2. The ETIAS Central System shall indicate the Member State responsible in the application file.

*Article 22*  
*Manual processing of applications by the ETIAS National Units*

- ~~[1. The Member State responsible for the manual processing of applications pursuant to this Article (the 'responsible Member State') shall be the Member State of first entry as declared by the applicant in accordance with Article 15(2)(j).]~~
2. Where the automated processing laid down in Article 18(2) to (5) reported one or several hit(s), the application shall be processed manually by the ETIAS National Unit of the responsible Member State. ~~The~~ That ETIAS National Unit shall have access to the application file and the linked application file(s), if any, as well as to all the hits triggered during the automated processing laid down in Article 18(2) to (5). The ETIAS Central Unit shall inform the ETIAS National Unit of the responsible Member State whether one or several other Member States or Europol were identified as having entered or supplied the data that triggered the hit pursuant to Article 18(2) or (4). Where one or several Member States were identified as having entered or supplied the data that triggered such hit, the ETIAS Central Unit shall also specify the Member States concerned.
3. Following the manual processing of the application, the ETIAS National Unit of the responsible Member State shall:
- (a) issue a travel authorisation; or
  - (b) refuse a travel authorisation.
4. Where the automated processing laid down in Article 18(2) has reported a hit, the ETIAS National Unit of the responsible Member State shall:
- (a) where the hit corresponds to one or several of the categories laid down in Article 18(2)(a) ~~to~~ and (c), refuse a travel authorisation.
  - (b) where the hit corresponds to one or several of the categories laid down in Article 18(2)(b) and (d) to (m), assess the security or ~~irregular~~ illegal immigration risk and decide whether to issue or refuse a travel authorisation.

5. Where the automated processing laid down in Article 18(3) has reported that the applicant replied affirmatively to one of the questions referred to in Article 15(4), the ETIAS National Unit of the responsible Member State shall assess the security, irregular illegal immigration, security or public health risk and decide whether to issue or refuse a travel authorisation.
6. Where the automated processing laid down in Article 18(4) has reported a hit, the ETIAS National Unit of the responsible Member State shall assess the security risk and decide whether to issue or refuse a travel authorisation.
7. Where the automated processing laid down in Article 18(5) has reported a hit, the ETIAS National Unit of the responsible Member State shall assess the security, irregular illegal immigration, security or public health risk and decide whether to issue or refuse a travel authorisation.

### *Article 23*

#### *Request for additional information or documentation from the applicant*

1. Where the ETIAS National Unit of the responsible Member State deems the information provided by the applicant in the application form to be insufficient to enable it ~~does not~~ allow ~~the ETIAS National Unit of the responsible Member State~~ to decide whether to issue or refuse a travel authorisation, that ETIAS National Unit may request the applicant for additional information or documentation. The ETIAS National Unit of the responsible Member State shall request additional information or documentation upon request of a Member State consulted in accordance with Article 24.

2. The request for additional information or documentation shall be notified through the email service referred to in Article 6(2)(f) to the contact e-mail address recorded in the application file. The request for additional information or documentation shall clearly indicate the information or documentation that the applicant is required to provide, as well as a list of the languages in which the information or documentation may be submitted. That list shall include at least English or French or German unless it includes a language which is an official language of the third country which the applicant has declared to be a national of. Where additional documentation is requested, a copy of the original document(s) shall also be requested. ~~If the original document(s) are in one of the official languages of the EU, no translation shall be required.~~

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) within ~~7~~ 12 calendar working days ~~from~~ of the date of receipt of the request. The applicant shall provide such information or documentation in one of the languages notified in the request.

2a. For the purpose of requesting additional information or documentation as referred to in paragraph 1, the ETIAS National Unit shall use a predetermined list of options. The Commission shall be empowered to adopt delegated acts in accordance with Article 78 to lay down the content and format of that predetermined list of options.

~~3. The ETIAS National Unit shall process the additional information or documentation within 72 hours of the date of the submission by the applicant.~~

4. In exceptional circumstances, where the necessary arrangements have been made by the Member State concerned to enable this, the ETIAS National Unit of the responsible Member State may invite the applicant for an interview at a consulate in his or her country of residence.
5. The invitation shall be notified to the applicant by the ETIAS National Unit through the email service referred to in Article 6(2)(f) of the Member and ~~shall be notified~~ to the contact e-mail address recorded in the application file. Such notification shall take place within 84 96 hours from the lodging of an application which is admissible or 72 hours from the submission of the additional information or documentation pursuant to paragraph 2. The invitation shall include information as to the Member State issuing that invitation and the contact details of the consulate where the interview may take place. The interview shall take place within 40 8 calendar days from the notification of the invitation. The invitation shall be recorded in the application file by the ETIAS Central System.
6. ~~Where the applicant fails to reply to the invitation within the deadline or~~ Where the applicant fails to attend the interview following the notification of the invitation in accordance with paragraph 5, the application shall be refused in accordance with Article 31(1) and the ETIAS National Unit of the responsible Member State shall inform the applicant without delay.
- 6b. Upon submission of the additional information or documentation in accordance with paragraph 2, the ETIAS Central System shall record and store that information or documentation in the application file. Additional information or documentation provided during an interview in accordance with paragraph 5 shall be added to the application file by the ETIAS National Unit of the responsible Member State.
7. The ETIAS National Unit shall resume the examination of the application from the moment the applicant provides the additional information or documentation or, where applicable, from the date of the interview.

