I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2018/1240 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 12 September 2018

establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226

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 points (b) and (d) of Article 77(2) and point (a) of Article 87(2) thereof,

Having regard to the proposal from the European Commission,

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

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

Acting in accordance with the ordinary legislative procedure [2],

Whereas:

(1) The Communication of the Commission of 6 April 2016 entitled 'Stronger and Smarter Information Systems for Borders and Security' outlined the need for the Union 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. Among them are 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 was to launch a study on the feasibility of establishing a European Travel Information and Authorisation System (ETIAS). The feasibility study was completed in November 2016. The 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, illegal immigration or high epidemic 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' confirms the priority of securing external borders and presents concrete initiatives to accelerate and broaden the Union's response in continuing to strengthen the management of external borders.

[1] OJ C 246, 28.7.2017, p. 28.

[2] Position of the European Parliament of 5 July 2018 (not yet published in the Official Journal) and decision of the Council of 5 September 2018.

(4) It is necessary to specify the objectives of ETIAS, to define its technical and organisational architecture, to lay down rules concerning the operation and the use of the data to be entered into the system by the applicant and rules on the issue 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 the protection of personal data.

(5) ETIAS should apply to third-country nationals who are exempt from the 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 of the European Parliament and of the Council ([1]) applies or of a national of a third country enjoying the right of free movement equivalent to that of Union citizens under an agreement between the Union and its Member States on the one hand and a third country on the other and who do not hold a residence card pursuant to Directive 2004/38/EC or a residence permit pursuant to Council Regulation (EC) No 1030/2002 ([2]). Article 21(1) of the Treaty on the Functioning of the European Union (TFEU) 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.

(7) As confirmed by the Court of Justice ([3]), such family members have the right to enter the territory of the Member States and to obtain an entry visa for that purpose. Consequently, 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 should 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 as these are relevant for assessment of the security threat they could represent. Similarly, examination of their travel authorisation applications should be made exclusively against security concerns, and not those related to migration risks.

(9) ETIAS should provide a travel authorisation for third-country nationals exempt from the visa requirement enabling consideration of whether their presence on the territory of the Member States does not pose or will not pose a security, illegal immigration or a high epidemic risk. A travel authorisation should therefore constitute a decision indicating that there are no factual indications or reasonable grounds to consider that the presence of a person on the territory of the Member States poses such risks. As such, a travel authorisation is by its nature distinct from a visa; it will not require more information or place a heavier burden on applicants than a visa does. Holding a valid travel authorisation should be a new entry condition for the territory of the Member States. Mere possession of a travel authorisation should not, however, confer an automatic right of entry.

(10) ETIAS should contribute to a high level of security, to the prevention of illegal immigration and to the protection of public health by providing an assessment of visitors prior to their arrival at the external border crossing points.

(11) ETIAS should contribute to the facilitation of border checks performed by border guards at the external border crossing points. It should also ensure a coordinated and harmonised assessment of third-country nationals subject to the travel authorisation requirement who intend to travel to Member States. Furthermore, it should enable applicants to be better informed of their eligibility to travel to Member States. In addition, ETIAS should contribute to the facilitation of border checks by reducing the number of refusals of entry at the external borders and by providing border guards with certain additional information related to flags.

([1]) Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (OJ L 158, 30.4.2004, p. 77).

([2]) Council Regulation (EC) No 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third-country nationals (OJ L 157, 15.6.2002, p. 1).

([3]) Judgment of the Court of Justice of 31 January 2006, *Commission v Spain*, C-503/03, ECLI:EU:C:2006:74.

(12) ETIAS should also support the objectives of the Schengen Information System (SIS) related to alerts on third-country nationals subject to a refusal of entry and stay, on persons wanted for arrest for surrender purposes or extradition purposes, on missing persons, on persons sought to assist with a judicial procedure and on persons for discreet checks or specific checks. For this purpose, ETIAS should compare relevant data from application files against relevant alerts in SIS. Where the comparison reveals a correspondence between personal data in the application file and alerts on third-country nationals subject to a refusal of entry and stay or on persons wanted for arrest for surrender purposes or extradition purposes, the application file should be processed manually by the ETIAS National Unit of the Member State responsible. The assessment performed by the ETIAS National Unit should lead to a decision whether to issue a travel authorisation or not. Where the comparison reveals a correspondence between personal data in the application file and alerts on missing persons, on persons sought to assist with a judicial procedure and on persons for discreet checks or specific checks, this information should be transferred to the SIRENE bureau and should be dealt with in accordance with the relevant legislation relating to SIS.

(13) The conditions for issuing a travel authorisation should be coherent with the specific objectives associated with the different types of alerts recorded in SIS. In particular, the fact that applicants would be subject to an alert on persons wanted for arrest for surrender purposes or extradition purposes or to an alert on persons for discreet checks or specific checks should not prevent them from being issued with a travel authorisation with a view to Member States taking appropriate action in accordance with Council Decision 2007/533/JHA ([1]).

(14) ETIAS should consist of a large-scale information system, the ETIAS Information System, the ETIAS Central Unit and the ETIAS National Units.

(15) The ETIAS Central Unit should be part of the European Border and Coast Guard Agency. The ETIAS Central Unit should be responsible for verifying, in cases where the automated application process has reported a hit, whether the applicant's personal data correspond to the personal data of the person having triggered that hit. Where a hit is confirmed or where doubts remain, the ETIAS Central Unit should initiate the manual processing of the application. It should ensure that the data it enters in the applications files are up to date and define, establish, assess *ex ante*, implement, evaluate *ex post*, revise and delete the specific risk indicators, ensuring that the verifications that are performed and their results are recorded in the application files. It should also carry out regular audits of the processing of applications and of the implementation of the ETIAS screening rules, including by regularly assessing their impact on fundamental rights, in particular with regard to privacy and personal data protection. It should furthermore be responsible for fulfilling a number of support tasks such as ensuring the necessary notifications are sent and providing information and support. It should be operational 24 hours a day, 7 days a week.

(16) Each Member State should establish an ETIAS National Unit responsible for examining applications and deciding whether to issue or refuse, annul or revoke travel authorisations. The ETIAS National Units should cooperate with each other and with the European Union Agency for Law Enforcement Cooperation (Europol) for the purpose of assessing applications. The ETIAS National Units should be provided with adequate resources to fulfil their tasks in accordance with the deadlines set out in this Regulation. In order to facilitate the decision-making process and the exchange of information between Member States and to reduce translation costs and response times, it is preferable that all ETIAS National Units communicate in a single language.

(17) To meet its objectives, 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, level of education and job group, any status he or she holds of family member to Union citizens or third-country nationals enjoying the right of free movement and not holding a residence card pursuant to Directive 2004/38/EC or a residence permit pursuant to Regulation (EC) No 1030/2002, where the applicant is minor, details of the person responsible for him or her, and answers to a set of background questions.

(18) ETIAS should accept applications introduced on behalf of the applicant for travellers who are themselves not in a position to create an application, for whatever reason. In such cases, the application should be submitted by a third party authorised by the traveller or legally responsible for him or her, provided this person's identity is included in

([1]) Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007, p. 63).

the application form. It should be possible for travellers to authorise commercial intermediaries to create and submit an application on their behalf. The ETIAS Central Unit should act upon any reports of abuses by commercial intermediaries appropriately.

(19) Parameters for ensuring the completeness of an application and the coherence of the data submitted should be established to verify the admissibility of applications for a travel authorisation. For instance, such verification should preclude the use of travel documents which will expire in less than three months, have expired or were issued more than 10 years previously. The verification should be undertaken before the applicant is invited to pay the fee.

(20) In order to finalise the application, applicants should be required to pay a travel authorisation fee. The payment should be managed by a bank or a financial intermediary. The data required for securing the electronic payment should only be provided to the bank or financial intermediary operating the financial transaction and not form part of data stored in ETIAS.

(21) Most of the travel authorisations should be issued within minutes, though a reduced number could require longer, especially in exceptional cases. In such exceptional cases, it may be necessary to request additional information or documentation from the applicant, to process that additional information or documentation and, following examination of the information or documentation provided by the applicant, to invite him or her to an interview. Interviews should only be conducted in exceptional circumstances, as a last resort and when serious doubts remain regarding the information or documentation provided by the applicant. The exceptional nature of interviews should lead to less than 0,1 % of applicants being invited to an interview. The number of applicants invited to an interview should be subject to regular review by the Commission.

(22) The personal data provided by the applicant should be processed by ETIAS for the sole purposes of assessing whether the entry of the applicant into the Union could pose a security, illegal immigration or high epidemic risk in the Union.

(23) The assessment of such risks cannot be carried out without processing the personal data to be provided in a travel authorisation application. The personal data in the applications should be compared with the data present in a record, file or alert registered in an EU information system or database (the ETIAS Central System, SIS, the Visa Information System (VIS), the Entry/Exit System (EES) or Eurodac), in Europol data or in the Interpol databases (the Interpol Stolen and Lost Travel Document database (SLTD) or the Interpol Travel Documents Associated with Notices database (TDAWN)). The personal data in the applications should also be compared against the ETIAS watchlist and 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 those EU information systems that are consulted, in Europol data, in Interpol databases, in the ETIAS watchlist or in the specific risk indicators.

(24) The comparison should take place by automated means. Whenever such comparison reveals that a correspondence (a 'hit') exists between any of the personal data or combination thereof in the application and the specific risk indicators or the personal data either in a record, file or alert in the above information systems or in the ETIAS watchlist, the application should be processed manually by the ETIAS National Unit of the Member State responsible. The assessment performed by the ETIAS National Unit should lead to the decision to issue the travel authorisation or not to do so.

(25) It is expected that the vast majority of applications will obtain a positive answer by automated means. No refusal, annulment or revocation of a travel authorisation should be based only on the automated processing of personal data in the applications. For this reason, the applications generating a hit should be processed manually by an ETIAS National Unit.

(26) 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.

(27) The ETIAS screening rules should be used to analyse an application file by enabling a comparison between the data recorded in it and specific risk indicators corresponding to previously identified security, illegal immigration or high epidemic risks. The criteria used for defining the specific risk indicators should in no circumstances be based

solely on a person's sex or age. They should also in no circumstances be based on information revealing a person's colour, race, ethnic or social origin, genetic features, language, political or any other opinion, religion or philosophical belief, trade union membership, membership of a national minority, property, birth, disability, or sexual orientation. The specific risk indicators should be defined, established, assessed *ex ante*, implemented, evaluated *ex post*, revised and deleted by the ETIAS Central Unit following consultation of an ETIAS screening board composed of representatives of the ETIAS National Units and the agencies involved. To help ensure the respect of fundamental rights in the implementation of the ETIAS screening rules and specific risk indicators, an ETIAS Fundamental Rights Guidance Board should be established. The secretariat for its meetings should be provided by the Fundamental Rights Officer of the European Border and Coast Guard Agency.

(28) An ETIAS watchlist should be established for the purposes of identifying connections between data in an application file and information related to persons who are suspected of having committed or having taken part in a terrorist offence or other serious criminal offence or regarding whom there are factual indications or reasonable grounds, based on an overall assessment of a person, to believe that they will commit a terrorist offence or other serious criminal offences. The ETIAS watchlist should form part of the ETIAS Central System. Data should be entered into the ETIAS watchlist by Europol, without prejudice to the relevant provisions on international cooperation in Regulation (EU) 2016/794 of the European Parliament and of the Council [1], and by Member States. Before entering data into the ETIAS watchlist, it should be determined that the data are adequate, accurate and important enough to be included in the ETIAS watchlist and that their entry would not lead to a disproportionate number of applications being processed manually. The data should be regularly reviewed and verified to ensure their continued accuracy.

(29) The continuous emergence of new forms of security threats, new patterns of illegal immigration and high epidemic risks requires effective responses using modern means. Since these means often involve the processing of significant 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.

(30) Personal data in ETIAS should therefore be kept secure. Access to them should be limited to strictly authorised personnel. In no circumstances should access be used to reach decisions based on any form of discrimination. The personal data stored should be kept securely in the facilities of the European Agency for the operational management of large-scale information systems in the area of freedom, security and justice (eu-LISA) in the Union.

(31) Issued travel authorisations should be annulled or revoked as soon as it becomes evident that the conditions for issuing them were not or are no longer met. In particular, where a new alert for refusal of entry and stay or an alert reporting a travel document as lost, stolen, misappropriated or invalidated is entered in SIS, SIS should inform ETIAS. ETIAS should then verify whether this new alert corresponds to a valid travel authorisation. Where a new refusal of entry and stay alert has been issued, the ETIAS National Unit of the Member State responsible should revoke the travel authorisation. Where the travel authorisation is linked to a travel document reported as lost, stolen, misappropriated or invalidated in SIS, or reported as lost, stolen or invalidated in SLTD, the ETIAS National Unit of the Member State responsible should manually process the application file. Following a similar approach, new data entered into the ETIAS watchlist should be compared with the application files stored in ETIAS in order to verify whether those new data correspond to a valid travel authorisation. In such cases, the ETIAS National Unit of the Member State that entered the new data, or the Member State of first intended stay in the case of data entered by Europol, should assess the hit and, where necessary, revoke the travel authorisation. It should also be possible to revoke a travel authorisation at the request of the applicant.

(32) 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 valid only for a limited territory and period.

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

(33) Prior to boarding, air and sea carriers and international carriers transporting groups overland by coach should have the obligation to verify that travellers are in possession of a valid travel authorisation. The ETIAS file itself should not be accessible to carriers. Carriers should have secure access to the ETIAS Information System to allow them to consult it using travel document data.

(34) The technical specifications for accessing the ETIAS Information System through the carrier gateway should limit the impact on passenger travel and carriers to the extent possible. For this purpose, integration with the EES should be considered.

(35) With a view to limiting the impact of the obligations set out in this Regulation on international carriers transporting groups overland by coach, user-friendly mobile solutions should be made available.

(36) Within two years following the start of operations of ETIAS, the appropriateness, compatibility and coherence of provisions referred to in Article 26 of the 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 ([1]) for the purposes of the ETIAS provisions for overland transport by coaches should be assessed by the Commission. The recent evolution of overland transport by coaches should be taken into account. The need for amending provisions concerning overland transport by coaches referred to in Article 26 of that Convention or this Regulation should be considered.

(37) In order to ensure compliance with the revised conditions for entry, border guards should check whether travellers are in possession of a valid travel authorisation. Therefore, during the standard border check process, border guards should read travel document data electronically. This operation should trigger a query in different databases as provided under the Regulation (EU) 2016/399 of the European Parliament and of the Council ([2]) (Schengen Borders Code), including a query in ETIAS which should provide the up-to-date travel authorisation status. If there is no valid travel authorisation, the border guard should refuse entry and should complete the border check process accordingly. If there is a valid travel authorisation, the decision to authorise or refuse entry should be taken by the border guard. Certain data in the ETIAS file should be accessible to border guards to assist them in carrying out their tasks.

(38) Where the ETIAS National Unit of the Member State responsible considers that some aspects of the application for a travel authorisation deserve further examination by the border authorities, it should be able to attach a flag to the travel authorisation it issues, recommending a second line check at the border crossing point. It should also be possible for such a flag to be attached at the request of a consulted Member State. Where the ETIAS National Unit of the Member State responsible considers that a specific hit triggered during the processing of the application constitutes a false hit or where the manual processing shows that there were no grounds for refusing a travel authorisation, it should be able to attach a flag to the travel authorisation it issues to facilitate border checks by providing border authorities with information related to the verifications that have been carried out and to limit the negative consequences of false hits on travellers. Operational instructions for border authorities for handling travel authorisations should be provided in a practical handbook.

(39) Since the possession of a valid travel authorisation is a condition of entry and stay for certain categories of third-country national, the immigration authorities of the Member States should be able to consult the ETIAS Central System when a prior search has been conducted in the EES and this search indicates that the EES does not contain an entry record corresponding to the presence of the third-country national on the territory of the Member States. 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.

(40) In the fight against terrorist offences and other serious criminal offences and given the globalisation of criminal networks, it is imperative that designated authorities responsible for the prevention, detection or investigation of terrorist offences and other serious criminal offences ('designated authorities') have the necessary information to

([1]) OJ L 239, 22.9.2000, p. 19.
([2]) Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ L 77, 23.3.2016, p. 1).

perform their tasks effectively. Access to data contained in the VIS for such purposes has already proven effective in helping investigators to make substantial progress in cases related to trafficking in human beings, terrorism or drug trafficking. VIS does not contain data on visa-exempt third-country nationals.

(41) Access to the information contained in ETIAS is necessary to prevent, detect and investigate terrorist offences as referred to in Directive (EU) 2017/541 of the European Parliament and of the Council ([1]) or other serious criminal offences as referred to in Council Framework Decision 2002/584/JHA ([2]). In a specific investigation and in order to establish evidence and information related to a person suspected of having committed a serious crime or to a victim of a serious crime, 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 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 the protection of personal data of those persons whose personal data are processed in ETIAS. Therefore, the data in ETIAS should be retained and made available to the designated authorities of the Member States and to Europol only subject to the strict conditions set out in this Regulation. This will ensure that the processing of data stored in ETIAS is limited to what is strictly necessary for the prevention, detection and investigation of terrorist offences and other serious criminal offences in accordance with requirements laid down in the jurisprudence of the Court, in particular in the Digital Rights Ireland case ([3]).

(42) In particular, access to data stored in ETIAS 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 a designated authority explaining its necessity. In cases of urgency, where there is a need to prevent an imminent danger to the life of a person associated with a terrorist offence or another serious criminal offence, the verification of whether the conditions were fulfilled should take place after access to such data has been granted to the designated competent authorities. This *ex post* verification should take place without undue delay and in any event no later than seven working days after the processing of the request.

(43) It is therefore necessary to designate the 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.

(44) The central access point(s) should act independently of the designated authorities and should verify that the conditions to request access to the ETIAS Central System are fulfilled in the concrete case at hand.

(45) Europol is the hub for information exchange in the Union. It plays a key role in cooperation between Member States' authorities responsible for cross-border criminal investigations by supporting the Union-wide prevention, analysis and investigation of crime. 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 in specific cases where this is necessary for Europol to support and strengthen action by Member States to prevent, detect or investigate terrorist offences or other serious criminal offences.

(46) 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 assist them in preventing, detecting or investigating a terrorist offence or other serious criminal offence.

(47) The personal data recorded in ETIAS should be kept for no longer than is necessary for the purposes for which the data are processed. In order for ETIAS to function, it is necessary to keep the data related to applicants for the validity period of the travel authorisation. After the validity period has expired, the data should only be stored with the explicit consent of the applicant and only for the purpose of facilitating a new ETIAS application. A

([1]) Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, p. 6).

([2]) 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).

([3]) Judgment of the Court of Justice (Grand Chamber) of 8 April 2014, Digital Rights Ireland Ltd, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.

decision to refuse, annul or revoke a travel authorisation could indicate a security, illegal immigration or high epidemic risk posed by the applicant. Where such a decision has been issued, the data should therefore be kept for five years from the date of that decision, in order for ETIAS to be able to take into account accurately the higher risk possibly posed by the applicant concerned. If the data giving rise to this decision are deleted earlier, the application file should be deleted within seven days. After the expiry of such period, the personal data should be deleted.

(48) Personal data stored in the ETIAS Central System should not be made available to any third country, international organisation or private party. As an exception to that rule, however, it should be possible to transfer such personal data to a third country where the transfer is subject to strict conditions and necessary in the individual case for the purposes of return. In the absence of an adequacy decision by means of implementing act pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ([1]) or of appropriate safeguards to which transfers are subject pursuant to that Regulation, it should exceptionally be possible to transfer data stored in ETIAS to a third country for the purposes of return, but only where the transfer is necessary for important reasons of public interest as referred to in that Regulation.

(49) It should also be possible to transfer personal data obtained by Member States pursuant to this Regulation to a third country in an exceptional case of urgency, where there is an imminent danger associated with a terrorist offence or where there is an imminent danger to the life of a person associated with a serious criminal offence. An imminent danger to the life of a person should be understood as covering a danger arising from a serious criminal offence committed against that person such as grievous bodily injury, illicit trade in human organs and tissue, kidnapping, illegal restraint and hostage-taking, sexual exploitation of children and child pornography, and rape.

(50) In order to ensure public awareness of ETIAS, particularly among third-country nationals subject to the travel authorisation requirement, information concerning ETIAS, including the relevant Union legislation, and the procedure for the application for a travel authorisation should be made available to the general public through a public website and an application for mobile devices to be used for applying to ETIAS. This information should also be disseminated through a common leaflet and by any other appropriate means. In addition, applicants for a travel authorisation should receive an email notification with information related to their application. That email notification should include weblinks to applicable Union and national legislation.

(51) Precise rules should be laid down as regards the responsibilities of eu-LISA for the design, development and technical management of the ETIAS Information System. Rules should also be laid down governing the responsibilities of the European Border and Coast Guard Agency, the responsibilities of the Member States and the responsibilities of Europol as regards ETIAS. eu-LISA should pay particular attention to the risk of cost increases and ensure sufficient monitoring of contractors.

(52) Regulation (EC) No 45/2001 of the European Parliament and of the Council ([2]) applies to the activities of eu-LISA and the European Border and Coast Guard Agency when carrying out the tasks entrusted to them in this Regulation.

(53) Regulation (EU) 2016/679 applies to the processing of personal data by the Member States in application of this Regulation.

(54) Where the processing of personal data by Member States for the purpose of assessing applications is carried out by the competent authorities for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences, Directive (EU) 2016/680 of the European Parliament and of the Council ([3]) applies.

(55) Directive (EU) 2016/680 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.

([1]) 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) (OJ L 119, 4.5.2016, p. 1).

([2]) Regulation (EC) No 45/2001 of the European Parliament and of 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).

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

(56) The independent supervisory authorities established in accordance with Regulation (EU) 2016/679 should monitor the lawfulness of the processing of personal data by Member States, whilst the European Data Protection Supervisor 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 monitoring ETIAS.

(57) 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, rectification, restriction, completion, erasure and redress in relation to personal data, in particular the right to a judicial remedy and the supervision of processing operations by public independent authorities.

(58) In order to assess the security, illegal immigration or high epidemic risks which could be posed by a traveller, interoperability between the ETIAS Information System and other EU information systems should be established. Interoperability should be established in full compliance with the Union *acquis* concerning fundamental rights. If a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons is established at Union level, ETIAS should be able to query it.

(59) This Regulation should contain clear provisions on liability and the right to compensation for the unlawful processing of personal data and for any other act incompatible with this Regulation. Such provisions should be without prejudice to the right to compensation from, and liability of the controller or processor under Regulation (EU) 2016/679, Directive (EU) 2016/680 and Regulation (EC) No 45/2001. eu-LISA should be responsible for any damage it causes in its capacity as a data processor where it has not complied with the obligations specifically imposed on it by this Regulation, or where it has acted outside or contrary to lawful instructions of the Member State which is the data controller.

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

(61) In order to establish the technical measures needed for the application of this Regulation, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission:

— to define the requirements of the secure account service,

— to lay down the predetermined list of job groups used in the application form,

— to specify the content and format of questions to applicants relating to convictions for criminal offences, stays in war or conflict zones and decisions to leave the territory or return decisions,

— to specify the content and format of additional questions to applicants who reply affirmatively to one of the questions relating to convictions for criminal offences, stays in war or conflict zones and decisions to leave the territory or return decisions, and to set out a predetermined list of answers,

— to lay down the payment methods and process for collecting the travel authorisation fee and any changes to the amount of that fee to reflect any increase in the costs of ETIAS,

— to lay down the content and format of a predetermined list of options for applicants requested to provide additional information or documentation,

— to further define the verification tool,

— to further define the security, illegal immigration or high epidemic risks to be used to establish the specific risk indicators,

— to define the type of additional information related to flags that may be added in the ETIAS application file, its formats, language and the reasons for the flags,

— to establish adequate safeguards by providing rules and procedures to avoid conflicts with alerts in other information systems and to define the conditions, the criteria and the duration of the flagging,

— to further define the tool to be used by applicants to give and withdraw their consent,

— to extend the duration of the transitional period during which no travel authorisation is required and the duration of the grace period during which border guards will allow third-country nationals requiring a travel authorisation but not in possession of one exceptionally to enter subject to certain conditions,

— to define the financial support for Member States for expenses they incur to customise and automate border checks when implementing ETIAS.

(62) 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 of 13 April 2016 on Better Law-Making ([1]). 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.

(63) 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:

— a form allowing the reporting of abuses by commercial intermediaries authorised by applicants to submit applications on their behalf,

— the conditions for operation of the public website and the app for mobile devices, and detailed rules on data protection and security applicable to the public website and the app for mobile devices,

— the requirements governing the format of the personal data to be inserted in the application form and the parameters and verifications to be implemented for ensuring the completeness of the application and the coherence of these data,

— the requirements, testing and operation of the means of audio and video communication relied on for applicant interviews, and detailed rules on data protection, security and confidentiality applicable to such communication,

— the security, illegal immigration and high epidemic risks on which specific risk indicators are to be based,

— the technical specifications of the ETIAS watchlist and of the assessment tool to be used to assess the potential impact of entering data into the ETIAS watchlist on the proportion of applications that are manually processed,

— a form for refusal, annulment or revocation of a travel authorisation,

— the conditions for ensuring secure access to the ETIAS Information System by carriers, and the data protection and security rules applicable to this access,

— an authentication scheme for access to the ETIAS Information System for duly authorised members of carrier staff,

— the fall-back procedures to be followed in the case of a technical impossibility for carriers to query the ETIAS Information System,

([1]) OJ L 123, 12.5.2016, p. 1.

— model contingency plans in the case of a technical impossibility for border authorities to consult the ETIAS Central System or in case of a failure of ETIAS,

— a model security plan and a model business continuity and disaster recovery plan concerning the security of processing of personal data,

— access to the data in the ETIAS Information System,

— amendment, erasure and advance erasure of data,

— the keeping of logs and access to them,

— performance requirements,

— specifications for technical solutions to connect central access points to the ETIAS Central System,

— a mechanism, procedures and interpretations of data quality compliance for the data contained in the ETIAS Central System,

— common leaflets to inform travellers of the requirement to be in possession of a valid travel authorisation,

— the operation of a central repository containing data solely for the purpose of reporting and statistics, and the data protection and security rules applicable to the repository, and

— the specifications of a technical solution for the purpose of facilitating the collection of statistical data necessary to report on the effectiveness of access to data stored in the ETIAS Central System for law enforcement purposes.

Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council ([1]).

(64) Since the objectives of this Regulation, namely, the establishment of a European Travel Information and Authorisation System and the creation of common obligations, conditions and procedures for use of the data stored in it cannot be sufficiently achieved by the Member States but can rather, by reason of the scale and effects of the action, be better achieved at Union level, the Union may adopt measures 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, this Regulation does not go beyond what is necessary in order to achieve those objectives.

(65) The operational and maintenance costs of the ETIAS Information System, of the ETIAS Central Unit and of the ETIAS National Units should be covered entirely by the revenues generated by the travel authorisation fees. The fee should therefore be adjusted as necessary in light of the costs incurred.

(66) 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 internal assigned revenue. Any revenue remaining after covering these costs should be assigned to the Union budget.

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

(68) This Regulation respects fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the European Union.

(69) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the TEU and to the TFEU, 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.

([1]) 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 the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

(70) 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 ([1]); 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.

(71) 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 ([2]); Ireland is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(72) As regards Iceland and Norway, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latters' association with the implementation, application and development of the Schengen *acquis* ([3]) which fall within the area referred to in Article 1, point A of Council Decision 1999/437/EC ([4]).

(73) 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* ([5]) which fall within the area referred to in Article 1, point A of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/146/EC ([6]) and with Article 3 of Council Decision 2008/149/JHA ([7]).

(74) 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* ([8]) which fall within the area referred to in Article 1, point A of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU ([9]) and with Article 3 of Council Decision 2011/349/EU ([10]).

(75) In order to determine the modalities relating to the financial contribution of third countries associated with the implementation, application and development of the Schengen *acquis*, further arrangements should be concluded between the Union and those countries under the relevant provisions of their association agreements. Such arrangements should constitute international agreements within the meaning of Article 218 TFEU.

([1]) 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).
([2]) 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).
([3]) OJ L 176, 10.7.1999, p. 36.
([4]) 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).
([5]) OJ L 53, 27.2.2008, p. 52.
([6]) Council Decision 2008/146/EC of 28 January 2008 on the conclusion, on behalf of the European Community, of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L 53, 27.2.2008, p. 1).
([7]) 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).
([8]) OJ L 160, 18.6.2011, p. 21.
([9]) 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).
([10]) 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).

(76) In order to integrate this Regulation into the existing legal framework and to reflect the necessary operational changes for eu-LISA and the European Border and Coast Guard Agency, Regulations (EU) No 1077/2011 ([1]), (EU) No 515/2014 ([2]), (EU) 2016/399, (EU) 2016/1624 ([3]) and (EU) 2017/2226 ([4]) of the European Parliament and of the Council should be amended.

(77) 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 ([5]),

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') enabling consideration of whether the presence of those third-country nationals in the territory of the Member States would pose a security, illegal immigration or high epidemic 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' designated authorities and 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:

(a) nationals of third countries listed in Annex II to Council Regulation (EC) No 539/2001 ([6]) who are exempt from the visa requirement for intended stays in the territory of the Member States of a duration of no more than 90 days in any 180-day period;

(b) persons who, pursuant to Article 4(2) of Regulation (EC) No 539/2001, are exempt from the visa requirement 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 equivalent to that of Union citizens under an agreement between the Union and its Member States on the one hand and a third country on the other; and

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

([1]) Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 286, 1.11.2011, p. 1).
([2]) 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).
([3]) Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC (OJ L 251, 16.9.2016, p. 1).
([4]) Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (OJ L 327, 9.12.2017, p. 20).
([5]) OJ C 162, 23.5.2017, p. 9.
([6]) Council Regulation (EC) No 539/2001 of 15 March 2001 listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement (OJ L 81, 21.3.2001, p. 1).

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 family members 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 family members of a third-country national enjoying a right of free movement equivalent to that of Union citizens, under an agreement between the Union and its Member States on the one hand and a third country on the other, and who hold a residence card pursuant to Directive 2004/38/EC or a residence permit pursuant to Regulation (EC) No 1030/2002;

(d) holders of residence permits referred to in point 16 of Article 2 of Regulation (EU) 2016/399;

(e) holders of uniform visas;

(f) holders of national long-stay visas;

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

(h) nationals of third countries who are holders of a local border traffic permit issued by the Member States pursuant to Regulation (EC) No 1931/2006 of the European Parliament and of the Council [1] when such holders exercise their right within the context of the Local Border Traffic regime;

(i) persons or categories of persons referred to in points (a) to (f) of Article 4(1) of Regulation (EC) No 539/2001;

(j) third-country nationals holding diplomatic or service passports who have been exempted from the visa requirement pursuant to an international agreement concluded by the Union and a third country;

(k) persons who are subject to a visa requirement pursuant to Article 4(3) of Regulation (EC) No 539/2001;

(l) third-country nationals exercising their right to mobility in accordance with Directive 2014/66/EU [2] or (EU) 2016/801 [3] of the European Parliament and of the Council.

Article 3

Definitions

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

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

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

(3) 'second line check' means a second line check as defined in point 13 of Article 2 of Regulation (EU) 2016/399;

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

(5) 'travel authorisation' means a decision issued in accordance with this Regulation which is required for third-country nationals referred to in Article 2(1) of this Regulation to fulfil the entry condition laid down in point (b) of Article 6(1) of Regulation (EU) 2016/399 and which indicates:

(a) that no factual indications or reasonable grounds based on factual indications have been identified to consider that the presence of the person on the territory of the Member States poses or will pose a security, illegal immigration or high epidemic risk;

[1] Regulation (EC) No 1931/2006 of the European Parliament and of the Council of 20 December 2006 laying down rules on local border traffic at the external land borders of the Member States and amending the provisions of the Schengen Convention (OJ L 405, 30.12.2006, p. 1).

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

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

(b) that no factual indications or reasonable grounds based on factual indications have been identified to consider that the presence of the person on the territory of the Member States poses or will pose a security, illegal immigration or high epidemic risk, although doubt remains concerning the existence of sufficient reasons to refuse the travel authorisation, in accordance with Article 36(2);

(c) where factual indications have been identified to consider that the presence of the person on the territory of the Member States poses or will pose a security, illegal immigration or high epidemic risk, that the territorial validity of the authorisation has been limited in accordance with Article 44; or

(d) where factual indications have been identified to consider that the presence of the person on the territory of the Member States poses or will pose a security risk, that the traveller is the subject of an alert in SIS on persons for discreet checks or specific checks or of an alert in SIS on persons wanted for arrest for surrender purposes on the basis of an European Arrest Warrant or wanted for arrest for extradition purposes, in support of the objectives of SIS referred to in point (e) of Article 4;

(6) 'security risk' means the risk of a threat to public policy, internal security or international relations for any of the Member States;

(7) '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;

(8) 'high epidemic risk' means any disease with epidemic potential as defined by the International Health Regulations of the World Health Organization (WHO) or the European Centre for Disease Prevention and Control (ECDC) and other infectious diseases or contagious parasitic diseases if they are the subject of protection provisions applying to nationals of the Member States;

(9) 'applicant' means any third-country national referred to in Article 2 who has submitted an application for a travel authorisation;

(10) '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;

(11) 'short stay' means stays in the territory of the Member States within the meaning of Article 6(1) of Regulation (EU) 2016/399;

(12) '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;

(13) 'app for mobile devices' means a software application designed to run on mobile devices such as smartphones and tablet computers;

(14) '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 specific risk indicators referred to in Article 33 or with the personal data present in a record, file or alert registered in the ETIAS Central System, in another EU information system or database listed in Article 20(2) ('EU information systems'), in Europol data or in an Interpol database queried by the ETIAS Central System;

(15) 'terrorist offence' means an offence which corresponds or is equivalent to one of the offences referred to in Directive (EU) 2017/541;

(16) 'serious criminal offence' means an offence which corresponds or is equivalent to one of the offences referred to in Article 2(2) of Framework Decision 2002/584/JHA, if it is punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years;

(17) 'Europol data' means personal data processed by Europol for the purpose referred to in point (a) of Article 18(2) of Regulation (EU) 2016/794;

(18) 'electronically signed' means the confirmation of agreement through the ticking of an appropriate box in the application form or the request for consent;

(19) 'minor' means a third-country national or a stateless person below the age of 18 years;

(20) 'consulate' means a Member State's diplomatic mission or a Member State's consular post as defined by the Vienna Convention on Consular Relations of 24 April 1963;

(21) 'designated authority' means an authority designated by a Member State pursuant to Article 50 as responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences;

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

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

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

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

2. The terms defined in Article 2 of Regulation (EC) No 45/2001 shall have the same meaning in this Regulation insofar as personal data are processed by the European Border and Coast Guard Agency and eu-LISA.

3. The terms defined in Article 4 of Regulation (EU) 2016/679 shall have the same meaning in this Regulation insofar as personal data are processed by the authorities of Member States for the purposes laid down in points (a) to (e) of Article 4 of this Regulation.

4. The terms defined in Article 3 of Directive (EU) 2016/680 shall have the same meaning in this Regulation insofar as personal data are processed by the authorities of the Member States for the purposes laid down in point (f) of Article 4 of this Regulation.

Article 4

Objectives of ETIAS

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

(a) contribute to a high level of security by providing for a thorough security risk assessment of applicants, prior to their arrival at external border crossing points, in order to determine whether there are factual indications or reasonable grounds based on factual indications 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 illegal immigration by providing for an illegal immigration risk assessment of applicants prior to their arrival at external border crossing points;

(c) contribute to the protection of public health by providing for an assessment of whether the applicant poses a high epidemic risk within the meaning of point 8 of Article 3(1) prior to his or her arrival at external border crossing points;

(d) enhance the effectiveness of border checks;

(e) support the objectives of SIS related to alerts on third-country nationals subject to a refusal of entry and stay, alerts on persons wanted for arrest for surrender purposes or extradition purposes, alerts on missing persons, alerts on persons sought to assist with a judicial procedure and alerts on persons for discreet checks or specific checks;

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

([1]) Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection (OJ L 180, 29.6.2013, p. 60).

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

Article 5

General structure of ETIAS

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

Establishment and technical architecture of the ETIAS Information System

1. The European Agency for the operational management of large-scale IT 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) the ETIAS Central System, including the ETIAS watchlist referred to in Article 34;

(b) a national uniform interface (NUI) in each Member State based on common technical specifications and identical for all Member States enabling the ETIAS Central System to connect to the national border infrastructures and to the central access points in Member States referred to in Article 50(2) in a secure manner;

(c) a communication infrastructure between the ETIAS Central System and the NUIs which shall be secure and encrypted;

(d) a secure communication infrastructure between the ETIAS Central System and the information systems referred to in Article 11;

(e) a public website and an app for mobile devices;

(f) an email service;

(g) a secure account service enabling applicants to provide any additional information or documentation required;

(h) a verification tool for applicants;

(i) a tool enabling applicants to give or withdraw their consent for an additional retention period of their application file;

(j) a tool enabling Europol and Member States to assess the potential impact of entering new data into the ETIAS watchlist on the proportion of applications that are manually processed;

(k) a carrier gateway;

(l) a secure web service enabling the ETIAS Central System to communicate with the public website, the app for mobile devices, the email service, the secured account service, the carrier gateway, the verification tool for applicants, the consent tool for applicants, the payment intermediary and the Interpol databases;

(m) software enabling the ETIAS Central Unit and the ETIAS National Units to process applications and to manage consultations with other ETIAS National Units as referred to in Article 28 and with Europol as referred to in Article 29;

(n) a central repository of data for the purposes of reporting and statistics.

3. The ETIAS Central System, the NUIs, the web service, the carrier gateway and the communication infrastructure of ETIAS shall to the extent technically possible share and re-use the hardware and software components of the EES Central System, of the EES National Uniform Interfaces, of the EES web service and of the EES Communication Infrastructure referred to in Regulation (EU) 2017/2226.