## Article 24

### Consultation of other Member States

1. ~~1. For the purpose of carrying out the assessment referred to in Article 22(4)(b) the ETIAS National Unit of the responsible Member State shall consult the authorities of the Member State(s) responsible for the data having triggered a hit pursuant to Article 18(2)(d),(e),(g),(h),(i) or (k). Where one or several Member States are identified as having entered or supplied the data having triggered a hit in accordance with Article 18(8), the ETIAS Central Unit shall notify the ETIAS National Unit of the Member State(s) involved, thereby launching a consultation process between them and the ETIAS National Unit of the responsible Member State.~~
2. ~~For the purpose of carrying out the assessment referred to in Article 22(4)(b), (6) and (7) the ETIAS National Unit of the responsible Member State may consult the authorities of one or several Member States.~~
3. ~~Where the responsible Member State consults with one or several Member States during the manual processing of an application, The ETIAS National Units of those the Member States consulted shall have access to the relevant data of the application file as well as to the hits obtained by the automated system pursuant to Article 18 (2), (4) and (5) which are necessary for the purpose of the consultation. The ETIAS National Units of the Member States consulted shall also have access to the relevant additional information or documentation provided by the applicant following a request from the responsible Member State in relation to the matter for which they are being consulted.~~
4. The ETIAS National Unit of the Member States consulted shall:
  - (a) provide a reasoned positive opinion on the application; or
  - (b) provide a reasoned negative opinion on the application.

The positive or negative opinion shall be recorded in the application file by the ETIAS National Unit of the Member State consulted.

5. ~~The ETIAS National Unit of the Member States consulted shall reply within 24 hours from the date of the notification of the consultation. The failure by Member States to reply within the deadline shall be considered as a positive opinion on the application.~~
6. The ETIAS National Unit of the responsible Member State may also consult the ETIAS National Units of one or several Member States following the reply of an applicant to a request for additional information. Where such additional information was requested on behalf of a consulted Member State pursuant to Article 23(1), the ETIAS National Unit of the responsible Member State shall consult the ETIAS National Unit of that consulted Member State following the reply of the applicant to that request for additional information. In such a cases, the ETIAS National Units of the Member States consulted shall also have access to the relevant additional information or documentation provided by the applicant following a request from the responsible Member State in relation to the matter for which they are being consulted. Where several Member States are consulted, the ETIAS National Unit of the responsible Member State shall ensure the coordination.
- 6a. ~~The ETIAS National Unit of the Member States consulted shall reply within 60 48 36 hours from the date of the notification of the consultation. The failure by Member States to reply within the deadline shall be considered as a positive opinion on the application.~~
7. During this consultation process, the consultation request and the replies thereto shall be transmitted through the software referred to in Article 6(2)(j) ETIAS Communication Infrastructure and shall be made available to the ETIAS National Unit of the responsible Member State.
8. Where one or several Member States consulted provide a negative opinion on the application, the responsible Member State shall refuse the travel authorisation pursuant to Article 31.

*Article 25*  
*Consultation of Europol*

1. ~~For the purpose of carrying out the assessment of security risks following a hit pursuant to Article 18(2)(j) and (4), the ETIAS National Unit of the responsible Member State shall consult Europol in cases falling under Europol's mandate. The consultation shall take place through existing communication channels between the Member State and Europol as established under Article 7 of Regulation (EU) 2016/794. Where Europol is identified as having supplied the data having triggered a hit in accordance with Article 18(9), the ETIAS Central Unit shall notify it, thereby launching a consultation process between Europol and the ETIAS National Unit of the responsible Member State. Such consultation shall take place without prejudice to Chapter IV of Regulation (EU) 2016/794.~~
2. ~~Where the responsible Member State consults Europol~~ is consulted, the ETIAS National Unit of that Member State ~~Central Unit~~ shall transmit to Europol the relevant data of the application file as well as the hit(s) which are necessary for the purpose of the consultation. ~~The ETIAS National Unit may transmit to Europol the relevant additional information or documentation provided by the applicant in relation to the request for travel authorisation for which Europol is consulted.~~
3. In any case, Europol shall not have access to the personal data concerning the education of the applicant as referred to in Article 15(2)(h) and the health of the applicant as referred to in Article 15(4)(a).
4. Where consulted in accordance with paragraph 1, Europol shall provide a reasoned opinion on the application. Europol's opinion shall be made available to the ETIAS National Unit of the responsible Member State which shall recorded it in the application file ~~by the responsible Member State.~~

- 4a. The ETIAS National Unit of the responsible Member State may consult Europol following the reply of an applicant to a request for additional information. In such a case, the ETIAS National Unit may transmit to Europol the relevant additional information or documentation provided by the applicant in relation to the request for travel authorisation for which Europol is consulted.
5. Europol shall reply within ~~24~~ ~~36~~ ~~48~~ 60 hours of the date of the notification of the consultation. The failure by Europol to reply within the deadline shall be considered as a positive opinion on the application.
- 5a. During this consultation process, the consultation request and the replies thereto shall be transmitted through the software referred to in Article 6(2)(j) and shall be made available to the ETIAS National Unit of the responsible Member State.
6. Where Europol provides a negative opinion on the application and the responsible Member State decides to issue the travel authorisation, the ETIAS National Unit shall justify its decision and shall record it in the application file.

*Article 26*  
*Deadlines for notification to the applicant*

Within ~~72~~ ~~84~~ 96 hours from the lodging of an application which is admissible in accordance with Article 17, the applicant shall receive a notification indicating:

- (a) whether his or her travel authorisation has been issued or refused, or
- (b) if that additional information or documentation is requested and/or (e) that the applicant is invited to an interview.

*Article 27*  
*Decision on the application*

1. Applications shall be decided on no later than ~~72~~ 84 96 hours after the lodging of an application which is admissible in accordance with Article 17.
2. Exceptionally, when a request for additional information or documentation is notified, or when the applicant is invited to an interview, the period laid down in paragraph 1 shall be extended and in accordance with Article 23. such application shall ~~in all cases~~ be decided on no later than ~~72~~ 84 96 hours after the submission of the additional information or documentation by the applicant or 84 48 hours after the interview.
3. Before expiry of the deadlines referred to in paragraphs 1 and 2 a decision shall be taken to:
  - (a) issue a travel authorisation in accordance with Article 30; or
  - (b) refuse a travel authorisation in accordance with Article 31.

## CHAPTER V

### The ETIAS screening rules and the ETIAS watchlist

#### Article 28

#### *The ETIAS screening rules*

1. ~~The ETIAS screening rules shall be an algorithm enabling the comparison between the data recorded in an application file of the ETIAS Central System and specific risk indicators pointing to irregular migration, security or public health risks. The ETIAS screening rules shall be registered in the ETIAS Central System.~~
2. The Commission shall be empowered to adopt an implementing delegated acts in accordance with the examination procedure referred to in Article 79(2) 78 to further identify specific risks relating to specify the security, irregular illegal immigration, security or public health risks shall be determined on the basis of:

  - (a) [statistics generated by the EES indicating abnormal rates of overstayers and refusals of entry for a specific group of travellers; ]
  - (b) statistics generated by the ETIAS in accordance with Article 73 indicating abnormal rates of refusals of travel authorisations due to an security, irregular illegal immigration; security or public health risk associated with a specific group of travellers;
  - (c) [statistics generated by the ETIAS in accordance with Article 73 and the EES indicating correlations between information collected through the application form and overstay or refusals of entry;]
  - (d) information provided by Member States concerning specific security risk indicators or threats identified by that Member State;

- (e) information provided by Member States concerning abnormal rates of overstayers and refusals of entry for a specific group of travellers for that Member State;
- (f) information concerning specific public health risks provided by Member States as well as epidemiological surveillance information and risk assessments provided by the European Centre for Disease Prevention and Control (ECDC).

~~The specific risks shall be reviewed at least every six months and, where necessary, a new delegated implementing act shall be adopted by the Commission in accordance with the examination procedure referred to in Article 79(2) 78.~~

~~3. The Commission shall be empowered to adopt delegated acts in accordance with Article 78 to further specify the irregular migration, security or public health risks referred to in paragraph 2.~~

4. Based on the risks determined in accordance with paragraph 2, the ETIAS Central Unit shall establish the specific risk indicators consisting of a combination of data including one or several of the following:

- (a) age range, sex, ~~current~~ nationality;
- (b) country and city of residence;
- (c) education level;
- (d) current occupation.

~~The specific risk indicators referred to in sub-paragraphs (a) to (d) may be combined with one or several of the following data:~~

~~(a) purpose of first intended stay;~~

~~(b) means of subsistence for the first intended stay and the return trip, and duration of the first intended stay.~~

5. The specific risk indicators shall be targeted and proportionate. They shall in no circumstances be based on a person's sex, race, ~~or~~ ethnic origin, ~~political opinions~~, religion ~~or or philosophical beliefs~~, ~~trade union membership~~, ~~sexual life~~ disability, age or sexual orientation.
6. The specific risk indicators shall be established ~~defined~~, modified, added and deleted by the ETIAS Central Unit after consultation of the ETIAS Screening Board.
7. The ETIAS screening rules shall be an algorithm enabling the comparison between the data recorded in an application file of the ETIAS Central System and specific risk indicators pointing to security, illegal immigration or public health risks in accordance with Article 18. The Central Unit shall register the ETIAS screening rules in the ETIAS Central System.