4. The Commission shall adopt delegated acts in accordance with Article 89 in order to define the requirements of the secure account service referred to in point (g) of paragraph 2 of this Article.

Article 7

ETIAS Central Unit

1. An ETIAS Central Unit is hereby established within the European Border and Coast Guard Agency.

2. The ETIAS Central Unit shall be operational 24 hours a day, 7 days a week. It shall have the following responsibilities:

(a) in cases where the automated application process has reported a hit, verifying in accordance with Article 22 whether the applicant's personal data correspond to the personal data of the person having triggered that hit in the ETIAS Central System, including the ETIAS watchlist referred to in Article 34, any of the EU information systems that are consulted, Europol data, any of the Interpol databases referred to in Article 12, or the specific risk indicators referred to in Article 33, and where a correspondence is confirmed or where doubts remain, launching the manual processing of the application as referred to in Article 26;

(b) ensuring that the data it enters in the applications files are up to date in accordance with the relevant provisions of Articles 55 and 64;

(c) defining, establishing, assessing *ex ante*, implementing, evaluating *ex post*, revising and deleting the specific risk indicators as referred to in Article 33 after consultation of the ETIAS Screening Board;

(d) ensuring that the verifications performed in accordance with Article 22 and the corresponding results are recorded in the application files;

(e) carrying out regular audits of the processing of applications and of the implementation of Article 33, including by regularly assessing their impact on fundamental rights, in particular with regard to privacy and personal data protection;

(f) indicating, where necessary, the Member State responsible for the manual processing of applications as referred to in Article 25(2);

(g) in cases of technical problems or unforeseen circumstances, facilitating where necessary the consultations between Member States referred to in Article 28 and between the Member State responsible and Europol referred to in Article 29;

(h) notifying carriers in cases of a failure of the ETIAS Information System as referred to in Article 46(1);

(i) notifying the ETIAS National Units of the Member States of a failure of the ETIAS Information System as referred to in Article 48(1);

(j) processing requests for consultation of data in the ETIAS Central System by Europol as referred to in Article 53;

(k) providing the general public with all relevant information in relation to the application for a travel authorisation as referred to in Article 71;

(l) cooperating with the Commission as regards the information campaign referred to in Article 72;

(m) providing support in writing to travellers who have encountered problems when filling in the application form and have requested assistance through a standard contact form; maintaining a list of frequent questions and answers available online;

(n) ensuring follow-up and regularly reporting to the Commission on reported abuses by commercial intermediaries as referred to in Article 15(5).

3. The ETIAS Central Unit shall publish an annual activity report. That report shall include:

(a) statistics on:

(i) the number of travel authorisations issued automatically by the ETIAS Central System;

(ii) the number of applications verified by the ETIAS Central Unit;

(iii) the number of applications processed manually per Member State;

(iv) the number of applications that were refused by third country and the grounds for the refusal;

(v) the extent to which the deadlines referred to in Article 22(6) and Articles 27, 30 and 32 have been met.

(b) general information on the functioning of the ETIAS Central Unit, its activities as set out in this Article and information on current trends and challenges affecting the conduct of its tasks.

The annual activity report shall be transmitted to the European Parliament, the Council and the Commission by 31 March of the following year.

Article 8

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) examining and deciding on applications for travel authorisation where the automated application process has reported a hit and the manual processing of the application has been initiated by the ETIAS Central Unit;

(b) ensuring that the tasks performed under point (a) and the corresponding results are recorded in the application files;

(c) ensuring that the data they enter in the application files are up to date in accordance with the relevant provisions of Articles 55 and 64;

(d) deciding to issue travel authorisations with limited territorial validity as referred to in Article 44;

(e) ensuring coordination with other ETIAS National Units and Europol concerning the consultation requests referred to in Articles 28 and 29;

(f) providing applicants with information regarding the procedure to be followed in the event of an appeal under Article 37(3);

(g) annulling and revoking a travel authorisation as referred to in Articles 40 and 41.

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.

Article 9

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, of the European Border and Coast Guard Agency and of Europol.

2. The ETIAS Screening Board shall be consulted:

(a) by the ETIAS Central Unit on the definition, establishment, assessment *ex ante*, implementation, evaluation *ex post*, revision and deletion of the specific risk indicators referred to in Article 33;

(b) by Member States on the implementation of the ETIAS watchlist referred to in Article 34;

(c) by Europol on the implementation of the ETIAS watchlist referred to in Article 34.

3. The ETIAS Screening Board shall issue opinions, guidelines, recommendations and best practices for the purposes referred to in paragraph 2. When issuing recommendations, the ETIAS Screening Board shall take into consideration the recommendations issued by the ETIAS Fundamental Rights Guidance Board.

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 may consult the ETIAS Fundamental Rights Guidance Board on specific issues related to fundamental rights, in particular with regard to privacy, personal data protection and non-discrimination.

6. The ETIAS Screening Board shall adopt rules of procedure at its first meeting by a simple majority of its members.

Article 10

ETIAS Fundamental Rights Guidance Board

1. An independent ETIAS Fundamental Rights Guidance Board with an advisory and appraisal function is hereby established. Without prejudice to their respective competences and independence, it shall be composed of the Fundamental Rights Officer of the European Border and Coast Guard Agency, a representative of the consultative forum on fundamental rights of the European Border and Coast Guard Agency, a representative of the European Data Protection Supervisor, a representative of the European Data Protection Board established by Regulation (EU) 2016/679 and a representative of the European Union Agency for Fundamental Rights.

2. The ETIAS Fundamental Rights Guidance Board shall perform regular appraisals and issue recommendations to the ETIAS Screening Board on the impact on fundamental rights of the processing of applications and of the implementation of Article 33, in particular with regard to privacy, personal data protection and non-discrimination.

The ETIAS Fundamental Rights Guidance Board shall also support the ETIAS Screening Board in the execution of its tasks when consulted by the latter on specific issues related to fundamental rights, in particular with regard to privacy, personal data protection and non-discrimination.

The ETIAS Fundamental Rights Guidance Board shall have access to the audits referred to in point (e) of Article 7(2).

3. The ETIAS Fundamental Rights Guidance 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. Its meetings shall take place in premises of the European Border and Coast Guard Agency. The secretariat of its meetings shall be provided by the European Border and Coast Guard Agency. The ETIAS Fundamental Rights Guidance Board shall adopt rules of procedure at its first meeting by a simple majority of its members.

4. One representative of the ETIAS Fundamental Rights Guidance Board shall be invited to attend the meetings of the ETIAS Screening Board in an advisory capacity. The members of the ETIAS Fundamental Rights Guidance Board shall have access to the information and files of the ETIAS Screening Board.

5. The ETIAS Fundamental Rights Guidance Board shall produce an annual report. The report shall be made publicly available.

Article 11

Interoperability with other EU information systems

1. Interoperability between the ETIAS Information System, other EU information systems and Europol data shall be established to enable the verification referred to in Article 20.

2. The amendments to the legal acts establishing the EU information systems that are necessary for establishing their interoperability with ETIAS as well as the addition of corresponding provisions in this Regulation shall be the subject of a separate legal instrument.

Article 12

Querying the Interpol databases

The ETIAS Central System shall query the Interpol Stolen and Lost Travel Document database (SLTD) and the Interpol Travel Documents Associated with Notices database (TDAWN). Any queries and verification shall be performed in such a way that no information shall be revealed to the owner of the Interpol alert.

Article 13

Access to data stored in ETIAS

1. Access to the ETIAS Information System shall be reserved exclusively for duly authorised staff of the ETIAS Central Unit and of the ETIAS National Units.

2. Access by border authorities to the ETIAS Central System in accordance with Article 47 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 the data referred to in points (a), (c) and (d) of Article 47(2). In addition, border authorities shall be informed automatically of the flags referred to in Article 36(2) and (3) and of the reasons for the flags.

When exceptionally, according to a flag, a second line check is recommended at the border or additional verifications are needed for the purpose of a second line check, border authorities shall access the ETIAS Central System to obtain the additional information provided for in point (e) of Article 39(1) or point (f) of Article 44(6).

3. Access by carriers to the ETIAS Information System in accordance with Article 45 shall be limited to sending queries to the ETIAS Information System to obtain the travel authorisation status of a traveller.

4. Access by immigration authorities to the ETIAS Central System in accordance with Article 49 shall be limited to obtaining the travel authorisation status of a traveller present on the territory of the Member State, and to certain data as referred to in that Article.

Access by immigration authorities to the ETIAS Central System in accordance with Article 65(3) shall be limited to the data referred to in that Article.

5. Each Member State shall designate the competent national authorities referred to in paragraphs 1, 2 and 4 of this Article and shall communicate a list of those authorities to eu-LISA without delay, in accordance with Article 87(2). That list shall specify for which purpose the duly authorised staff of each authority shall have access to the data in the ETIAS Information System in accordance with paragraphs 1, 2 and 4 of this Article.

Article 14

Non-discrimination and fundamental rights

Processing of personal data within the ETIAS Information System by any user shall not result in discrimination against third-country nationals on the grounds of sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation. It shall fully respect human dignity and integrity and fundamental rights, including the right to respect for one's private life and to the protection of personal data. Particular attention shall be paid to children, the elderly and persons with a disability. The best interests of the child shall be a primary consideration.

CHAPTER II

APPLICATION

Article 15

Practical arrangements for submitting an application

1. Applicants shall submit an application by filling in the online application form via the dedicated public website or via the app for mobile devices sufficiently in advance of any intended travel, or, if they are already present on the territory of Member States, before the expiry of an existing travel authorisation they hold.

2. Holders of a travel authorisation may submit an application for a new travel authorisation from 120 days before the expiry of the travel authorisation.

120 days before the expiry of the travel authorisation, the ETIAS Central System shall automatically inform the holder of that travel authorisation via the email service of:

(a) the expiry date of the travel authorisation;

(b) the possibility to submit an application for a new travel authorisation;

(c) the obligation to be in possession of a valid travel authorisation for the entire duration of a short stay on the territory of Member States.

3. All notifications to the applicant for the purpose of his or her application for a travel authorisation shall be sent to the email address provided by the applicant in the application form as referred to in point (g) of Article 17(2).

4. Applications may be submitted by the applicant or by a person or a commercial intermediary authorised by the applicant to submit the application on his or her behalf.

5. The Commission shall, by means of an implementing act, create a form allowing abuses by the commercial intermediaries referred to in paragraph 4 of this Article to be reported. This form shall be made accessible via the dedicated public website or via the app for mobile devices referred to in paragraph 1 of this Article. Such completed forms shall be sent to the ETIAS Central Unit which shall take appropriate action, including by regularly reporting to the Commission. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 90(2).

Article 16

The public website and the app for mobile devices

1. The public website and the app for mobile devices shall enable third-country nationals subject to the travel authorisation requirement to submit a travel authorisation application, to provide the data required in the application form in accordance with Article 17 and to pay the travel authorisation fee.

2. The public website and the app for mobile devices shall make the application form widely available and easily accessible to applicants free of charge. Specific attention shall be paid to the accessibility of the public website and the app for mobile devices for persons with disabilities.

3. The public website and the 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 to Regulation (EC) No 539/2001 do not correspond to the languages referred to in paragraph 3, factsheets with explanatory information concerning ETIAS, the application procedure, the use of the public website and the app for mobile devices as well as a step-by-step guide to the application shall be made available by eu-LISA on the public website and on the 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 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 app for mobile devices shall provide the applicant with an account service enabling applicants to provide additional information or documentation, where required.

7. The public website and the app for mobile devices shall inform applicants of their right to an appeal under this Regulation if a travel authorisation is refused, revoked or annulled. To this end, they shall contain information about the national law applicable, the competent authority, how to lodge an appeal, the time limit for lodging an appeal and information as to any assistance that may be provided by the national data protection authority.

8. The public website and the app for mobile devices shall enable applicants to indicate that the purpose of their intended stay relates to humanitarian grounds or international obligations.

9. The public website shall contain the information referred to in Article 71.

10. The Commission shall, by means of implementing acts, adopt detailed rules on the operation of the public website and the app for mobile devices, and detailed rules on data protection and security applicable to the public website and the app for mobile devices. Those detailed rules shall be based on information security risk management and on principles of data protection by design and by default. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 90(2).

Article 17

Application form and personal data of the applicant

1. Each applicant shall submit a completed application form including a declaration of the authenticity, completeness, correctness and reliability of the data submitted and a declaration of the veracity and reliability of the statements made. Each applicant shall also state that he or she has understood the conditions for entry referred to in Article 6 of Regulation (EU) 2016/399 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 issue of the travel document;

(e) the date of issue 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;

(g) email address and, if available, phone numbers;

(h) education (primary, secondary, higher or none);

(i) current occupation (job group); where the application is subject to the manual processing in accordance with the procedure laid down in Article 26, the Member State responsible may in accordance with Article 27 request that the applicant provide additional information concerning his or her exact job title and employer or, for students, the name of their educational establishment;

(j) Member State of first intended stay, and optionally, the address of first intended stay;

(k) for minors, surname and first name(s), home address, email address and, if available, phone number of the person exercising parental authority or of the applicant's legal guardian;

(l) where he or she claims the status of family member referred to in point (c) of Article 2(1):

  (i) his or her status of family member;

  (ii) the surname, first name(s), date of birth, place of birth, country of birth, current nationality, home address, email address and, if available, phone number of the family member with whom the applicant has family ties;

  (iii) his or her 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, organisation if applicable, email address, mailing address and phone number if available of that person; relationship to the applicant and a signed representation declaration.

3. The applicant shall choose his or her current occupation (job group) from a predetermined list. The Commission shall adopt delegated acts in accordance with Article 89 to lay down this predetermined list.

4. In addition, the applicant shall provide answers to the following questions:

(a) whether he or she has been convicted of any criminal offence listed in the Annex over the previous 10 years and in the case of terrorist offences, over the previous 20 years, and if so when and in which country;

(b) whether he or she has stayed in a specific war or conflict zone over the previous 10 years and the reasons for the stay;

(c) whether he or she has been the subject of any decision requiring him or her to leave the territory of a Member State or of any third countries listed in Annex II to Regulation (EC) No 539/2001 or whether he or she was subject to any return decision issued over the previous 10 years.

5. The Commission shall adopt delegated acts in accordance with Article 89 specifying the content and format of the questions referred to in paragraph 4 of this Article. The content and format of those questions shall enable applicants to give clear and precise answers.

6. 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 an additional set of predetermined questions on the application form by selecting from a predetermined list of answers. The Commission shall adopt delegated acts in accordance with Article 89 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.

8. On submission of the application form, the ETIAS Information System shall collect the IP address from which the application form was submitted.

9. The Commission shall, by means of implementing acts, define the requirements concerning the format of the personal data referred to in paragraphs 2 and 4 of this Article to be inserted in the application form as well as parameters and verifications to be implemented for ensuring the completeness of the application and the coherence of those data. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 90(2).

Article 18

Travel authorisation fee

1. A travel authorisation fee of EUR 7 shall be paid by the applicant for each application.

2. The travel authorisation fee shall be waived for applicants under 18 years or above 70 years of age at the time of the application.

3. The travel authorisation fee shall be charged in euros.

4. The Commission shall adopt delegated acts in accordance with Article 89 on the payment methods and process for the travel authorisation fee and on changes to the amount of that fee. Changes to the amount shall take into account any increase in the costs referred to in Article 85.

CHAPTER III

CREATION OF THE APPLICATION FILE AND EXAMINATION OF THE APPLICATION BY THE ETIAS CENTRAL SYSTEM

Article 19

Admissibility and creation of the application file

1. The ETIAS Information 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 17(2) and (4);

(b) the travel authorisation fee has been collected.

2. If the conditions in points (a) and (b) of paragraph 1 are met, the application shall be deemed admissible. The ETIAS Central System shall then 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 17(2) and, where applicable, Article 17(4) and (6), including the three-letter code of the country issuing the travel document;

(d) the data referred to in Article 17(8);

(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 point (a) of Article 17(2) 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 explaining that, during the processing of the application, the applicant may be asked to provide additional information or documentation or, in exceptional circumstances, attend an interview. This notification shall include:

(a) status information, acknowledging the submission of an application for travel authorisation; and

(b) the application number.

The notification shall enable the applicant to make use of the verification tool provided for in point (h) of Article 6(2).

Article 20

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 points (a),(b), (c), (d), (f), (g), (j), (k) and (m) of Article 17(2) and in Article 17(8) to the data present in a record, file or alert registered in the ETIAS Central System, SIS, the EES, VIS, Eurodac, Europol data and Interpol SLTD and TDAWN databases.

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, misappropriated or invalidated in 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 and stay alert entered in 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 SIS;

(e) whether the applicant and the travel document correspond to a refused, revoked or annulled 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 point (a) of Article 17(2) in the ETIAS Central System;

(g) whether the applicant is currently reported as an overstayer or whether he or she has been reported as an overstayer in the past in the EES;

(h) whether the applicant is recorded as having been refused entry in the EES;

(i) whether the applicant has been subject to a decision to refuse, annul or revoke a short stay visa recorded in VIS;

(j) whether the data provided in the application correspond to data recorded in Europol data;

(k) whether the applicant is registered in Eurodac;

(l) whether the travel document used for the application corresponds to a travel document recorded in a file in TDAWN;

(m) in cases where the 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 SIS;

  (ii) is subject to a refusal of entry and stay alert entered in SIS.

3. The ETIAS Central System shall verify whether the applicant has replied affirmatively to any of the questions listed in Article 17(4) and whether the applicant has not provided a home address but only his city and country of residence, as referred to in point (f) of Article 17(2).

4. The ETIAS Central System shall compare the relevant data referred to in points (a), (b), (c), (d), (f), (g), (j), (k) and (m) of Article 17(2) and in Article 17(8) to the data present in the ETIAS watchlist referred to in Article 34.

5. The ETIAS Central System shall compare the relevant data referred to in points (a), (c), (f), (h) and (i) of Article 17(2) to the specific risk indicators referred to in Article 33.

6. The ETIAS Central System shall add a reference to any hit obtained pursuant to paragraphs 2 to 5 to the application file.

7. Where the data recorded in the application file correspond 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 and shall record this in the application file.

8. Following any hit pursuant to paragraph 2(j) and paragraph 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 21

Results of the automated processing

1. Where the automated processing laid down in Article 20(2) to (5) does not report any hit, the ETIAS Central System shall automatically issue a travel authorisation in accordance with Article 36 and shall notify the applicant in accordance with Article 38.

2. Where the automated processing laid down in Article 20(2) to (5) reports one or several hits, the application shall be processed in accordance with the procedure laid down in Article 22.

3. Where verification under Article 22 confirms that the data recorded in the application file correspond to the data triggering a hit during the automated processing pursuant to Article 20(2) to (5) or where doubts remain concerning the identity of the applicant following such verification, the application shall be processed in accordance with the procedure laid down in Article 26.

4. Where automated processing under Article 20(3) reports that the applicant has replied affirmatively to any of the questions listed in Article 17(4), and if there is no other hit, the application shall be sent to the ETIAS National Unit of the Member State responsible, for manual processing as set out in Article 26.