*Article 29*

*The ETIAS watchlist*

01. The ETIAS watchlist shall be hosted by Europol. The technical specifications shall be established by means of an implementing measure adopted in accordance with the examination procedure referred to in Article 79(2).
  1. The ETIAS watchlist shall consist of data related to persons who have committed or are suspected of having committed or taken part in a serious criminal offence or persons regarding whom there are factual indications or reasonable grounds to believe that they will commit serious criminal offences.
  2. The ETIAS watchlist shall contain information related to: ~~be established on the basis of:~~
    - (a) the United Nations list of war criminals
    - (b) ~~information related to~~ terrorist offences or other serious criminal offences provided by Member States;
    - (c) ~~information related to~~ terrorist offences or other serious criminal offences obtained by Europol through international cooperation.

- 2a. ~~Europol shall enter into the watchlist~~ The information referred to in paragraph 2(a) and (c) shall be entered into the watchlist by Europol, without prejudice to Regulation (EU) 2016/794 in relation to international cooperation. It ~~and~~ shall be responsible for each data element it enters. The ETIAS watchlist shall indicate, for each data element, the date and time of storing.
- 2b. ~~Member States shall enter into the watchlist~~ The information referred to in paragraph 2(b) shall be entered into the watchlist by Member States. They ~~and~~ shall be responsible for each data element they enter. The ETIAS watchlist shall indicate, for each data element, the date and time of storing and the Member State that entered it.
3. On the basis of the information referred to in paragraph 2 ~~and relevant Europol data~~, ~~Europol shall establish~~ the ETIAS watchlist shall be composed of items consisting of one or more of the following data elements:
- (a) surname, and, if available, first name(s), surname at birth, date of birth, place of birth, country of birth, sex, nationality;
  - (b) other names (alias(es), artistic name(s), usual name(s));
  - (c) ~~a~~ travel document(s) (type, number and country of issuance of the travel document(s));
  - (d) ~~home~~ address;
  - (e) e-mail address:
  - (ea) phone number;
  - (f) the name, e-mail address, mailing address, phone number of a firm or organization;
  - (g) IP address.

## 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~~ **consider** that the presence of the person on the territory of the Member States **will** pose a security, irregular illegal immigration, 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 flag to the travel authorisation it issues, recommending further or specific checks at the border crossing point. Such flag may also be attached upon the request of a consulted Member State. This flag shall only be visible to the border guards and it shall indicate the reason for such flag. The flag may shall be removed automatically by the border guard once the border guard check has been carried out the check and has entered registered the corresponding entry/exit record in the EES. In case of refusal of entry, the flag shall remain attached to the travel authorisation.
2. A travel authorisation shall be valid for three ~~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~~ used a lost, stolen or invalidated travel document ~~which is reported as lost, stolen or invalidated;~~
  - (b) poses ~~an irregular migration~~ security risk;
  - (c) poses ~~an illegal immigration~~ 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.
  
- (1a) 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, with reference to the situation obtaining at the time of the application.
  
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 and to be annulled where it becomes evident that the conditions for issuing it were not met at the time it was issued.
  
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 without delay:

  - (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 flag 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, by indicating the relevant ground from those listed ~~as laid down~~ in Article 31(1).

3. In addition to the data referred to in paragraphs 1 and 2, where a decision has been taken to issue or refuse a travel authorisation, the ETIAS National Unit of the responsible Member State shall also add the reasons for its final decision, unless that decision is a refusal based on a negative opinion from a consulted Member State.

*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) and (1a).
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 intended stay or, in the case of transit, Member State of first intended transit entry as declared by the applicant in accordance with Article 15(2)(j). That ETIAS National Unit shall assess the security risk and, if it shall revoke the travel authorisation where it concludes that the conditions for granting it are no longer met.
- 4a. Where a refusal of entry record concerning the holder of a valid travel authorisation justified by reasons B, G or I listed in Annex V, Part B of Regulation (EU) 2016/399 is entered in the EES, the ETIAS Central System shall transfer the application file to the ETIAS National Unit of the Member State having refused entry with a view to reassessing the security and illegal immigration risks. That ETIAS National Unit shall assess whether the conditions for granting the travel authorisation are still met, and if not, shall revoke the travel authorisation.

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. No appeal shall be possible against such revocation of a travel authorisation 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, by indicating the relevant ground from those listed 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 without delay:
  - (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 relevant ground(s) for annulment or revocation as laid down from those listed in Article 31(1) or that the travel authorisation was revoked at the request of the applicant as refererd 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. Where an application has been deemed admissible in accordance with Article 17, the Member State to which the third country national intends to travel a Member State may exceptionally issue a travel authorisation with limited territorial validity may be issued exceptionally, when the that Member State concerned considers it necessary on humanitarian grounds in accordance with national law, 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 the purposes of 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 his or her application number, 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.
3. ~~The Member State to which the third country national intends to travel may 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 and may set the deadline within which such additional information or documentation is to be submitted. 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, and shall indicate the languages in which the information or documentation may be submitted. That list shall include at least English or French or German unless it includes an official language of the third country of which the applicant has declared to be a national. 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). Upon submission of the additional information or documentation, the ETIAS Central System shall record and store that information or documentation in the application file.
4. A travel authorisation with limited territorial validity shall be valid only for the territory of the issuing Member State and for a maximum of ~~15~~ 90 days from the date of first entry on the basis of that authorisation ~~on which the authorisation was issued~~. It may be exceptionally valid for the territory of more than one Member State, subject to the consent of each such Member State through their ETIAS National Units.
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 which issued that authorisation:
- (a) status information indicating that ~~the~~ a 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.

Where an ETIAS National Unit issues a travel authorisation with limited territorial validity with no information or documentation having been submitted by the applicant, that ETIAS National Unit shall record and store appropriate information or documentation in the application file justifying that decision.

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,
  - (c) a clear indication of the territory on which the holder of that authorisation is entitled to travel and that he or she can only travel within that territory; and
  - (d) 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 carriers*

1. ~~In accordance with Article 26 of the Convention Implementing the Schengen Agreement~~  
Air carriers, sea carriers and international carriers transporting groups overland by coach 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. In case a travel authorisation has been issued with limited territorial validity in accordance with Article 38, the ETIAS Central System shall respond by indicating that the person has a valid travel authorisation and the Member State(s) for which that authorisation is valid, providing the carriers with an OK answer and an indication of the Member State(s) concerned. Carriers may store the information sent and the answer received in accordance with the applicable law.

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).

4. The carriers referred to in paragraph 1 shall be subject to the penalties provided for in accordance with Article 26(2) of the Convention Implementing the Schengen Agreement and Article 4 of Council Directive 2001/51/EC when they transport third country nationals who, although subject to the travel authorisation requirement, are not in possession of a valid travel authorisation.
5. If third country nationals are refused entry, any carrier which brought them to the external borders by air, sea and land shall be obliged to immediately assume responsibility for them again. At the request of the authorities competent to carry out the border checks, the carriers shall be obliged to return the third country nationals to the third country from which they were transported or to the third country which issued the travel document on which they travelled or to any other third country to which they are certain to be admitted.

*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 any part of the ETIAS Information System ~~or for other reasons related to its technical architecture that can be detected by eu-LISA beyond the carriers' control~~, the carriers shall be exempted of the obligation to verify the possession of a valid travel authorisation. Where such failure is detected by eu-LISA ~~In such cases of a failure of the ETIAS Information System~~, the ETIAS Central Unit shall notify the carriers. It shall also notify the carriers when the failure is remedied. Where such failure is detected by the carriers, they may notify the ETIAS Central Unit.
- 1a. ~~Penalties referred to in Article 39(4) 26(2) of the Convention Implementing the Schengen Acquis shall not be imposed on carriers in the cases referred to in this paragraph 1.~~
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).

## **CHAPTER VIII**

### **Use of ETIAS by border authorities at the external borders**

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

1. ~~For the sole purpose of verifying whether the person has a valid travel authorisation, the~~  
bBorder guards authorities competent for carrying out border checks at external border  
crossing points in accordance with Regulation (EU) 2016/399 shall be permitted to consult  
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
  - (a) whether or not the person has a valid travel authorisation, and in the case of a travel  
authorisation with limited territorial validity as referred to in Article 38, the Member  
State(s) for which it is valid;
  
  - (b) any flag referred to in Article 30(1a) attached to that application file;
  
  - (c) whether the travel authorisation will expire within the next 90 days and the  
remaining validity period;
  
  - (d) the data referred to in Article 15(2)(k) and (l);
  
  - (e) at the first entry, the address for the first intended stay and the data referred to in  
Article 15(2)(ja), (jb) and (je).
  
3. Where additional verifications are needed for the purpose of a thorough second line check  
in accordance with Article 2(13) of Regulation (EU) N°2016/399, border guards shall be  
given access to the data referred to in Article 15(2)(a) to (g) and (i) to (m), and in Article  
15(4)(b) to (d) 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.

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 National Units of the Member States 's authorities competent for carrying out checks at external border crossing points shall be notified by the ETIAS Central Unit and shall ensure that their border guards competent for carrying out border checks are informed.
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 National Unit ~~competent authority~~ shall notify ~~eu-LISA~~, the ETIAS Central Unit. The ETIAS Central Unit shall then immediately inform eu-LISA 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.
- 3a. Model contingency plans for cases referred to in paragraphs 1 and 2 shall be adopted by the Commission by means of implementing acts in accordance with the examination procedure referred to in Article 79(2). Member States may draw up their national contingency plans on the basis of the model contingency plans, adapted as necessary at the national level.