Article 22

Verification by the ETIAS Central Unit

1. Where the automated processing pursuant to Article 20(2) to (5) reports one or several hits the ETIAS Central System shall automatically consult the ETIAS Central Unit.

2. When consulted, the ETIAS Central Unit shall have access to the application file and any linked application files, as well as to all the hits triggered during automated processing pursuant to Article 20(2) to (5) and to the information identified by the ETIAS Central System under Article 20(7) and (8).

3. The ETIAS Central Unit shall verify whether the data recorded in the application file correspond to one or more of the following:

(a) the specific risk indicators referred to in Article 33;

(b) the data present in the ETIAS Central System, including the ETIAS watchlist referred to in Article 34;

(c) the data present in one of the EU information systems that are consulted;

(d) Europol data;

(e) the data present in the Interpol SLTD or TDAWN databases.

4. Where the data do not correspond, and no other hit has been reported during automated processing pursuant to Article 20(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 36.

5. Where the data correspond to those of the applicant or where doubts remain concerning the identity of the applicant, the application shall be processed manually in accordance with the procedure laid down in Article 26.

6. The ETIAS Central Unit shall complete the manual processing within a maximum of 12 hours from receipt of the application file.

Article 23

Support of the objectives of SIS

1. For the purposes of point (e) of Article 4, the ETIAS Central System shall compare the relevant data referred to in points (a), (b) and (d) of Article 17(2) to the data present in SIS in order to determine whether the applicant is the subject of 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 or specific checks.

2. Where the comparison referred to in paragraph 1 reports one or several hits, the ETIAS Central System shall send an automated notification to the ETIAS Central Unit. The ETIAS Central Unit shall verify whether the applicant's personal data correspond to the personal data contained in the alert having triggered that hit and if a correspondence is confirmed, the ETIAS Central System shall send an automated notification to the SIRENE Bureau of the Member State that entered the alert. The SIRENE Bureau concerned shall further verify whether the applicant's personal data correspond to the personal data contained in the alert having triggered the hit and take any appropriate follow-up action.

The ETIAS Central System shall also send an automated notification to the SIRENE Bureau of the Member State that entered the alert having triggered a hit against SIS during the automated processing referred to in Article 20 where, following verification by the ETIAS Central Unit as referred to in Article 22, that alert has led to manual processing of the application in accordance with Article 26.

3. The notification provided to the SIRENE Bureau of the Member State that entered the alert shall contain the following data:

(a) surname(s), first name(s) and, if any, alias(es);

(b) place and date of birth;

(c) sex;

(d) nationality and, if any, other nationalities;

(e) Member State of first intended stay, and if available, the address of first intended stay;

(f) the applicant's home address or, if not available, his or her city and country of residence;

(g) travel authorisation status information, indicating whether a travel authorisation has been issued, refused or whether the application is subject to manual processing pursuant to Article 26;

(h) a reference to any hits 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 24

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

1. For third-country nationals referred to in point (c) of Article 2(1), the travel authorisation as defined in point 5 of Article 3(1) shall be understood as a decision issued in accordance with this Regulation indicating that there are no factual indications or reasonable grounds based on factual indications to conclude that the presence of the person on the territory of the Member States poses a security or high epidemic risk in accordance with Directive 2004/38/EC.

2. When a third-country national referred to in point (c) of Article 2(1) applies for a travel authorisation, the following specific rules shall apply:

(a) the applicant shall not reply to the question referred to in point (c) of Article 17(4);

(b) the fee referred to in Article 18 shall be waived.

3. When processing an application for a travel authorisation for a third-country national referred to in point (c) of Article 2(1), the ETIAS Central System 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 point (g) of Article 20(2);

(b) the applicant corresponds to a person whose data is recorded in Eurodac as referred to in point (k) of Article 20(2).

The specific risk indicators based on illegal immigration risks determined pursuant to Article 33 shall not apply.

4. An application for a travel authorisation shall not be refused on the ground of an illegal immigration risk as referred to in point (c) of Article 37(1).

5. Where automated processing under Article 20 has reported a hit corresponding to a refusal of entry and stay alert referred to in Article 24 of Regulation (EC) No 1987/2006 of the European Parliament and of the Council [1], the ETIAS National Unit shall verify the basis for the decision following which this alert was entered in SIS. If this basis is related to an illegal immigration risk, the alert shall not be taken into consideration for the assessment of the application. The ETIAS National Unit shall proceed according to Article 25(2) of the Regulation (EC) No 1987/2006.

6. The following rules shall also apply:

(a) in the notification laid down in Article 38(1) the applicant shall receive information regarding the fact that, when crossing the external border, he or she needs to be able to prove his or her status as family member referred to in point (c) of Article 2(1); such information 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 that family member is accompanied by or joining the Union citizen or other third-country national exercising his or her right of free movement;

(b) an appeal as referred to in Article 37(3) shall be lodged in accordance with Directive 2004/38/EC;

(c) the retention period of the application file referred to in Article 54(1) shall be:

(i) the period of validity of the travel authorisation;

(ii) five years from the last decision to refuse, annul or revoke the travel authorisation in accordance with Articles 37, 40 and 41. If the data present in a record, file or alert registered in one of the EU information systems, Europol data, the Interpol SLTD or TDAWN databases, the ETIAS watchlist, or the ETIAS screening rules giving rise to such a decision are deleted before the end of that five-year period, the application file shall be deleted within seven days from the date of the deletion of the data in that record, file or alert. For that purpose, the ETIAS Central System shall regularly and automatically verify whether the conditions for the retention of application files referred to in this point are still fulfilled. Where they are no longer fulfilled, it shall delete the application file in an automated manner.

[1] Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 381, 28.12.2006, p. 4).

For the purpose of facilitating a new application after the expiry of the validity period of an ETIAS travel authorisation, the application file may be stored in the ETIAS Central System for an additional period of no more than three years after the end of the validity period of the travel authorisation and only where, following a request for consent, the applicant freely and explicitly consents by means of an electronically signed declaration. Requests for consent shall be presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form and using clear and plain language, in accordance with Article 7 of Regulation (EU) 2016/679.

Consent shall be requested following the provision of information under Article 15(2). The automatically provided information shall remind the applicant of the purpose of the data retention in line with the information referred to in point (o) of Article 71.

CHAPTER IV

EXAMINATION OF THE APPLICATION BY THE ETIAS NATIONAL UNITS

Article 25

Member State responsible

1. The Member State responsible for the manual processing of applications under Article 26 (the 'Member State responsible') 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 20, that Member State shall be the Member State responsible;

(b) where several Member States are identified as having entered or supplied the data that triggered the hits pursuant to Article 20, the Member State responsible shall be:

(i) the Member State that has entered or supplied the most recent data on an alert referred to in point (d) of Article 20(2); or

(ii) if none of those data correspond to an alert referred to in point (d) of Article 20(2), the Member State that has entered or supplied the most recent data on an alert referred to in point (c) of Article 20(2); or

(iii) if none of those data correspond to an alert referred to in either point (c) or (d) of Article 20(2), the Member State that has entered or supplied the most recent data on an alert referred to in point (a) of Article 20(2);

(c) where several Member States are identified as having entered or supplied the data that triggered the hits pursuant to Article 20, but none of those data correspond to alerts referred to in point (a), (c) or (d) of Article 20(2), the Member State responsible shall be the one that entered or supplied the most recent data.

For the purposes of points (a) and (c) of the first subparagraph, hits triggered by data not entered or supplied by a Member State shall not be taken into account in order to identify the Member State responsible. Where the manual processing of an application is not triggered by data entered or supplied by a Member State, the Member State responsible shall be the Member State of first intended stay.

2. The ETIAS Central System shall indicate the Member State responsible in the application file. Where the ETIAS Central System is not able to identify the Member State responsible as referred to in paragraph 1, the ETIAS Central Unit shall identify it.

Article 26

Manual processing of applications by the ETIAS National Units

1. Where the automated processing laid down in Article 20(2) to (5) has reported one or several hits, the application shall be processed manually by the ETIAS National Unit of the Member State responsible. That ETIAS National Unit shall have access to the application file and any linked application files, as well as to any hits triggered during the automated processing laid down in Article 20(2) to (5). The ETIAS Central Unit shall inform the ETIAS National Unit of the Member State responsible 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 20(2) or (4). Where one or several Member States have been identified as having entered or supplied the data that triggered such a hit, the ETIAS Central Unit shall also specify the Member States concerned.

2. Following the manual processing of the application, the ETIAS National Unit of the Member State responsible shall:

(a) issue a travel authorisation; or

(b) refuse a travel authorisation.

3. Where the automated processing laid down in Article 20(2) has reported a hit, the ETIAS National Unit of the Member State responsible shall:

(a) refuse a travel authorisation where the hit corresponds to one or several of the verifications referred to in points (a) and (c) of Article 20(2);

(b) assess the security or illegal immigration risk and decide whether to issue or refuse a travel authorisation where the hit corresponds to any of the verifications referred to in points (b) and (d) to (m) of Article 20(2).

4. Where automated processing under Article 20(3) has reported that the applicant replied affirmatively to one of the questions referred to in Article 17(4), the ETIAS National Unit of the Member State responsible shall assess the security or illegal immigration risk and decide whether to issue or refuse a travel authorisation.

5. Where automated processing under Article 20(4) has reported a hit, the ETIAS National Unit of the Member State responsible shall assess the security risk and decide whether to issue or refuse a travel authorisation.

6. Where automated processing under Article 20(5) has reported a hit, the ETIAS National Unit of the Member State responsible shall assess the security, illegal immigration or high epidemic risk and decide whether to issue or refuse a travel authorisation. In no circumstances may the ETIAS National Unit of the Member State responsible take a decision automatically on the basis of a hit based on specific risk indicators. The ETIAS National Unit of the Member State responsible shall individually assess the security, illegal immigration and high epidemic risks in all cases.

7. The ETIAS Information System shall keep records of all data processing operations carried out for assessments under this Article by the ETIAS National Unit of the Member State responsible or by the ETIAS National Units of the Member States consulted in accordance with Article 28. Those records shall be created and entered automatically in the application file. They shall show the date and time of each operation, the data used for consultation of other EU information systems, the data linked to the hit received and the staff member having performed the risk assessment.

The results of the assessment of the security, illegal immigration or high epidemic risk and the justification behind the decision to issue or refuse a travel authorisation shall be recorded in the application file by the staff member having performed the risk assessment.

Article 27

Request for additional information or documentation from the applicant

1. Where the ETIAS National Unit of the Member State responsible deems the information provided by the applicant in the application form to be insufficient to enable it to decide whether to issue or refuse a travel authorisation, it may request additional information or documentation from the applicant. The ETIAS National Unit of the Member State responsible shall request additional information or documentation upon the request of a Member State consulted in accordance with Article 28.

2. The request for additional information or documentation shall be notified through the email service referred to in point (f) of Article 6(2) to the contact email 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 an official language of the third country of which the applicant has declared to be a national. Where additional documentation is requested, an electronic copy of the original documentation shall also be requested. The applicant shall provide the additional information or documentation directly to the ETIAS National Unit of the Member State responsible through the secure account service referred to in point (g) of Article 6(2) within 10 days 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. The applicant shall not be required to provide an official translation. Only additional information or documentation necessary for the assessment of the ETIAS application may be requested.

3. For the purpose of requesting additional information or documentation as referred to in paragraph 1, the ETIAS National Unit of the Member State responsible shall use a predetermined list of options. The Commission shall adopt delegated acts in accordance with Article 89 to lay down the content and format of that predetermined list of options.

4. In exceptional circumstances and as a last resort after processing the additional information or documentation, when serious doubts remain regarding the information or documentation provided by the applicant, the ETIAS National Unit of the Member State responsible may invite the applicant to an interview in his or her country of residence at its consulate located the nearest to the place of residence of the applicant. Exceptionally and when in the interest of the applicant, the interview may take place in a consulate located in a different country than the country of residence of the applicant.

If the consulate located the nearest to the place of residence of the applicant is at a distance of more than 500 km, the applicant shall be offered the possibility to conduct the interview by remote means of audio and video communication. If the distance is less than 500 km, the applicant and the ETIAS National Unit of the Member State responsible may jointly agree to the use of such means of audio and video communication. Where such means of audio and video communication are used, the interview shall be conducted by the ETIAS National Unit of the Member State responsible or, exceptionally, by one of that Member State's consulates. The remote means of audio and video communication shall ensure an appropriate level of security and confidentiality.

The reason for requesting an interview shall be recorded in the application file.

5. The Commission shall, by means of implementing acts, define the requirements for the means of audio and video communication referred to in paragraph 4, including as regards data protection, security and confidentiality rules and adopt rules on testing and selecting suitable tools and on their operation.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 90(2).

6. The invitation to an interview shall be issued to the applicant by the ETIAS National Unit of the Member State responsible through the email service referred to in point (f) of Article 6(2) to the contact email address recorded in the application file. The invitation to the interview shall be issued within 72 hours of the applicant's submission of additional information or documentation pursuant to paragraph 2 of this Article. The invitation to the interview shall include information on the Member State issuing the invitation, on the options referred to in paragraph 4 of this Article and relevant contact details. The applicant shall contact the ETIAS National Unit of the Member State responsible or the consulate as soon as possible, but no later than five days after the invitation to the interview was issued, to agree on a mutually suitable time and date for the interview and on whether the interview shall take place remotely. The interview shall take place within 10 days of the date of the invitation.

The invitation to the interview shall be recorded in the application file by the ETIAS Central System.

7. Where the applicant fails to attend the interview in accordance with paragraph 6 of this Article following an invitation to the interview, the application shall be refused in accordance with point (g) of Article 37(1). The ETIAS National Unit of the Member State responsible shall inform the applicant without delay.

8. For the purpose of the interview referred to in paragraph 4, the ETIAS National Unit of the Member State responsible shall indicate the elements to be addressed by the interviewer. Those elements shall relate to the reasons for which the interview was requested.

The interview by remote means of audio and video communication shall be conducted in the language of the ETIAS National Unit of the Member State responsible requesting the interview or its chosen language for the submission of additional information or documentation.

The interview taking place in a consulate shall be conducted in an official language of the third country in which the consulate is located, or any other language agreed by the applicant and the consulate.

Following the interview, the interviewer shall issue an opinion which provides justifications for his or her recommendations.

The elements addressed and the opinion shall be included in a form to be recorded in the application file on the same day as the date of the interview.

9. Upon the applicant's submission of 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 6 shall be added to the application file by the ETIAS National Unit of the Member State responsible.

The form used for the interview and the additional information or documentation recorded in the application file shall be consulted only for the purpose of assessing and deciding on the application, for the purpose of managing an appeal procedure and for the purpose of processing a new application by the same applicant.

10. The ETIAS National Unit of the Member State responsible 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 28

Consultation of other Member States

1. Where one or several Member States are identified as having entered or supplied the data having triggered a hit in accordance with Article 20(7) following verification under Article 22, 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 Member State responsible.

2. The ETIAS National Units of the Member States consulted shall have access to the application file for the purpose of the consultation.

3. 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.

4. The ETIAS National Unit of the Member State responsible 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 Member State consulted pursuant to Article 27(1), the ETIAS National Unit of the Member State responsible shall consult the ETIAS National Unit of the consulted Member State following the reply of the applicant to that request for additional information. In such 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 ETIAS National Unit of the Member State responsible in relation to the matter for which they are being consulted. Where several Member States are consulted, the ETIAS National Unit of the Member State responsible shall ensure the coordination.

5. The ETIAS National Unit of the Member States consulted shall reply within 60 hours of the notification of the consultation. A failure to reply within the deadline shall be considered to be a positive opinion on the application.

6. During the consultation process, the consultation request and the replies thereto shall be transmitted through the software referred to in point (m) of Article 6(2) and shall be made available to the ETIAS National Unit of the Member State responsible.

7. Where the ETIAS National Unit of at least one Member State consulted provides a negative opinion on the application, the ETIAS National Unit of the Member State responsible shall refuse the travel authorisation pursuant to Article 37. This paragraph is without prejudice to Article 44.

8. Where necessary in cases of technical problems or unforeseen circumstances, the ETIAS Central Unit shall determine the Member State responsible and Member States to be consulted and shall facilitate the consultations between Member States referred to in this Article.

Article 29

Consultation of Europol

1. Where Europol is identified as having supplied the data having triggered a hit in accordance with Article 20(8) of this Regulation, the ETIAS Central Unit shall notify it, thereby launching a consultation process between Europol and the ETIAS National Unit of the Member State responsible. Such consultation shall take place in accordance with Regulation (EU) 2016/794 and in particular its Chapter IV.

2. Where Europol is consulted, the ETIAS Central Unit shall transmit to Europol the relevant data of the application file and of the hits which are necessary for the purpose of the consultation.

3. In any case, Europol shall not have access to the personal data concerning the education of the applicant referred to in point (h) of Article 17(2).

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 Member State responsible which shall record it in the application file.

5. The ETIAS National Unit of the Member State responsible may consult Europol following the reply of an applicant to a request for additional information. In such cases, the ETIAS National Unit shall transmit to Europol the relevant additional information or documentation provided by the applicant relating to the request for a travel authorisation on which Europol is being consulted.

6. Europol shall reply within 60 hours of the notification of the consultation. The failure by Europol to reply within the deadline shall be considered to be a positive opinion on the application.

7. During the consultation process, the consultation request and the replies thereto shall be transmitted through the software referred to in point (m) of Article 6(2) and shall be made available to the ETIAS National Unit of the Member State responsible.

8. Where Europol provides a negative opinion on the application and the ETIAS National Unit of the Member State responsible decides to issue the travel authorisation, it shall justify its decision and shall record the justification in the application file.

9. Where necessary in cases of technical problems or unforeseen circumstances, the ETIAS Central Unit shall determine the Member State responsible and facilitate the consultations between the Member State responsible and Europol referred to in this Article.

Article 30

Deadlines for notification to the applicant

Within 96 hours of the submission of an application which is admissible in accordance with Article 19, the applicant shall receive a notification indicating:

(a) whether his or her travel authorisation has been issued or refused; or

(b) that additional information or documentation is requested and that the applicant may be invited to an interview, indicating the maximum processing times applicable under Article 32(2).

Article 31

Verification tool

The Commission shall arrange for a verification tool for applicants to check the status of their applications and to check the period of validity and status of their travel authorisations (valid, refused, annulled or revoked). This tool shall be made accessible via the dedicated public website or via the app for mobile devices referred to in Article 16.

The Commission shall adopt delegated acts in accordance with Article 89 to further define the verification tool.

Article 32

Decision on the application

1. Applications shall be decided on no later than 96 hours after the submission of an application which is admissible in accordance with Article 19.

2. Exceptionally, when a request for additional information or documentation is notified, and when the applicant is invited to an interview, the period laid down in paragraph 1 of this Article shall be extended. Such applications shall be decided on no later than 96 hours after the submission of the additional information or documentation by the applicant. When the applicant is invited to an interview as referred to in Article 27(4), the application shall be decided on no later than 48 hours after the interview has taken place.