## **Chapter VIIIa**

### **Use of ETIAS by immigration authorities**

#### *Article 42a*

##### *Access to data by immigration authorities*

1. For the purpose of checking or verifying if the conditions for entry or stay on the territory of the Member States are fulfilled and for the purpose of taking appropriate measures relating thereto, 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, and in the case of a travel authorisation with limited territorial validity as referred to in Article 38, the Member State(s) for which the authorisation is valid. The ETIAS Central System shall also indicate whether the travel authorisation will expire within the next 90 days and the remaining validity period. The Immigration Authorities shall also have access to the information referred to in Article 15(2)(f) and (g) and the relevant additional documentation or information. This shall not include information on whether or not the applicant may pose a public health risk as referred to in Article 15(4)(a). ~~submitted pursuant to Article 23.~~

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(2)(k).

## CHAPTER IX

### **Procedure and conditions for access to the ETIAS Central System ~~for~~ by designated authorities in order to prevent, detect and investigate ~~terrorist offences or other serious criminal offences 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~~ operating 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 in order to prevent, detect and investigate terrorist offences or other serious criminal offences for law enforcement purposes*

1. ~~The competent authorities~~ operational operating 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)~~. 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~~ operational operating 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) and, if available, 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;
  - (ee) ~~œ~~ phone number or mobile 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 ~~operational~~ 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 [five years from the last entry/exit record of the applicant stored in the EES; ~~or~~.
  - (a) Where the travel authorisation is not used, the application file shall be stored for the period of validity of the travel authorisation.
  - (b)
  - (c) Where the travel authorisation has been refused, revoked or annulled, the application file shall be stored for 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)~~ (c), 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.~~

- 5a. Where a third country national has fallen under the scope of Article 2(2)(d) or (e), he or she may inform the competent authorities of the Member State that issued that ~~long-stay visa or~~ residence permit, uniform visa or long-stay visa that he or she has a valid travel authorisation and may request the deletion of the application file from the ETIAS Central System. The authorities of that Member State shall verify whether that person has a valid travel authorisation and, ~~where relevant,~~ if confirmed, the ETIAS National Unit of the Member State that issued the residence permit, uniform visa or long stay visa shall delete the application file without delay from the ETIAS Central System.
6. Where a third country national has fallen under the scope of Article 2(2)(f) ~~to (h)~~, he or she ~~shall~~ may 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, the border guards competent for carrying out border checks and the immigration authorities. Where the processing of personal data by the ETIAS National Units falls within the scope of [Directive (EU) 2016/680], this Directive shall apply.
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(e)~~(d)~~ 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.

- 3a. A model security plan and a model business continuity and disaster recovery plan shall be adopted by the Commission by means of implementing acts in accordance with the examination procedure referred to in Article 79(2). eu-LISA, the ETIAS Central Unit and the ETIAS National Units shall adopt their business continuity and disaster recovery national plans as referred to in paragraph 3 on the basis of these model plans, adjusted as necessary by eu-LISA, the ETIAS Central Unit and the ETIAS National Units.
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 as soon as possible.

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 illegal immigration, 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, upon request.

#### *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, except insofar as necessary for the purpose of fair trial.

- 2a. By way of derogation from paragraph 1, the data accessed from the ETIAS Central System by the immigration authorities pursuant to Article 42a(2) may be transferred to a third country in individual cases, if necessary 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 45(3) of [Regulation 2016/679] ~~25(6)~~ of Directive 95/46/EC, or a readmission agreement or any other type of similar arrangement is in force between the European Union or a Member State and that third country, or Article 49(1)(d) ~~(e)~~ of [Regulation 2016/679] ~~26(1)(d)~~ of Directive 95/46/EC applies;
  - (b) the Member State shall inform the third country of the obligation to use the data only for purposes for which it was provided;
  - (c) the data is transferred or made available in accordance with the relevant provisions of Union law, in particular readmission agreements and transfer of personal data, 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.
3. Transfers of personal data to third countries pursuant to paragraph 2a shall not prejudice the rights of applicants for and beneficiaries of international protection, in particular as regards non-refoulement.

4. By way of derogation from paragraph 2, the data from the ETIAS Central System accessed by the designated authorities for the purposes referred to in Article 1(2) may be transferred or made available by the designated authority to a third country upon a duly motivated request, only if the following cumulative conditions are met:

(a) in an exceptional case of urgency, where there is an immediate and serious threat of a terrorist offence or other serious criminal offences as defined respectively under Article 3(1)(m) and (n) of this Regulation,

(b) the transfer is carried out in accordance with the applicable conditions set under Directive (EU) N0 2016/680,

(c) the reciprocal provision of any information held by the requesting third country, in the framework of systems for travel authorisation, to the Member States is ensured.