3. Before expiry of the deadlines referred to in paragraphs 1 and 2 of this Article, a decision shall be taken to:

(a) issue a travel authorisation in accordance with Article 36; or

(b) refuse a travel authorisation in accordance with Article 37.

CHAPTER V

THE ETIAS SCREENING RULES AND THE ETIAS WATCHLIST

Article 33

The ETIAS screening rules

1. The ETIAS screening rules shall be an algorithm enabling profiling as defined in point 4 of Article 4 of Regulation (EU) 2016/679 through the comparison in accordance with Article 20 of this Regulation of the data recorded in an application file of the ETIAS Central System with specific risk indicators established by the ETIAS Central Unit under paragraph 4 of this Article pointing to security, illegal immigration or high epidemic risks. The ETIAS Central Unit shall register the ETIAS screening rules in the ETIAS Central System.

2. The Commission shall adopt a delegated act in accordance with Article 89 to further define the risks related to security or illegal immigration or a high epidemic risk on the basis of:

(a) statistics generated by the EES indicating abnormal rates of overstaying and refusals of entry for a specific group of travellers;

(b) statistics generated by ETIAS in accordance with Article 84 indicating abnormal rates of refusals of travel authorisations due to a security, illegal immigration or high epidemic risk associated with a specific group of travellers;

(c) statistics generated by ETIAS in accordance with Article 84 and the EES indicating correlations between information collected through the application form and overstaying by travellers or refusals of entry;

(d) information substantiated by factual and evidence-based elements provided by Member States concerning specific security risk indicators or threats identified by that Member State;

(e) information substantiated by factual and evidence-based elements provided by Member States concerning abnormal rates of overstaying and refusals of entry for a specific group of travellers for that Member State;

(f) information concerning specific high epidemic risks provided by Member States as well as epidemiological surveillance information and risk assessments provided by the ECDC and disease outbreaks reported by the WHO.

3. The Commission shall, by means of an implementing act, specify the risks, as defined in this Regulation and in the delegated act referred to in paragraph 2 of this Article, on which the specific risks indicators referred to in paragraph 4 of this Article shall be based. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 90(2).

The specific risks shall be reviewed at least every six months and, where necessary, a new implementing act shall be adopted by the Commission in accordance with the examination procedure referred to in Article 90(2).

4. Based on the specific risks determined in accordance with paragraph 3, the ETIAS Central Unit shall establish a set of specific risk indicators consisting of a combination of data including one or several of the following:

(a) age range, sex, nationality;

(b) country and city of residence;

(c) level of education (primary, secondary, higher or none);

(d) current occupation (job group).

5. The specific risk indicators shall be targeted and proportionate. They shall in no circumstances be based solely on a person's sex or age. They shall in no circumstances be based on information revealing a person's colour, race, ethnic or social origin, genetic features, language, political or any other opinion, religion or philosophical belief, trade union membership, membership of a national minority, property, birth, disability or sexual orientation.

6. The specific risk indicators shall be defined, established, assessed *ex ante*, implemented, evaluated *ex post*, revised and deleted by the ETIAS Central Unit after consultation of the ETIAS Screening Board.

Article 34

The ETIAS watchlist

1. The ETIAS watchlist shall consist of data related to persons who are suspected of having committed or taken part in a terrorist offence or other serious criminal offence or persons regarding whom there are factual indications or reasonable grounds, based on an overall assessment of the person, to believe that they will commit a terrorist offence or other serious criminal offence. The ETIAS watchlist shall form part of the ETIAS Central System.

2. The ETIAS watchlist shall be established on the basis of information related to terrorist offences or other serious criminal offences.

3. The information referred to in paragraph 2 shall be entered into the ETIAS watchlist by Europol without prejudice to Regulation (EU) 2016/794 or by Member States. Each of Europol or the Member State concerned shall be responsible for all the data they enter. The ETIAS watchlist shall indicate, for each item of data, the date and time of entry by Europol or by the Member State that entered it.

4. On the basis of the information referred to in paragraph 2, the ETIAS watchlist shall be composed of data consisting of one or more of the following items:

(a) surname;

(b) surname at birth;

(c) date of birth;

(d) other names (alias(es), artistic name(s), usual name(s));

(e) travel document(s) (type, number and country of issuance of the travel document(s));

(f) home address;

(g) email address:

(h) phone number;

(i) the name, email address, mailing address, phone number of a firm or organisation;

(j) IP address.

If available, the following items of data shall be added to the related items constituted of at least one of the items of data listed above: first name(s), place of birth, country of birth, sex and nationality.

Article 35

Responsibilities and tasks regarding the ETIAS watchlist

1. Before Europol or a Member State enters data into the ETIAS watchlist, it shall:

(a) determine whether the information is adequate, accurate and important enough to be included in the ETIAS watchlist;

(b) assess the potential impact of the data on the proportion of applications manually processed;

(c) verify whether the data correspond to an alert entered in SIS.

2. eu-LISA shall create a specific tool for the purpose of assessment under point (b) of paragraph 1.

3. Where verification under point (c) of paragraph 1 reveals that the data correspond to an alert entered in SIS, it shall not be entered into the ETIAS watchlist. Where the conditions for using the data to enter an alert in SIS are fulfilled, priority shall be given to entering an alert in SIS.

4. Member States and Europol shall be responsible for the accuracy of the data referred to in Article 34(2) that they enter into the ETIAS watchlist and for keeping them up to date.

5. Europol shall review and verify the continued accuracy of the data it has entered into the ETIAS watchlist regularly, and at least once a year. Member States shall likewise review and verify the continued accuracy of the data they have entered into the ETIAS watchlist regularly and at least once a year. Europol and Member States shall develop and implement a joint procedure to ensure fulfilment of their responsibilities under this paragraph.

6. Following a review, Member States and Europol shall withdraw data from the ETIAS watchlist if it is proven that the reasons for which they were entered no longer hold, or that the data are obsolete or not up to date.

7. The ETIAS watchlist and the assessment tool referred to in paragraphs 1 and 2 of this Article shall be developed technically and hosted by eu-LISA. The Commission shall, by means of implementing acts, establish the technical specifications of the ETIAS watchlist and of that assessment tool. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 90(2).

CHAPTER VI

ISSUE, REFUSAL, ANNULMENT OR REVOCATION OF A TRAVEL AUTHORISATION

Article 36

Issue 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 based on factual indications to conclude that the presence of the person on the territory of the Member States poses a security, illegal immigration or high epidemic risk, a travel authorisation shall be issued by the ETIAS Central System or the ETIAS National Unit of the Member State responsible.

2. In cases where there is doubt as to whether sufficient reasons to refuse the travel authorisation exist, the ETIAS National Unit of the Member State responsible shall have the possibility, including after an interview, to issue a travel authorisation with a flag recommending to border authorities to proceed with a second line check.

The ETIAS National Unit of the Member State responsible may also attach such a flag upon the request of a consulted Member State. Such a flag shall only be visible to the border authorities.

The flag shall be removed automatically once the border authorities have carried out the check and have entered the entry record in the EES.

3. The ETIAS National Unit of the Member State responsible shall have the possibility to add a flag indicating to border authorities and other authorities with access to the data in the ETIAS Central System that a specific hit triggered during the processing of the application has been assessed and that it has been verified that the hit constituted a false hit or that the manual processing has shown that there were no grounds for the refusal of the travel authorisation.

4. The Commission shall adopt delegated acts in accordance with Article 89 to establish adequate safeguards by providing rules and procedures to avoid conflicts with alerts in other information systems and to define the conditions, the criteria and the duration of flagging pursuant to this Regulation.

5. A travel authorisation shall be valid for three 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.

6. A travel authorisation shall not confer an automatic right of entry or stay.

Article 37

Refusal of a travel authorisation

1. A travel authorisation shall be refused if the applicant:

(a) used a travel document which is reported as lost, stolen, misappropriated or invalidated in SIS;

(b) poses a security risk;

(c) poses an illegal immigration risk;

(d) poses a high epidemic risk;

(e) is a person for whom an alert has been entered in SIS for the purpose of refusing entry and stay;

(f) fails to reply to a request for additional information or documentation within the deadlines referred to in Article 27;

(g) fails to attend an interview as referred to in Article 27(4).

2. A travel authorisation shall also be refused if, at the time of the application, there are reasonable and serious 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.

3. 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 Member State responsible shall provide applicants with information regarding the appeal procedure. The information shall be provided in one of the official languages of the countries listed in Annex II to Regulation (EC) No 539/2001 of which the applicant is a national.

4. A previous refusal of a travel authorisation shall not lead to an automatic refusal of a new application. A new application shall be assessed on the basis of all the available information.

Article 38

Notification on the issue or refusal of a travel authorisation

1. Once a travel authorisation is issued, the applicant shall immediately receive a notification via the email service, including:

(a) a clear statement that the travel authorisation has been issued and the travel authorisation application number;

(b) the commencement and expiry dates of the travel authorisation;

(c) a clear statement that upon entry the applicant will have to present the same travel document as that indicated in the application form and that any change of travel document will require a new application for a travel authorisation;

(d) a reminder of the entry conditions laid down in Article 6 of Regulation (EU) 2016/399 and the fact that a short stay is only possible for a duration of no more than 90 days in any 180-day period;

(e) a reminder that the mere possession of a travel authorisation does not confer an automatic right of entry;

(f) a reminder that the border authorities may request supporting documents at external borders in order to verify fulfilment of the conditions of entry and stay;

(g) a reminder that the possession of a valid travel authorisation is a condition for stay that has to be fulfilled during the entire duration of a short stay on the territory of Member States;

(h) a link to the web service referred to in Article 13 of Regulation (EU) 2017/2226 enabling third-country nationals to verify at any moment their remaining authorised stay;

(i) where applicable, the Member States to which the applicant is authorised to travel;

(j) a link to the ETIAS public website containing information on the possibility for the applicant to request the revocation of the travel authorisation, the possibility for the travel authorisation to be revoked if the conditions for issuing it are no longer met and the possibility for its annulment where it becomes evident that the conditions for issuing it were not met at the time it was issued;

(k) information on the procedures for exercising the rights under Articles 13 to 16 of Regulation (EC) No 45/2001 and Articles 15 to 18 of Regulation (EU) 2016/679; 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 Member State of first intended stay where the travel authorisation has been issued by the ETIAS Central System, or of the Member State responsible where the travel authorisation has been issued by an ETIAS National Unit.

2. Where a travel authorisation has been refused, the applicant shall immediately receive a notification via the email service including:

(a) a clear statement that the travel authorisation has been refused and the travel authorisation application number;

(b) a reference to the ETIAS National Unit of the Member State responsible that refused the travel authorisation and its address;

(c) a statement of the grounds for refusal of the travel authorisation indicating the applicable grounds from those listed in Article 37(1) and (2) enabling the applicant to lodge an appeal;

(d) information on the right to lodge an appeal and the time limit for doing so; a link to the information referred to in Article 16(7) on the website;

(e) information on the procedures for exercising the rights under Articles 13 to 16 of Regulation (EC) No 45/2001 and Articles 15 to 18 of Regulation (EU) 2016/679; 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 Member State responsible.

3. The Commission shall, by means of implementing acts, adopt a standard form for refusal, annulment or revocation of a travel authorisation. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 90(2).

Article 39

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

1. Where a decision has been taken to issue a travel authorisation, the ETIAS Central System or, where the decision has been taken following manual processing as provided for in Chapter IV, the ETIAS National Unit of the Member State responsible shall add the following data to the application file without delay:

(a) status information indicating that the travel authorisation has been issued;

(b) a reference as to whether the travel authorisation was issued by the ETIAS Central System or following manual processing; in the latter case a reference to the ETIAS National Unit of the Member State responsible which took the decision and its address;

(c) the date of the decision to issue the travel authorisation;

(d) the commencement and expiry dates of the travel authorisation;

(e) any flags attached to the travel authorisation as laid down in Article 36(2) and (3), together with an indication of the reasons for such flag(s), and additional information relevant to second line checks in the case of Article 36(2), and additional information relevant to border authorities in the case of Article 36(3).

2. The Commission shall adopt delegated acts in accordance with Article 89 to further define the type of additional information that may be added, its language and formats, as well as the reasons for the flags.

3. Where a decision has been taken to refuse a travel authorisation, the ETIAS National Unit of the Member State responsible 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 of the Member State responsible that refused the travel authorisation and its address;

(c) date of the decision to refuse the travel authorisation;

(d) the grounds for refusal of the travel authorisation, by indicating the grounds from those listed in Article 37(1) and (2).

4. In addition to the data referred to in paragraphs 1 and 3, where a decision has been taken to issue or to refuse a travel authorisation, the ETIAS National Unit of the Member State responsible 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 40

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 37(1) and (2).

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 and in accordance with the national law of that Member State. The ETIAS National Unit of the Member State responsible shall provide applicants with information regarding the appeal procedure. The information shall be provided in one of the official languages of the countries listed in Annex II to Regulation (EC) No 539/2001 of which the applicant is a national.

4. The justification for the decision to annul a travel authorisation shall be recorded in the application file by the staff member having performed the risk assessment.

Article 41

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 37(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 alert is issued in SIS concerning a new refusal of entry and stay or concerning a travel document reported as lost, stolen, misappropriated or invalidated, 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 entered the alert. Where a new alert for refusal of entry and stay has been issued, the ETIAS National Unit shall revoke the travel authorisation. Where the travel authorisation is linked to a travel document reported as lost, stolen, misappropriated or invalidated in SIS or SLTD, the ETIAS National Unit shall manually process the application file.

4. New data entered into 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 those new data correspond 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 data, or where Europol entered the new data, to the ETIAS National Unit of the Member State of first intended stay as declared by the applicant in accordance with point (j) of Article 17(2). That ETIAS National Unit shall assess the security risk and shall revoke the travel authorisation where it concludes that the conditions for granting it are no longer met.

5. Where a refusal of entry record is entered in the EES concerning the holder of a valid travel authorisation and that record is justified by reason B or I listed in Annex V, Part B, to Regulation (EU) 2016/399, the ETIAS Central System shall transfer the application file to the ETIAS National Unit of the Member State having refused entry. 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.

6. The justification for the decision to revoke a travel authorisation shall be recorded in the application file by the staff member having performed the risk assessment.

7. 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. The ETIAS National Unit of the Member State responsible shall provide applicants with information regarding the appeal procedure. The information shall be provided in one of the official languages of the countries listed in Annex II to Regulation (EC) No 539/2001 of which the applicant is a national.

8. A travel authorisation may be revoked at the request of the applicant. No appeal shall be possible against a revocation on this basis. If the applicant is present on the territory of a Member State when such a request is introduced, the revocation shall become effective once the applicant has exited the territory and from the moment the corresponding entry/exit record has been created in the EES in accordance with Articles 16(3) and 17(2) of Regulation (EU) 2017/2226.

Article 42

Notification of 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 email service including:

(a) a clear statement that the travel authorisation has been annulled or revoked and the travel authorisation application number;

(b) a reference to the ETIAS National Unit of the Member State responsible that annulled or revoked the travel authorisation and its address;

(c) a statement of the grounds for the annulment or revocation of the travel authorisation indicating the applicable grounds from those listed in Article 37(1) and (2) enabling the applicant to lodge an appeal;

(d) information on the right to lodge an appeal and the time limit for doing so; a link to the information referred to in Article 16(7) on the website;

(e) a clear statement that the possession of a valid travel authorisation is a condition for stay that has to be fulfilled during the entire duration of a short stay on the territory of Member States;

(f) information on the procedures for exercising the rights under Articles 13 to 16 of Regulation (EC) No 45/2001 and Articles 15 to 18 of Regulation (EU) 2016/679; 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 Member State responsible.

Article 43

Data to be added to the application file following the decision to annul or to revoke a travel authorisation

1. Where a decision has been taken to annul or to revoke a travel authorisation, the ETIAS National Unit of the Member State responsible that annulled or revoked 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 of the Member State responsible that revoked or annulled the travel authorisation and its address; and

(c) date of the decision to annul or revoke the travel authorisation.

2. The ETIAS National Unit of the Member State responsible that annulled or revoked the travel authorisation shall also indicate in the application file either the ground(s) for annulment or revocation that are applicable under Article 37(1) and (2) or that the travel authorisation was revoked at the request of the applicant under Article 41(8).

Article 44

Issue 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 19, the Member State to which the third-country national concerned intends to travel may exceptionally issue a travel authorisation with limited territorial validity when that Member State considers it necessary on humanitarian grounds in accordance with its national law, for reasons of national interest or because of international obligations, notwithstanding the fact that:

(a) the manual processing pursuant to Article 26 is not yet completed; or

(b) a travel authorisation has been refused, annulled or revoked.

Such authorisations will generally be valid only in the territory of the issuing Member State. However, they may also exceptionally be issued with a territorial validity covering more than one Member State, subject to the consent of each such Member State through their ETIAS National Units. Where an ETIAS National Unit is considering issuing a travel authorisation with limited territorial validity covering several Member States, that ETIAS National Unit of the Member State responsible shall consult those Member States.

Where a travel authorisation with limited territorial validity has been requested or issued in the circumstances referred to in point (a) of the first subparagraph of this paragraph, this shall not interrupt the manual processing of the application allowing issue of a travel authorisation without limited territorial validity.

2. For the purposes of paragraph 1, and as referred to in the public website and the app for mobile devices, 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 humanitarian grounds or is linked to international obligations. Where such contact has been made, 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 in the application file.

3. 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. Such requests shall be notified through the email service referred to in point (f) of Article 6(2) to the contact email address recorded in the application file, and shall indicate 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 an official language of the third country of which the applicant has declared to be a national. The applicant shall not be required to provide an official translation into those languages. The applicant shall provide the additional information or documentation directly to the ETIAS National Unit through the secure account service referred to in point (g) of Article 6(2). Upon submission of the additional information or documentation, the ETIAS Central System shall record and store that information or documentation in the application file. The additional information or documentation recorded in the application file shall be consulted only for the purpose of assessing and deciding on the application, for the purpose of managing an appeal procedure or for the purpose of processing a new application by the same applicant.

4. A travel authorisation with limited territorial validity shall be valid for a maximum of 90 days from the date of first entry on the basis of that authorisation.

5. Travel authorisations issued under this Article may be the subject of a flag under Article 36(2) or (3).

6. Where a travel authorisation with limited territorial validity is issued, the following data shall be added to the application file by the ETIAS National Unit which issued that authorisation:

(a) status information indicating that a travel authorisation with limited territorial validity has been issued;

(b) the Member State(s) to which the travel authorisation holder is entitled to travel and the validity period of that travel authorisation;

(c) the ETIAS National Unit of the Member State that issued the travel authorisation with limited territorial validity and its address;

(d) date of the decision to issue the travel authorisation with limited territorial validity;

(e) a reference to the humanitarian grounds, reasons of national interest or international obligations invoked;

(f) any flags attached to the travel authorisation, as laid down in Article 36(2) and (3), together with an indication of the reasons for such flag(s) and additional information relevant to second line checks in the case of Article 36(2), and additional information relevant to border authorities in the case of Article 36(3).

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.

7. Where a travel authorisation with limited territorial validity has been issued, the applicant shall receive a notification via the email service, including:

(a) a clear statement 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 travel authorisation with limited territorial validity;

(c) a clear statement of the Member States to which the holder of the authorisation is entitled to travel and that he or she can only travel within the territory of those Member States;

(d) a reminder that the possession of a valid travel authorisation is a condition for stay that has to be fulfilled during the entire duration of a short stay on the territory of the Member State for which the travel authorisation with limited territorial validity has been issued;

(e) a link to the web service referred to in Article 13 of Regulation (EU) 2017/2226 enabling third-country nationals to verify at any moment their remaining authorised stay.

CHAPTER VII

USE OF ETIAS BY CARRIERS

Article 45

Access to data for verification by carriers

1. Air carriers, sea carriers and international carriers transporting groups overland by coach shall send a query to the ETIAS Information 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. Secure access to the carrier gateway referred to in point (k) of Article 6(2), including the possibility to use mobile technical solutions, shall allow carriers to proceed with the query referred to in paragraph 1 of this Article prior to the boarding of a passenger. The carrier shall provide the data contained in the machine-readable zone of the travel document and indicate the Member State of entry. By way of derogation, in the case of airport transit, the carrier shall not be obliged to verify whether the third-country national is in possession of a valid travel authorisation.

The ETIAS Information System shall, through the carrier gateway, provide the carriers with an 'OK/NOT OK' answer indicating whether or not the person has a valid travel authorisation. If a travel authorisation has been issued with limited territorial validity in accordance with Article 44, the response provided by the ETIAS Central System shall take into account the Member State(s) for which the authorisation is valid as well as the Member State of entry indicated by the carrier. Carriers may store the information sent and the answer received in accordance with the applicable law. The OK/NOT OK answer shall not be regarded as a decision to authorise or refuse entry in accordance with Regulation (EU) 2016/399.

The Commission shall, by means of implementing acts, adopt detailed rules concerning the conditions for the operation of the carrier gateway and the data protection and security rules applicable. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 90(2).

3. The Commission shall, by means of implementing acts, set up an authentication scheme reserved exclusively for carriers in order to allow access to the carrier gateway for the purposes of paragraph 2 of this Article to the duly authorised members of the carriers' staff. When setting up the authentication scheme, information security risk management and the principles of data protection by design and by default shall be taken into account. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 90(2).

4. The carrier gateway shall make use of a separate read-only database updated on a daily basis via a one-way extraction of the minimum necessary subset of data stored in ETIAS. eu-LISA shall be responsible for the security of the carrier gateway, for the security of the personal data it contains and for the process of extracting the personal data into the separate read-only database.

5. The carriers referred to in paragraph 1 of this Article shall be subject to the penalties provided for in accordance with Article 26(2) of the 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 ('the Convention implementing the Schengen Agreement') and Article 4 of Council Directive 2001/51/EC [1] when they transport third-country nationals who, although subject to the travel authorisation requirement, are not in possession of a valid travel authorisation.

6. By way of derogation from paragraph 5 of this Article, where, for the same third-country national, the carriers referred to in paragraph 1 of this Article are already subject to the penalties provided for in accordance with Article 26(2) of the Convention Implementing the Schengen Agreement and Article 4 of Directive 2001/51/EC, the penalties referred to in paragraph 5 of this Article shall not apply.

7. For the purpose of implementing paragraph 5 or for the purpose of resolving any potential dispute arising from its application, eu-LISA shall keep logs of all data processing operations carried out within the carrier gateway by carriers. Those logs shall show the date and time of each operation, the data used for interrogation, the data transmitted by the carrier gateway and the name of the carrier in question.

[1] Council Directive 2001/51/EC of 28 June 2001 supplementing the provisions of Article 26 of the Convention implementing the Schengen Agreement of 14 June 1985 (OJ L 187, 10.7.2001, p. 45).

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

8. 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 border authorities, the carriers shall be obliged to return the third-country nationals to one of either the third country from which they were transported, the third country which issued the travel document on which they travelled, or any other third country to which they are certain to be admitted.

9. By way of derogation from paragraph 1, for carriers transporting groups overland by coach, for the first three years following the ETIAS entry into operations, the verification referred to in paragraph 1 shall be optional and the provisions referred to in paragraph 5 shall not apply to them.

Article 46

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

1. Where it is technically impossible to proceed with the query referred to in Article 45(1) because of a failure of any part of the ETIAS Information System, the carriers shall be exempted of the obligation to verify the possession of a valid travel authorisation. Where such a failure is detected by eu-LISA, the ETIAS Central Unit shall notify the carriers. It shall also notify the carriers once the failure is remedied. Where such a failure is detected by the carriers, they may notify the ETIAS Central Unit.

2. The penalties referred to in Article 45(5) shall not be imposed on carriers in the cases referred to in paragraph 1 of this Article.

3. Where for other reasons than a failure of any part of the ETIAS Information System it is technically impossible for a carrier to proceed with the consultation query referred to in Article 45(1) for a prolonged period of time, that carrier shall inform the ETIAS Central Unit.

4. The Commission shall, by means of an implementing act, lay down details of the fall-back procedures referred to in this Article. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 90(2).

CHAPTER VIII

USE OF ETIAS BY BORDER AUTHORITIES AT THE EXTERNAL BORDERS

Article 47

Access to data for verification at the external borders

1. The border authorities competent for carrying out border checks at external border crossing points in accordance with Regulation (EU) 2016/399 shall 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 issued under Article 44, the Member State(s) for which it is valid;

(b) any flag attached to the travel authorisation under Article 36(2) and (3);

(c) whether the travel authorisation will expire within the next 90 days and the remaining validity period;

(d) the data referred to in points (k) and (l) of Article 17(2).

3. Where the travel authorisation is due to expire within the next 90 days, the border authorities shall inform the holder of that travel authorisation of the remaining validity period, of the possibility to submit an application for a new travel authorisation even during a stay on the territory of Member States, and of the obligation to be in possession of a valid travel authorisation for the entire duration of a short stay. That information shall be provided either by the border guard at the moment of the border checks or by means of equipment installed at the border crossing point enabling the third-country national to consult the verification tool referred to in Article 31. The information shall in addition be provided through the public website referred to in Article 16. The ETIAS Central System shall also automatically provide the holder of a travel authorisation with the same information via the email service.

4. Where the ETIAS Central System responds by indicating a flag attached to a travel authorisation under Article 36(2), the border authorities shall proceed to a second line check. For the purposes of the second line check they shall be authorised to consult the additional information added to the application file in accordance with point (e) of Article 39(1) or point (f) of Article 44(6).

Where the ETIAS Central System responds by indicating a flag referred to in Article 36(3) and where additional verifications are needed, border authorities may access the ETIAS Central System to obtain the additional information provided for in point (e) of Article 39(1) or point (f) of Article 44(6).

Article 48

Fall-back procedures in the case of a technical impossibility to access data at the external borders

1. Where it is technically impossible to proceed with the consultation referred to in Article 47(1) because of a failure of any part of the ETIAS Information System, the ETIAS Central Unit shall notify the border authorities and the ETIAS National Units of the Member States.

2. Where it is technically impossible to perform the search referred to in Article 47(1) because of a failure of the national border infrastructure in a Member State, the border authorities shall notify the ETIAS Central Unit and that Member State's ETIAS National Unit. The ETIAS Central Unit shall then immediately inform eu-LISA and the Commission.

3. In both cases referred to in paragraphs 1 and 2 of this Article, the border authorities shall follow their national contingency plans. In accordance with Regulation (EU) 2016/399, the national contingency plan may authorise the border authorities to derogate temporarily from the obligation to consult the ETIAS Central System referred to in Article 47(1) of this Regulation.

4. The Commission shall, by means of implementing acts, adopt model contingency plans for the cases referred to in paragraphs 1 and 2 of this Article, including the procedures to be followed by border authorities. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 90(2). Member States shall adopt their national contingency plans using the model contingency plans as a basis, to be adapted as necessary at the national level.

CHAPTER IX

USE OF ETIAS BY IMMIGRATION AUTHORITIES

Article 49

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 with the data referred to in points (a) to (e) of Article 17(2).

2. Access to the ETIAS Central System under paragraph 1 of this Article shall be allowed only where the following conditions are met:

(a) a prior search has been conducted in the EES under Article 26 of Regulation (EU) 2017/2226; and

(b) the search result indicates that the EES does not contain an entry record corresponding to the presence of the third-country national on the territory of Member States.

Where necessary, fulfilment of the conditions referred to in points (a) and (b) of the first subparagraph of this paragraph shall be verified by accessing the logs in the EES provided for under Article 46 of Regulation (EU) 2017/2226 which correspond to the search referred to in point (a) of the first subparagraph of this paragraph and to the answer referred to in point (b) of that subparagraph.

3. 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 issued under Article 44, the Member States for which that travel 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.

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 point (k) of Article 17(2).

CHAPTER X

PROCEDURE AND CONDITIONS FOR ACCESS TO THE ETIAS CENTRAL SYSTEM FOR LAW ENFORCEMENT PURPOSES

Article 50

Member States' designated authorities

1. Member States shall designate the 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. Each Member State shall designate a central access point which shall have access to the ETIAS Central System. The central access point shall verify that the conditions to request access to the ETIAS Central System laid down in Article 52 are fulfilled.

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

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

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

3. At national level, each Member State shall keep a list of the 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 points.

4. Only duly empowered staff of the central access points shall be authorised to access the ETIAS Central System in accordance with Articles 51 and 52.

Article 51

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

1. An operating unit referred to in Article 50(3) shall submit a reasoned electronic or written request for consultation of a specific set of data stored in the ETIAS Central System to a central access point referred to in Article 50(2). Where consultation of data referred to in point (i) of Article 17(2) and points (a) to (c) of Article 17(4) is sought, the reasoned electronic or written request shall include a justification of the necessity to consult those specific data.

2. Upon receipt of the request for access, the central access point shall verify whether the conditions for access referred to in Article 52 are fulfilled, including by checking whether any request for consultation of data referred to in point (i) of Article 17(2) and points (a) to (c) of Article 17(4) is justified.

3. If the conditions for access referred to in Article 52 are fulfilled, the central access point shall process the request. The data stored in the ETIAS Central System accessed by the central access point shall be transmitted to the operating unit that made the request in such a way that the security of the data is not compromised.

4. In a case of urgency, where there is a need to prevent an imminent danger to the life of a person associated with a terrorist offence or other serious criminal offence, the central access point shall process the request immediately and shall only verify *ex post* whether all the conditions referred to in Article 52 are fulfilled, including whether a case of urgency actually existed. The *ex post* verification shall take place without undue delay and in any event no later than seven working days after the processing of the request.

Where an *ex post* verification reveals that the consultation of or access to data recorded in the ETIAS Central System was not justified, all the authorities that accessed the data shall erase the data they accessed from the ETIAS Central System. The authorities shall inform the relevant central access point of the Member State in which the request was made of the erasure.

Article 52

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

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

(c) evidence or reasonable grounds exist to consider that the consultation of data stored in the ETIAS Central System will contribute to the prevention, detection or investigation of any of the criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category of traveller covered by this Regulation.

2. Consultation of the ETIAS Central System shall be limited to searching with one or several of the following items of 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) email address;

(f) phone numbers;

(g) 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 points (a) to (g) and (j) to (m) of Article 17(2) which are recorded in that application file as well as to data entered in that application file in respect of the issue, refusal, annulment or revocation of a travel authorisation in accordance with Articles 39 and 43. Access to the data referred to in point (i) of Article 17(2) and points (a) to (c) of Article 17(4) recorded in the application file shall only be given if consultation of that data was explicitly requested by an operating unit in a reasoned electronic or written request submitted under Article 51(1) and that request has been independently verified and approved by the central access point. Consultation of the ETIAS Central System shall not give access to the data concerning education referred to in point (h) of Article 17(2).

Article 53

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 to consult data stored in the ETIAS Central System and submit a reasoned electronic request to consult a specific set of data stored in the ETIAS Central System to the ETIAS Central Unit. Where consultation of data referred to in point (i) of Article 17(2) and points (a) to (c) of Article 17(4) 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 all the following conditions are met:

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

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

(c) the consultation shall be limited to searching with data referred to in Article 52(2) in combination with the data listed under Article 52(3) where necessary;

(d) evidence or reasonable grounds exist to consider that the consultation will contribute to the prevention, detection or investigation of any of the criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category of traveller covered by this Regulation.

3. Europol requests for consultation of data stored in the ETIAS Central System shall be subject to prior verification by a specialised unit of duly empowered Europol officials, which shall examine in an efficient and timely manner whether the request fulfils all the conditions in 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 points (a) to (g) and (j) to (m) of Article 17(2) as well as to the data added to the application file relating to the issue, refusal, annulment or revocation of a travel authorisation in accordance with Articles 39 and 43. Access to the data referred to in point (i) of Article 17(2) and points (a) to (c) of Article 17(4) added to the application file shall only be given if consultation of those data was explicitly requested by Europol. Consultation of the ETIAS Central System shall not give access to the data concerning education referred to in point (h) of Article 17(2).

5. Once the specialised unit of duly empowered Europol officials has approved the request, the ETIAS Central Unit shall process the request for consultation of data stored in the ETIAS Central System. It shall transmit the requested data to Europol in such a way as not to compromise the security of the data.

CHAPTER XI

RETENTION AND AMENDMENT OF DATA

Article 54

Data retention

1. Each application file shall be stored in the ETIAS Central System for:

(a) the period of validity of the travel authorisation;

(b) five years from the last decision to refuse, annul or revoke the travel authorisation in accordance with Articles 37, 40 and 41. If the data present in a record, file or alert registered in one of the EU information systems, Europol data, the Interpol SLTD or TDAWN databases, the ETIAS watchlist, or the ETIAS screening rules giving rise to such a decision are deleted before the end of that five-year period, the application file shall be deleted within seven days from the date of the deletion of the data in that record, file or alert. For that purpose, the ETIAS Central System shall regularly and automatically verify whether the conditions for the retention of application files referred to in this point are still fulfilled. Where they are no longer fulfilled, it shall delete the application file in an automated manner.

2. For the purpose of facilitating a new application after the expiry of the validity period of an ETIAS travel authorisation, the application file may be stored in the ETIAS Central System for an additional period of no more than three years from the end of the validity period of the travel authorisation and only where, following a request for consent, the applicant freely and explicitly consents by means of an electronically signed declaration. Requests for consent shall be presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form and using clear and plain language, in accordance with Article 7 of Regulation (EU) 2016/679.

Consent shall be requested following the automatic provision of information under Article 15(2). The automatically provided information shall remind the applicant of the purpose of the data retention in line with the information referred to in point (o) of Article 71 and of the possibility to withdraw consent at any time.

The applicant may withdraw his or her consent at any time, in accordance with Article 7(3) of Regulation (EU) 2016/679. If the applicant withdraws consent, the application file shall automatically be erased from the ETIAS Central System.

eu-LISA shall develop a tool to enable applicants to give and withdraw their consent. That tool shall be made accessible via the dedicated public website or via the app for mobile devices.

The Commission shall adopt delegated acts in accordance with Article 89 to further define the tool to be used by the applicants to give and withdraw their consent.

3. Upon expiry of its retention period the application file shall automatically be erased from the ETIAS Central System.

Article 55

Amendment of data and advance data erasure

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 accurate. The ETIAS Central Unit and the ETIAS National Units shall not have the right to modify data added to the application form directly by the applicant pursuant to Article 17(2), (3) or (4).

2. Where the ETIAS Central Unit has evidence that data recorded in the ETIAS Central System by the ETIAS Central Unit 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 Member State responsible 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 the ETIAS Central Unit 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 National Unit of the Member State responsible within 14 days. If a Member State different from the Member State responsible has such evidence, it shall contact the ETIAS Central Unit or the ETIAS National Unit of the Member State responsible, also within 14 days. The ETIAS Central Unit or the ETIAS National Unit of the Member State responsible shall check the accuracy of the data and the lawfulness of its processing within 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 points (a) to (c) of Article 2(2), the authorities of that Member State shall verify whether that person has a valid travel authorisation and, where relevant, shall erase the application file without delay from the ETIAS Central System. The authority responsible for erasing the application file shall be:

(a) the ETIAS National Unit of the Member State that issued the travel document as referred to in point (a) of Article 2(2);

(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 card or residence permit.

6. Where a third-country national has fallen under the scope of point (d), (e), (f) or (l) of Article 2(2), he or she may inform the competent authorities of the Member State that issued that residence permit, uniform visa or national long-stay visa referred to in that Article that he or she has a valid travel authorisation and may request the deletion of the corresponding application file from the ETIAS Central System. The authorities of that Member State shall verify whether that person holds a valid travel authorisation. If it is confirmed that the person does hold such an authorisation, the ETIAS National Unit of the Member State that issued the residence permit, uniform visa or national long-stay visa shall delete the application file without delay from the ETIAS Central System.

7. Where a third-country national has fallen under the scope of point (g) of Article 2(2), he or she 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 from the ETIAS Central System without delay.

8. Without prejudice to any available administrative or non-judicial remedy, individuals shall have access to an effective judicial remedy to ensure that data stored in ETIAS are amended or erased.

CHAPTER XII

DATA PROTECTION

Article 56

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 (EU) 2016/679 shall apply to the processing of personal data by the ETIAS National Units assessing applications, by border authorities and by immigration authorities.

Where the processing of personal data by the ETIAS National Units is performed by competent authorities assessing the applications for the purposes of the prevention, detection or investigation of terrorist offences or other serious criminal offences, Directive (EU) 2016/680 shall apply.

Where the ETIAS National Unit decides on the issue, refusal, revocation or annulment of a travel authorisation, Regulation (EU) 2016/679 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) of this Regulation.

4. Regulation (EU) 2016/794 shall apply to the processing of personal data by Europol pursuant to Articles 29 and 53 of this Regulation.

Article 57

Data controller

1. The European Border and Coast Guard Agency is to be considered a data controller in accordance with point (d) of Article 2 of Regulation (EC) No 45/2001 in relation to the processing of personal data in the ETIAS Central System. In relation to information security management of the ETIAS Central System, eu-LISA is to be considered a controller.

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 point 7 of Article 4 of Regulation (EU) 2016/679. It shall have central responsibility for the processing of personal data in the ETIAS Central System by that Member State.

Article 58

Data processor

1. eu-LISA is to be considered a processor in accordance with point (e) of Article 2 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 59

Security of processing

1. eu-LISA, the ETIAS Central Unit and the ETIAS National Units shall ensure the security of processing of personal data pursuant to 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 ETIAS Information System.

3. Without prejudice to Article 22 of Regulation (EC) No 45/2001 and Articles 32 and 34 of Regulation (EU) 2016/679, 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 web service, the email service, the secure account service, the carrier gateway, the verification tool for applicants and the consent tool for applicants;

(c) deny unauthorised persons access to data processing equipment and national installations in accordance with the purposes of ETIAS;

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

(e) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of recorded personal data;

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

(g) 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;

(h) 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 and unique user identities and confidential access modes only;

(i) 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;

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

(k) 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;

(l) 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;

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

(n) ensure reliability by making sure that any faults in the functioning of ETIAS are properly reported and that necessary technical measures are put in place to ensure that personal data can be restored in the event of corruption due to a malfunctioning of ETIAS;

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

4. The Commission shall, by means of implementing acts, adopt a model security plan and a model business continuity and disaster recovery plan. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 90(2). eu-LISA's Management Board, the European Border and Coast Guard Agency's Management Board and the Member States shall adopt the security, business continuity and disaster recovery plans for eu-LISA, for the ETIAS Central Unit and for the ETIAS National Units respectively. They shall use the model plans adopted by the Commission as a basis, adjusted as necessary.