Where a transfer is based on this paragraph, such a transfer shall be documented and the documentation shall be made available to the supervisory authority on request, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.

#### *Article 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 border checks at external border crossing points and access by immigration authorities~~ referred to in Article 39, ~~and 41 and 42a~~. 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 in order to prevent, detect and investigate terrorist offences or other serious criminal offences 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 must fulfill the entry conditions as set out in Article 6 of Regulation (EU) N°2016/399 and are requested to present proof that they fulfil ~~the entry~~ those 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 Article 64(1) 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 in cooperation with the MS Member States 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, and the National Uniform Interfaces., ~~which~~ These 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).

eu-LISA shall develop a technical solution referred to in Article 81(8) as soon as possible after the entry into force of this Regulation and after the adoption by the Commission of the measures provided for in Article 81(8).

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 regularly and at least three times per quarter ~~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.

4. eu-LISA shall develop and maintain a mechanism and procedures for carrying out quality checks on the data in the ETIAS Central System and shall provide regular reports to the Member States and the ETIAS Central Unit. eu-LISA shall provide a regular report to the Commission covering the issues encountered. This mechanism, procedures and interpretation of data quality compliance shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 79(2).

*Article 65*

*Responsibilities of the European ~~Coast~~ Border and ~~Border~~ Coast Guard Agency*

1. The European ~~Coast~~ Border and ~~Border~~ Coast 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 preventing, detecting and investigating terrorist offences or other serious criminal offences ~~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 development and hosting ~~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.
4. Europol shall be responsible for providing information to the ETIAS watchlist related to terrorist offences or other serious criminal offences obtained by Europol through international cooperation pursuant to Article 29(2)(c).

## **CHAPTER XIV**

### **Amendments to other Union instruments**

#### Article 67a

#### 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, [the Entry/Exit System (EES)] and the European Travel Information and Authorisation System (ETIAS).

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

#### "Article 5b

#### Tasks relating to the ETIAS

In relation to ETIAS, 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 European Travel Information and Authorisation System (ETIAS) and determining the conditions for access to the ETIAS for law enforcement purposes;

(b) tasks relating to training on the technical use of ETIAS."

(3) Article 7 is amended as follows:

(a) paragraph 5 and 6 are is 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, [EES] or ETIAS 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, [EES] and ETIAS, 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], ETIAS and other large-scale information systems".

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

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

"(sb) adopt the reports on the development of the ETIAS pursuant to Article 81(2) of Regulation (EU) XX/XX of XXX".

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

"(t) adopt the reports on the technical functioning of SIS II pursuant to Article 50(4) of Regulation (EC) No 1987/2006 and Article 66(4) of Decision 2007/533/JHA respectively, of VIS pursuant to Article 50(3) of Regulation (EC) No 767/2008 and Article 17(3) of Decision 2008/633/JHA, [of EES pursuant to Article 64(4) of Regulation (EU) XX/XX of XXX] and of ETIAS pursuant to Article 81(4) of Regulation (EU) XX/XX of XXX."

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

"(v) make comments on the European Data Protection Supervisor's reports on the audits pursuant to Article 45(2) of Regulation (EC) No 1987/2006, Article 42(2) of Regulation (EC) No 767/2008, Article 31(2) of Regulation (EU) No 603/2013, [Article 50(2) of Regulation (EU) XX/XX of XXX] and Article 57 of Regulation (EU) XX/XX of XXX [ETIAS] and ensure appropriate follow-up of those audits".

(d) a new point (xb) is inserted after point x:

"(xb) publish statistics related to ETIAS pursuant to Article 73 of Regulation (EU) No XXXX/XX.

(e) a new point (zb) is added to point z:

"(zb) ensure annual publication of the list of competent authorities pursuant to Article 11(5) 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], or a question concerning ETIAS in relation to the application of Regulation (EU) XX/XX of XXX is on the agenda. The European Border and Coast Guard Agency may also attend the meetings of the Management Board as observer when a question concerning ETIAS 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, [Article 34(4) of Regulation (EU) XX/XX of XXX.] and Article 64(2) of Regulation (EU) XX/XX of XXX.”

(8) In Article 17 paragraph 6, point (ha) is added:

(ha) reports [on the development of the EES referred to in Article 64(2) of Regulation XX/XX (establishing the EES)] and on the development of ETIAS referred to in Article 81(2) of Regulation (EU) XX/XX (establishing ETIAS) and submitting them to the Management Board for adoption:

(9) 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.~~

(d) [EES-]ETIAS Advisory Group.”