5. eu-LISA shall inform the European Parliament, the Council and the Commission and the European Data Protection Supervisor of the measures it takes pursuant to this Article.

Article 60

Security incidents

1. Any event that has or may have an impact on the security of ETIAS and may cause damage or loss to the data stored in ETIAS shall be considered to be a security incident, in particular where unauthorised access to data may have occurred or where the availability, integrity and confidentiality of data has or may have been compromised.

2. Security incidents shall be managed so as to ensure a quick, effective and proper response.

3. Without prejudice to the notification and communication of a personal data breach pursuant to Article 33 of Regulation (EU) 2016/679, Article 30 of Directive (EU) 2016/680, or both, Member States shall notify the Commission, eu-LISA and the European Data Protection Supervisor of security incidents. In the event of a security incident in relation to the ETIAS Information System, eu-LISA shall notify the Commission and the European Data Protection Supervisor. Europol shall notify the Commission and the European Data Protection Supervisor in the case of an ETIAS-related security incident.

4. Information regarding a security incident that has or may have an impact on the operation of ETIAS or on the availability, integrity and confidentiality of the data stored in ETIAS shall be provided to the Commission and, if affected, to the ETIAS Central Unit, to the ETIAS National Units and to Europol. Such incidents shall also be reported in compliance with the incident management plan to be provided by eu-LISA.

5. Member States, the European Border and Coast Guard Agency, eu-LISA and Europol shall cooperate in the event of a security incident.

Article 61

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 62

Penalties

Member States shall lay down the rules on penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.

Article 63

Liability

1. Without prejudice to the right to compensation from, and liability of the controller or processor under Regulation (EU) 2016/679, Directive (EU) 2016/680 and Regulation (EC) No 45/2001:

(a) any person or Member State that has suffered material or non-material damage as a result of an unlawful personal data processing operation or any other act incompatible with this Regulation by a Member State shall be entitled to receive compensation from that Member State;

(b) any person or Member State that has suffered material or non-material damage as a result of any act by eu-LISA incompatible with this Regulation shall be entitled to receive compensation from that agency. eu-LISA shall be liable for unlawful personal data processing operations in accordance with its role as processor or, where applicable, controller.

A Member State or eu-LISA shall be exempted from their liability under the first subparagraph, in whole or in part, if they prove that they are not responsible for the event which gave rise to the damage.

2. If any failure of a Member State to comply with its obligations under this Regulation causes damage to the ETIAS Central System, that Member State shall be held liable for such damage, unless and insofar as eu-LISA or another Member State participating in the ETIAS Central System failed to take reasonable measures to prevent the damage from occurring or to minimise its impact.

3. Claims for compensation against a Member State for the damage referred to in paragraphs 1 and 2 shall be governed by the national law of that Member State. Claims for compensation against the controller or eu-LISA for the damage referred to in paragraphs 1 and 2 shall be subject to the conditions provided for in the Treaties.

Article 64

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

1. Without prejudice to the right of information in Articles 11 and 12 of Regulation (EC) No 45/2001, applicants whose data are stored in the ETIAS Central System shall be informed, at the time their data are collected, of the procedures for exercising the rights under Articles 13 to 16 of Regulation (EC) No 45/2001 and Articles 15 to 18 of Regulation (EU) 2016/679. They shall also be provided with the contact details of the data protection officer of the European Border and Coast Guard Agency and of the European Data Protection Supervisor at the same time.

2. In order to exercise their rights under Articles 13 to 16 of Regulation (EC) No 45/2001 and Articles 15 to 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 his or her application. The unit that receives the request shall examine and reply to it as soon as possible, and at the latest within 30 days.

Where in response to a request, 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 Member State responsible shall rectify or erase those data in the ETIAS Central System without delay.

Where in response to a request pursuant to this paragraph, 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 20 to determine whether the amended application file triggers a hit pursuant to Article 20(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 period of the original and notify the applicant. Where the automated processing reports one or several hits, the ETIAS National Unit of the Member State responsible shall assess the security, illegal immigration or high epidemic risk in accordance with Article 26. It shall then 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 with the claim 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 shall adopt without delay an administrative decision explaining in writing to the person concerned why it is not prepared to correct or delete data relating to him or her.

4. That 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 available to the person, 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 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. It shall make that document available to the competent national data protection supervisory authorities without delay, and not later than seven days following the decision to rectify or erase data referred to in the second subparagraph of paragraph 2 or following the decision referred to in paragraph 3 respectively.

Article 65

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 to any private party with the exception of transfers to Interpol for the purpose of carrying out the automated processing referred to in points (b) and (l) of Article 20(2) of this Regulation. Transfers of personal data to Interpol are subject to the provisions of Article 9 of Regulation (EC) No 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 party. The prohibition shall also apply if those data are further processed at national level or between Member States.

3. By way of derogation from Article 49 of this Regulation, if necessary for the purpose of return, the immigration authorities may access the ETIAS Central System to retrieve data to be transferred to a third country in individual cases only where all of the following conditions are met:

(a) a prior search has been conducted in the EES in accordance with Article 26 of Regulation (EU) 2017/2226; and

(b) this search indicates that the EES does not contain data concerning the third-country national to be returned.

Where necessary, fulfilment of these conditions shall be verified by accessing the logs provided for in Article 46 of Regulation (EU) 2017/2226 corresponding to the search referred to in point (a) of the first subparagraph of this paragraph and to the answer corresponding to point (b) of that subparagraph.

If those conditions are met, the immigration authorities shall have access to query the ETIAS Central System with some or all of the data referred to in points (a) to (e) of Article 17(2) of this Regulation. If an ETIAS application file corresponds to those data, the immigration authorities will have access to the data referred to in points (a) to (g) of Article 17(2) of this Regulation and, in case of minors, point (k) of paragraph 2 of that Article.

By way of derogation from paragraph 1 of this Article, the data accessed from the ETIAS Central System by the immigration authorities may be transferred to a third country in individual cases if necessary in order to prove the identity of third-country nationals for the sole purpose of return, and only where one of the following conditions is satisfied:

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

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

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

The data referred to in points (a), (b), (d), (e) and (f) of Article 17(2) of this Regulation may be transferred only where all of the following conditions are satisfied:

(a) the transfer of the data is carried out in accordance with the relevant provisions of Union law, in particular provisions on data protection, including Chapter V of Regulation (EU) 2016/679, readmission agreements, and the national law of the Member State transferring the data;

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

(c) a return decision adopted pursuant to Directive 2008/115/EC of the European Parliament and of the Council [1] has been issued in relation to the third-country national concerned, provided that the enforcement of such a return decision is not suspended and provided that no appeal has been lodged which may lead to the suspension of its enforcement.

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

5. By way of derogation from paragraph 2 of this Article, the data from the ETIAS Central System referred to in Article 52(4) 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 in individual cases, but only where all of the following conditions are met:

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

(i) an imminent danger associated with a terrorist offence; or

[1] Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals (OJ L 348, 24.12.2008, p. 98).

(ii) an imminent danger to the life of a person and that danger is associated with a serious criminal offence;

(b) the transfer of data is necessary for the prevention, detection or investigation in the territory of the Member States or in the third country concerned of such a terrorist offence or serious criminal offence;

(c) the designated authority has access to such data in accordance with the procedure and the conditions set out in Articles 51 and 52;

(d) the transfer is carried out in accordance with the applicable conditions set out in Directive (EU) 2016/680, in particular Chapter V thereof;

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

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

Where a transfer is made pursuant to the first subparagraph of this paragraph, such a transfer shall be documented and the documentation shall, on request, be made available to the supervisory authority established in accordance with Article 41(1) of Directive (EU) 2016/680, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.

Article 66

Supervision by the supervisory authority

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

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

3. The supervisory authority established in accordance with Article 41(1) of Directive (EU) 2016/680 shall monitor the lawfulness of the access to personal data by Member States in accordance with Chapter X of this Regulation, including the transmission of data to and from ETIAS. Article 66(5) and (6) of this Regulation shall apply accordingly.

4. The supervisory authority or authorities established in accordance with Article 51(1) of Regulation (EU) 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 three years from the start of operations of ETIAS. The results of the audit may be taken into account in the evaluations conducted under the mechanism established by Council Regulation (EU) No 1053/2013 [1]. The supervisory authority established in accordance with Article 51(1) of Regulation (EU) 2016/679 shall publish annually the number of requests for rectification, completion or erasure, or restriction of processing of data, the action subsequently taken and the number of rectifications, completions, erasures and restrictions of processing made in response to requests by the persons concerned.

5. Member States shall ensure that their supervisory authority established in accordance with Article 51(1) of Regulation (EU) 2016/679 has sufficient resources and expertise to fulfil the tasks entrusted to it under this Regulation.

6. Member States shall supply any information requested by the supervisory authority established in accordance with Article 51(1) of Regulation (EU) 2016/679. They shall, in particular, provide it with information on the activities carried out in accordance with their responsibilities as laid down in this Regulation. Member States shall grant the supervisory authority established in accordance with Article 51(1) of Regulation (EU) 2016/679 access to their logs and allow it access at all times to all their premises used for the purposes of ETIAS.

[1] Council Regulation (EU) No 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen *acquis* and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen (OJ L 295, 6.11.2013, p. 27).

Article 67

Supervision by the European Data Protection Supervisor

1. The European Data Protection Supervisor shall be responsible for monitoring the personal data processing activities of eu-LISA, Europol and the European Border and Coast Guard Agency related to ETIAS and for ensuring that such activities are carried out in accordance with Regulation (EC) No 45/2001 and with this Regulation.

2. The European Data Protection Supervisor shall ensure that an audit of eu-LISA's and the ETIAS Central Unit's personal data processing activities is carried out in accordance with relevant international auditing standards at least every three years. A report of that audit shall be sent to the European Parliament, to the Council, to the Commission, to eu-LISA and to the supervisory authorities. eu-LISA and the European Border and Coast Guard Agency shall be given an opportunity to make comments before the report is adopted.

3. eu-LISA and the ETIAS Central Unit shall supply information requested by the European Data Protection Supervisor, give him or her access to all documents and to their logs, and allow him or her access to all their premises at any time.

Article 68

Cooperation between supervisory authorities and the European Data Protection Supervisor

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

2. The supervisory authorities and the European Data Protection Supervisor shall exchange relevant information, assist each other in carrying out audits and inspections, examine any difficulties concerning the interpretation or application of this Regulation, assess problems in the exercise of independent supervision or in the exercise of the rights of the data subject, draw up harmonised proposals for joint solutions to any problems and promote awareness of data protection rights, as necessary.

3. For the purpose of paragraph 2, the supervisory authorities and the European Data Protection Supervisor shall meet at least twice a year within the framework of the European Data Protection Board established by Regulation (EU) 2016/679. The costs of those meetings shall be borne and their organisation shall be undertaken by that Board. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary.

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

Article 69

Keeping of logs

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

(a) the purpose of the access;

(b) the date and time of each operation;

(c) the data used for the automated processing of the applications;

(d) the hits triggered while carrying out the automated processing laid down in Article 20;

(e) the data used for the verification of identity stored in the ETIAS Central System or other information systems and databases;

(f) the results of the verification process referred to in Article 22; and

(g) the staff member having performed it.

2. The ETIAS Central Unit shall keep records of the staff members duly authorised to perform the identity verifications.

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

3. eu-LISA shall keep logs of all data processing operations within the ETIAS Information System involving the access by border authorities referred to in Article 47 and the access by immigration authorities referred to in Article 49. Those logs 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 border authorities and immigration authorities entering and retrieving the data.

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

4. Such logs may be used only for monitoring the admissibility of data processing and to ensure data security and integrity. The logs shall be protected by appropriate measures against unauthorised access. They shall be deleted one year after the retention period referred to in Article 54 has expired, if they are not required for monitoring procedures which have already begun.

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

Article 70

Keeping of logs for requests for data consultation in order to prevent, detect and investigate terrorist offences or other serious criminal offences

1. eu-LISA shall keep logs of all data processing operations within the ETIAS Central System involving access by the central access points referred to in Article 50(2) for the purposes of Article 1(2). Those logs 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 logs of all data processing operations within the ETIAS Central System resulting from requests for consultation of data or from access to data stored in the ETIAS Central System for the purposes laid down in Article 1(2).

3. The logs referred to in paragraph 2 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 central access point to the ETIAS Central System;

(e) where applicable, the use of the urgency procedure referred to in Article 51(4) and the outcome of the *ex post* verification;

(f) which of the data or set of data referred to in Article 52(2) and (3) have been used for consultation; and

(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 transmission of data.

4. The logs referred to in paragraphs 1 and 2 of this Article shall be used only to check the admissibility of the request, monitor the lawfulness of data processing and to ensure data integrity and security. The logs shall be protected by appropriate measures against unauthorised access. They shall be deleted one year after the retention period referred to in Article 54 has expired, if they are not required for monitoring procedures which have already begun. 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 the logs 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 the logs for that purpose. Other than for such purposes, personal data shall be erased in all national and Europol files after a period of one month, unless those data are required for the purposes of the specific ongoing criminal investigation for which they were requested by a Member State or by Europol. Only logs containing non-personal data may be used for the monitoring and evaluation referred to in Article 92.

CHAPTER XIII

PUBLIC AWARENESS

Article 71

Information to the general public

After consulting the Commission and the European Data Protection Supervisor, the ETIAS Central Unit shall provide the general public with all relevant information in relation to applying for a travel authorisation. Such information shall be available on the public website and shall include:

(a) the criteria, conditions and procedures for applying for a travel authorisation;

(b) information concerning the website and the app for mobile devices where the application can be submitted;

(c) information on the possibility that an application may be submitted by another person or a commercial intermediary;

(d) information on the possibility to report abuses from commercial intermediaries using the form referred to in Article 15(5);

(e) the deadlines for deciding on an application provided for in Article 32;

(f) the fact that a travel authorisation is linked to the travel document indicated in the application form and that consequently the expiry and any modification of the travel document will result in the invalidity or non-recognition of the travel authorisation when crossing the border;

(g) the fact that applicants are responsible for the authenticity, completeness, correctness and reliability of the data they submit and for the veracity and reliability of the statements they make;

(h) the fact that decisions on applications must be notified to the applicant, that where a travel authorisation is refused, such decisions must state the grounds for the refusal 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 details of the competent authority, as well as the time limit for lodging an appeal;

(i) the fact that applicants have the possibility to contact the ETIAS Central Unit indicating that the purpose of their travel is based on humanitarian grounds or is linked to international obligations and the conditions and procedures for doing so;

(j) the entry conditions laid down in Article 6 of Regulation (EU) 2016/399 and the fact that a short stay is only possible for a duration of no more than 90 days in any 180-day period, except for third-country nationals benefiting from more favourable provisions of a bilateral agreement preexisting the Convention Implementing the Schengen Agreement;

(k) the fact that the mere possession of a travel authorisation does not confer an automatic right of entry;

(l) the fact that the border authorities may request supporting documents at external borders in order to verify the fulfilment of the conditions of entry;

(m) the fact that the possession of a valid travel authorisation is a condition for stay that has to be fulfilled during the entire duration of a short stay on the territory of Member States;

(n) a link to the web service referred to in Article 13 of Regulation (EU) 2017/2226 enabling third-country nationals to verify at any moment their remaining authorised stay;

(o) the fact that the data entered into the ETIAS Information System are used for the purposes of border management, including for checks in databases, and that the data may be accessed by the Member States and Europol for the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences, under the procedures and conditions referred to in Chapter X;

(p) the period for which data will be stored;

(q) the rights of data subjects under Regulations (EC) No 45/2001, (EU) 2016/679 and (EU) 2016/794 and Directive (EU) 2016/680;

(r) the possibility for travellers to obtain support as provided for in point (m) of Article 7(2).

Article 72

Information campaign

The Commission shall, in cooperation with the European External Action Service, the ETIAS Central Unit, and the Member States, including their consulates in the third countries concerned, accompany the start of operations by ETIAS with an information campaign to inform third-country nationals falling within the scope of this Regulation of the requirement for them to be in possession of a valid travel authorisation both to cross the external borders and for the entire duration of their short stay on the territory of Member States.

That information campaign shall be conducted regularly and in at least one of the official languages of the countries whose nationals fall within the scope of this Regulation.

CHAPTER XIV

RESPONSIBILITIES

Article 73

Responsibilities of eu-LISA during the designing and development phase

1. The ETIAS Central System shall be hosted by eu-LISA in its technical sites and shall provide the functionalities laid down in this Regulation in accordance with the conditions of security, availability, quality and speed pursuant to paragraph 3 of this Article and to Article 74(1).

2. The infrastructures supporting the public website, the app for mobile devices, the email service, the secure account service, the verification tool for applicants, the consent tool for applicants, the assessment tool for the ETIAS watchlist, the carrier gateway, the web service, the software to process the applications, the central repository of data and the technical solutions referred to in Article 92(8) 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, data protection and data security, availability, quality and speed pursuant to paragraph 3 of this Article and to Article 74(1). The ETIAS watchlist shall be hosted in an eu-LISA site.

3. eu-LISA shall be responsible for the technical development of the ETIAS Information System, for any technical development required for establishing interoperability between the ETIAS Central System and the EU information systems referred to in Article 11 and for enabling querying of Interpol databases referred to in Article 12.

eu-LISA shall define the design of the physical architecture of the system including its communication infrastructure as well as its technical specifications and their evolution and the NUIs. Those technical specifications shall be adopted by eu-LISA's Management Board, subject to a favourable opinion from the Commission. eu-LISA shall also implement any necessary adaptations to the EES, SIS, Eurodac or VIS deriving from the establishment of interoperability with ETIAS.

eu-LISA shall develop and implement the ETIAS Central System, including the ETIAS watchlist, the NUIs, and the communication infrastructure as soon as possible after the entry into force of this Regulation and the adoption by the Commission of:

(a) the measures provided for in Articles 6(4), 16(10), 17(9), Article 31, Articles 35(7), 45(2), 54(2), 74(5), 84(2), 92(8); and

(b) measures adopted in accordance with the examination procedure referred to in Article 90(2) necessary for the development and technical implementation of the ETIAS Central System, the NUIs, the communication infrastructure and the carrier gateway, in particular implementing acts for:

(i) accessing the data in accordance with Articles 22 to 29 and Articles 33 to 53;

(ii) amending, erasing and advance erasure of data in accordance with Article 55;

(iii) keeping and accessing the logs in accordance with Article 45 and Article 69;

(iv) performance requirements;

(v) specifications for technical solutions to connect central access points in accordance with Articles 51 to 53.