(b) paragraph (3) is replaced by the following:

“3. Europol and Eurojust may each appoint a representative to the SIS II Advisory Group. Europol may also appoint a representative to the VIS, Eurodac, [EES-] and ETIAS Advisory Groups. The European Border and Coast Guard Agency may also appoint a representative to the [EES-]ETIAS Advisory Group”.

*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."

4. In Annex VI, the second subparagraph of point 2.1.3 is replaced by the following:

"Member State shall ensure that the airport operator takes the necessary measures to prevent unauthorised persons entering and leaving the reserved areas, for example, the transit areas. Checks will normally not be carried out in the transit area, unless it is justified on the basis of an assessment of the risk related to internal security and illegal immigration; in particular, checks in this area may be carried out on persons subject to an airport transit visa or a travel authorisation order to check that they are in possession of such a visa or travel authorisation."

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

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

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 setting-up and operation ~~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 competent for carrying out border checks 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 competent for carrying out border checks 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~~. The 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 as referred to in Article 38, 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;
  - (j) IP address.

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 illegal immigration, 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 revenues generated by ETIAS 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 ~~internal~~ ~~external~~ assigned revenue in accordance with Article 21(4) of Regulation (EU, EURATOM) No 966/2012. ~~They shall be assigned to cover the costs of the operation of the ETIAS. Operation costs of the ETIAS including maintenance costs and other operational costs for Member States shall be fully covered by the fee revenue referred to in Article 16. The revenues needed to cover operation costs generated by the ETIAS shall constitute external assigned revenue in accordance with Article 21(4) of Regulation (EU, EURATOM) No 966/2012. If the fee revenue exceeds the operation costs of ETIAS, the surplus shall be entered into the general budget of the Union. The budget authority shall re-examine on a yearly basis the revenue generated from ETIAS and the level of operational costs.~~

## 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 ~~(4)(6)~~, Article 16(4), Article 23(2a) ~~28(3)(1)~~ and Article 72(1) and ~~(5)(4)~~ shall be conferred on the Commission for ~~an indeterminate~~ a period of five years from [*the date of entry into force of this Regulation*]. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.
3. The delegation of power referred to in Article 15(3), (5) and ~~(4)(6)~~, Article 16(4), Article 23(2a) ~~28(3)(1)~~ and Article 72(1) and ~~(5)(4)~~ 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.
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~~)(1) and Article 72(1) and ~~(5)~~(4) 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, **including the impact of the travel authorisation requirement for the purpose of airport transit, in relation to the objectives of the ETIAS and taking into account the economic impact of this requirement**;
  - (c) the rules of the automated application processes~~es~~ 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~~ the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences, 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 in order to prevent, detect and investigate terrorist offences or other serious criminal offences ~~for law enforcement purposes~~;
- (d) the number and type of cases which have ended in hits ~~successful identifications~~;
- (e) the need and use made of the ~~exceptional case of~~ urgency procedure referred to in Article 44(4) including those cases where that urgency was not accepted by the ex post verification carried out by the central access point in accordance with Article 44(5).

~~The specifications for~~ A technical solution shall ~~to~~ be made available to Member States in order to facilitate the collection of this data pursuant to Chapter IX for the purpose of generating statistics referred to in this paragraph. The specifications shall be adopted by the Commission by means of implementing acts in accordance with the examination procedure referred to in Article 79(2).

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

*Article 81a*  
*Practical Handbook*

The Commission shall, in close cooperation with the Member States and the relevant Union Agencies, make available a practical handbook, which shall contain guidelines, recommendations and best practices for the implementation of this Regulation, **also taking into account relevant existing handbooks**. The Commission shall adopt the handbook in the form of a recommendation.

*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*

*For the Council*

*The President*

*The President*

---

**List of offences referred to in Article 15(4)(b)**

0. terrorist offences

1. participation in a criminal organisation,
2. trafficking in human beings,
3. sexual exploitation of children and child pornography,
4. illicit trafficking in narcotic drugs and psychotropic substances,
5. illicit trafficking in weapons, munitions and explosives,
6. corruption,
7. fraud, including that against the financial interests of the Union,
8. laundering of the proceeds of crime and counterfeiting of currency, including the euro,
9. computer-related crime/cybercrime,
10. environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties,
11. facilitation of unauthorised entry and residence,
12. murder, grievous bodily injury,
13. illicit trade in human organs and tissue,
14. kidnapping, illegal restraint and hostage-taking,
15. organised and armed robbery,

16. illicit trafficking in cultural goods, including antiques and works of art,
  17. counterfeiting and piracy of products,
  18. forgery of administrative documents and trafficking therein,
  19. illicit trafficking in hormonal substances and other growth promoters,
  20. illicit trafficking in nuclear or radioactive materials,
  21. rape,
  22. crimes within the jurisdiction of the International Criminal Court,
  23. unlawful seizure of aircraft/ships,
  24. sabotage,
  25. trafficking in stolen vehicles,
  26. industrial espionage,
  27. arson,
  28. racism and xenophobia.
-