The development shall consist of the elaboration and implementation of the technical specifications, testing and overall project coordination. In this regard, the tasks of eu-LISA shall also be to:

(a) perform a security risk assessment;

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

(c) conduct a security risk assessment regarding the interoperability of ETIAS with the EU information systems and Europol data referred to in Article 11.

4. During the design 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 EES-ETIAS Advisory Group referred to in Article 91, 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 ETIAS. The Programme Management Board shall meet regularly and at least three times per quarter. It shall ensure the adequate management of the design and development phase of ETIAS. The Programme Management Board shall submit written reports every month to eu-LISA's Management Board on progress of the project. It shall have no decision-making power nor any mandate to represent the members of eu-LISA's Management Board.

5. eu-LISA's 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 to ensure that non-participating members of eu-LISA's Management Board are fully informed.

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

All travel and subsistence expenses incurred by the members of the Programme Management Board shall be paid by eu-LISA. 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 shall meet regularly until the start of operations by 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 74

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

1. Following the entry into operations of ETIAS, eu-LISA shall be responsible for the technical management of the ETIAS Central System and the NUIs. It shall also be responsible for any technical testing required for the establishment and update of the ETIAS screening rules. It shall ensure, in cooperation with the Member States that, at all times, the best available technology is used, subject to a cost-benefit analysis. eu-LISA shall also be responsible for the technical management of the communication infrastructure between the ETIAS Central System and the NUIs as well as for the public website, the app for mobile devices, the email service, the secure account service, the verification tool for applicants, the consent tool for applicants, the assessment tool for the ETIAS watchlist, the carrier gateway, the web service, the software to process the applications and the central repository of data referred to in Article 6.

Technical management of 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 consultation of the ETIAS Central System in accordance with the technical specifications.

2. Without prejudice to Article 17 of the Staff Regulations of Officials of the European Union, laid down in Council Regulation (EEC, Euratom, ECSC) No 259/68 [1], 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. That obligation shall also apply after such staff leave office or employment or after the termination of their activities.

3. Where eu-LISA cooperates with external contractors in any ETIAS-related tasks, it shall closely monitor the activities of the contractors to ensure compliance with all provisions of this Regulation, including in particular security, confidentiality and data protection.

4. eu-LISA shall also perform tasks related to providing training on the technical use of the ETIAS Information System.

5. 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 European Parliament, the Council and the Commission covering the issues encountered. The Commission shall, by means of implementing acts, lay down and develop that mechanism, the procedures and the appropriate requirements for data quality compliance. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 90(2).

Article 75

Responsibilities of the European Border and Coast Guard Agency

1. The European Border and Coast Guard Agency shall be responsible for:

(a) the setting up and operation of the ETIAS Central Unit and ensuring the conditions for the secure management of data stored in ETIAS;

(b) the automated processing of applications; and

(c) the ETIAS 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 on data security and fundamental rights, in particular data protection. They shall also take part in training offered by eu-LISA on the technical use of the ETIAS Information System and on data quality.

Article 76

Responsibilities of Member States

1. Each Member State shall be responsible for:

(a) the connection to the NUI;

(b) the organisation, management, operation and maintenance of the ETIAS National Units for the manual processing of applications for travel authorisation where the automated processing has reported a hit, as referred to in Article 26;

(c) the organisation of central access points and their connection to the NUI for the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences;

(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;

(f) entering data into the ETIAS watchlist related to terrorist offences or other serious criminal offences pursuant to Article 34(2) and (3); and

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

(g) ensuring that each of its authorities entitled to access the ETIAS Information System takes the measures necessary to comply with this Regulation, including those necessary to ensure the respect of fundamental rights and data security.

2. Each Member State shall use automated processes for querying the ETIAS Central System at the external borders.

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 on data security and on fundamental rights, in particular data protection.

They shall also take part in trainings offered by eu-LISA on the technical use of the ETIAS Information System and on data quality.

Article 77

Responsibilities of Europol

1. Europol shall ensure processing of the queries referred to in point (j) of Article 20(2) and in Article 20(4). It shall adapt its information system accordingly.

2. Europol shall have the responsibilities and tasks regarding the ETIAS watchlist laid down in Article 35(1) and (3) to (6).

3. Europol shall be responsible for providing a reasoned opinion following a consultation request pursuant to Article 29.

4. Pursuant to Article 34(2), Europol shall be responsible for entering data related to terrorist offences or other serious criminal offences obtained by Europol into the ETIAS watchlist.

5. Before being authorised to undertake any of the tasks referred to in Articles 34 and 35, the staff of Europol shall be given appropriate training on data security and on fundamental rights, in particular data protection. They shall also take part in training offered by eu-LISA on the technical use of the ETIAS Information System and on data quality.

CHAPTER XV

AMENDMENTS TO OTHER UNION INSTRUMENTS

Article 78

Amendment to Regulation (EU) No 1077/2011

The following article is inserted in Regulation (EU) No 1077/2011:

'*Article 5b*

Tasks relating to ETIAS

In relation to ETIAS, the Agency shall perform the tasks conferred on it by Article 73 of Regulation (EU) 2018/1240 of the European Parliament and of the Council (*).

(*) Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018, p. 1).'.

Article 79

Amendment to Regulation (EU) No 515/2014

In Article 6 of Regulation (EU) No 515/2014, the following paragraph is inserted:

'3a. During the development phase of the European Travel Information and Authorisation System (ETIAS), Member States shall receive an additional allocation of EUR 96,5 million to their basic allocation and shall devote this funding entirely to ETIAS to ensure its quick and effective development consistent with the implementation of the ETIAS Central System, as established in Regulation (EU) 2018/1240 of the European Parliament and of the Council (*).

(*) Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018, p. 1).'.

Article 80

Amendments to Regulation (EU) 2016/399

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

(1) Article 6(1) is amended as follows:

(a) 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 (EU) 2018/1240 of the European Parliament and of the Council (**), except where they hold a valid residence permit or a valid long-stay visa;

(*) Council Regulation (EC) No 539/2001 of 15 March 2001 listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement (OJ L 81, 21.3.2001, p. 1).

(**) Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018, p. 1).';

(b) the following subparagraphs are added:

'For a transitional period established pursuant to Article 83(1) and (2) of Regulation (EU) 2018/1240, the use of the European Travel Information and Authorisation System (ETIAS) shall be optional and the requirement to be in possession of a valid travel authorisation set out in point (b) of the first subparagraph of this paragraph shall not apply. Member States 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 transitional period. For this purpose, Member States shall distribute a common leaflet to this category of travellers as referred to in Article 83(2) of Regulation (EU) 2018/1240.

During a grace period established pursuant to Article 83(3) of Regulation (EU) 2018/1240 the border authorities 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 this Article, provided that they are crossing the external borders of the Member States for the first time since the end of the transitional period referred to in Article 83(1) and (2) of Regulation (EU) 2018/1240. Border authorities shall inform such third-country nationals of the requirement to be in possession of a valid travel authorisation in accordance with this Article. For this purpose, the border authorities shall distribute to these travellers a common leaflet as referred to in Article 83(3) of Regulation (EU) 2018/1240 informing them that they are exceptionally allowed to cross the external borders while not fulfilling the obligation to be in possession of a valid travel authorisation and explaining that obligation.'.

(2) Article 8(3) is amended as follows:

(a) in point (a), point (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 is inserted:

'(ba) if the third-country national holds a travel authorisation referred to in point (b) of Article 6(1) of this Regulation 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 through consultation of ETIAS in accordance with Article 47 of Regulation (EU) 2018/1240. Where it is technically impossible to proceed with the consultation or to perform the search that are referred to in Article 47(1) and (2) of Regulation (EU) 2018/1240, Article 48(3) of that Regulation shall apply.'.

(3) In Annex V, Part B, in the standard form for refusal of entry at the border, point (C) in the list of reasons for refusal is replaced by the following:

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

Article 81

Amendments to Regulation (EU) 2016/1624

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

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

'(qa) fulfil the tasks and obligations entrusted to the European Border and Coast Guard Agency referred to in Regulation (EU) 2018/1240 of the European Parliament and of the Council (*) and ensure the setting up and operation of the ETIAS Central Unit in accordance with Article 7 of that Regulation.

(*) Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018, p. 1).'.

(2) In Chapter II, the following Section is added:

'Section 5

ETIAS

Article 33a

Establishment 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 of an ETIAS Central Unit pursuant to Article 7 of Regulation (EU) 2018/1240 of the European Parliament and of the Council (*).

(*) Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018, p. 1).'.

Article 82

Amendment to Regulation (EU) 2017/2226

In Article 64 of Regulation (EU) 2017/2226, the following paragraph is added:

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

CHAPTER XVI

FINAL PROVISIONS

Article 83

Transitional period and transitional measures

1. For a period of six months from the date on which ETIAS starts operations, the use 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 89 to extend that period for a maximum of a further six months, renewable once.

2. During the period referred to in paragraph 1, Member States 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 Member States shall distribute a common leaflet to this category of travellers. The leaflet shall also be made available at the Member States' consulates in the countries whose nationals fall within the scope of this Regulation.

3. A grace period of six months shall apply following the end of the period referred to in paragraph 1 of this Article. During the grace period, the requirement to be in possession of a valid travel authorisation shall apply. During the grace period the border authorities 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 are crossing 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 authorities shall inform such third-country nationals of the requirement to be in possession of a valid travel authorisation in accordance with point (b) of Article 6(1) of Regulation (EU) 2016/399. For that purpose, the border authorities shall distribute to those travellers a common leaflet informing them that they are exceptionally allowed to cross the external borders while not fulfilling the obligation to be in possession of a valid travel authorisation and explaining that obligation. The Commission may adopt a delegated act in accordance with Article 89 of this Regulation to extend that period for a maximum of a further six months.

During the period of grace, entries into the territories of the Member States not operating the EES shall not be taken into consideration.

4. The Commission shall, by means of implementing acts, draw up the two common leaflets referred to in paragraphs 2 and 3 of this Article, containing at a minimum the information referred to in Article 71. The leaflets shall be clear and simple and available in at least one of the official languages of each country whose nationals fall within the scope of this Regulation. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 90(2).

5. During the transitional period referred to in paragraphs 1 and 2 of this Article, the ETIAS Information System shall respond to the carriers' query referred to in Article 45(2) by providing the carriers with an 'OK' answer. During the period of grace referred to in paragraph 3 of this Article, the response sent by the ETIAS Information System to the carriers' query shall take into consideration whether the third-country national is crossing 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.

Article 84

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 and in accordance with the safeguards related to non-discrimination referred to in Article 14:

(a) application status information;

(b) nationalities, sex and year of birth of the applicant;

(c) the country of residence;

(d) education (primary, secondary, higher or none);

(e) current occupation (job group);

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

(g) the type of travel authorisation and, for a travel authorisation with limited territorial validity as referred to in Article 44, a reference to the Member State(s) issuing the travel authorisation with limited territorial validity;

(h) the validity period of the travel authorisation; and

(i) the grounds for refusing, revoking or annulling a travel authorisation.

2. For the purpose of paragraph 1, eu-LISA shall establish, implement and host a central repository in its technical sites containing the data referred to in paragraph 1 which does not allow for the identification of individuals but would allow the authorities referred to in paragraph 1 to obtain customisable reports and statistics to improve the assessment of security, illegal immigration and high epidemic risks, to enhance the efficiency of border checks, to help the ETIAS Central Unit and the ETIAS National Units process travel authorisation applications and to support evidence-based Union migration policy-making. 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 TESTA with control of access and specific user profiles solely for the purpose of reporting and statistics.

The Commission shall, by means of implementing acts, adopt detailed rules on the operation of the central repository and the data protection and security rules applicable to the repository. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 90(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 92(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 issued or refused, including the grounds for refusal, and of third-country nationals whose travel authorisation was annulled or revoked.

5. At the end of each year, statistical data shall be compiled in an annual report for that year. The report shall be published and transmitted to the European Parliament, to the Council, to the Commission, to the European Data Protection Supervisor, to the European Border and Coast Guard Agency and to the national supervisory authorities.

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

Article 85

Costs

1. The costs incurred in connection with the development of the ETIAS Information System, with the integration of the existing national border infrastructure and the connection to the NUI, with the hosting of the NUI and with the establishment of the ETIAS Central Unit and the ETIAS National Units shall be borne by the general budget of the Union.

eu-LISA shall pay particular attention to the risk of costs increases and ensure sufficient monitoring of contractors.

2. ETIAS' operating costs shall be borne by the general budget of the Union. This shall include the operation and maintenance costs of the ETIAS Information System, including of the NUIs; the operating costs of the ETIAS Central Unit and the costs of staff and technical equipment (hardware and software) necessary for the fulfilment of the tasks of the ETIAS National Units; and translation costs incurred pursuant to Article 27(2) and (8).

The following costs shall be excluded:

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

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

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

(d) design, development, implementation, operation and maintenance of national communication networks.

3. ETIAS' operating costs shall also include financial support to Member States for expenses incurred to customise and automate border checks in order to implement ETIAS. The total amount of this financial support shall be limited to a maximum of EUR 15 million for the first year of operation, to a maximum of EUR 25 million for the second year of operation and to a maximum of EUR 50 million per year for the subsequent years of operation. The Commission shall adopt delegated acts in accordance with Article 89 to further define that financial support.

4. The European Border and Coast Guard Agency, eu-LISA and Europol shall receive appropriate additional funding and the staff necessary for the fulfilment of the tasks entrusted to them under this Regulation.

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

Article 86

Revenues

The revenues generated by the ETIAS shall constitute internal assigned revenue in accordance with Article 21(4) of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council [1]. They shall be assigned to cover the costs of the operation and maintenance of ETIAS. Any revenue remaining after covering these costs shall be assigned to the Union budget.

Article 87

Notifications

1. Member States shall notify the Commission of the authority which is to be considered as controller referred to in Article 57.

2. The ETIAS Central Unit and the Member States shall notify the Commission and eu-LISA of the competent authorities referred to in Article 13 which have access to the ETIAS Information System.

Three months after ETIAS has started operations in accordance with Article 88, eu-LISA shall publish a consolidated list of those authorities in the *Official Journal of the European Union*. Member States shall also notify the Commission and eu-LISA of any changes of those authorities without delay. In the event of such changes, eu-LISA shall publish once a year an updated consolidated version of that information. eu-LISA shall maintain a continuously updated public website containing that information.

3. Member States shall notify the Commission and eu-LISA of their designated authorities and of their central access points referred to in Article 50 and shall notify any changes in that regard without delay.

4. eu-LISA shall notify the Commission of the successful completion of the test referred to in point (e) of Article 88(1).

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

Article 88

Start of operations

1. The Commission shall determine the date from which ETIAS is to start operations once the following conditions have been met:

(a) the necessary amendments to the legal acts establishing the EU information systems referred to in Article 11(2) with which interoperability shall be established with the ETIAS Information System have entered into force;

(b) the Regulation entrusting eu-LISA with the operational management of ETIAS has entered into force;

(c) the necessary amendments to the legal acts establishing the EU information systems referred to in Article 20(2) providing for an access to these databases for the ETIAS Central Unit have entered into force;

(d) the measures referred to in Article 15(5), Article 17(3), (5) and (6), Article 18(4), Article 27(3) and (5), Article 33(2) and (3), Articles 36(3), 38(3), 39(2), 45(3), 46(4), 48(4), 59(4), Article 73(3)(b), Article 83(1), (3), and (4) and Article 85(3) have been adopted;

(e) eu-LISA has declared the successful completion of a comprehensive test of ETIAS;

(f) eu-LISA and the ETIAS Central Unit have validated the technical and legal arrangements to collect and transmit the data referred to in Article 17 to the ETIAS Central System and have notified them to the Commission;

(g) the Member States and the ETIAS Central Unit have notified to the Commission the data concerning the various authorities referred to in Article 87(1) and (3).

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

2. The test of ETIAS referred to in point (e) 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 (e) 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 ETIAS from the date determined by the Commission in accordance with paragraph 1.

Article 89

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 6(4), Article 17(3), (5) and (6), Articles 18(4), 27(3), Article 31, Articles 33(2), 36(4), 39(2), 54(2), Article 83(1) and (3) and Article 85(3) shall be conferred on the Commission for a period of five years from 9 October 2018. 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 6(4), Article 17(3), (5) and (6), Articles 18(4), 27(3), Article 31, Articles 33(2), 36(4), 39(2), 54(2), Article 83(1) and (3) and Article 85(3) 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.

4. 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 of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Article 6(4), Article 17(3), (5) or (6), Article 18(4), 27(3), Article 31, Article 33(2), 36(4), 39(2), 54(2), Article 83(1) or (3) or Article 85(3) 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 to 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 90

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 91

Advisory group

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

Article 92

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 ETIAS in light of objectives relating to the technical output, cost-effectiveness, security and quality of service.

2. By 10 April 2019 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 to the Council on the state of play of the development of the ETIAS Central System, the NUIs and the communication infrastructure between the ETIAS Central System and the NUIs. That report shall contain detailed information about the costs incurred and information as to any risks which may impact the overall costs of the system to be borne by the general budget of the Union in accordance with Article 85.

By 10 April 2019 and every six months thereafter during the development phase of the ETIAS Information System, Europol and the European Border and Coast Guard Agency shall submit a report to the European Parliament and to the Council on the state of preparation for the implementation of this Regulation including detailed information about the costs incurred and information as to any risks which may impact the overall costs of the system to be borne by the general budget of the Union in accordance with Article 85.

Once the development is finalised, eu-LISA shall submit a report to the European Parliament and to the Council explaining in detail how the objectives, in particular relating to planning and costs, were achieved as well as justifying any divergences.

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

4. Two years after the start of operations of ETIAS and every two years thereafter, eu-LISA shall submit to the European Parliament, to the Council and to the Commission a report on the technical functioning of ETIAS Information System, including the security thereof, and statistical data concerning the ETIAS watchlist in accordance with the review procedure referred to in Article 35(5) and (6).

5. Three years after the start of operations of ETIAS and every four years thereafter, the Commission shall evaluate ETIAS and shall make any necessary recommendations to the European Parliament and to the Council. That evaluation shall include:

(a) the querying of Interpol SLTD and TDAWN databases through ETIAS, including information on the number of hits against those Interpol databases, the number of travel authorisations refused following such hits and information on any problems encountered, as well as, if appropriate, an assessment of the need for a legislative proposal amending this Regulation;

(b) the results achieved by ETIAS having regard to its objectives, mandate and tasks;

(c) the impact, effectiveness and efficiency of ETIAS' performance and its working practices in light of its objectives, mandate and tasks;

(d) an assessment of the security of ETIAS;

(e) the ETIAS screening rules used for the purpose of risk assessment;

(f) the impact of the ETIAS watchlist including the number of travel authorisation applications which were refused for reasons that took into account a positive hit against the ETIAS watchlist;

(g) the possible need to modify the mandate of the ETIAS Central Unit and the financial implications of any such modification;

(h) the impact on fundamental rights;

(i) the impact on diplomatic relations between the Union and the third countries involved;

(j) the revenue generated through the travel authorisation fee, the costs incurred in connection with the development of ETIAS, the costs for the operation of ETIAS, the costs incurred by eu-LISA, Europol and the European Border and Coast Guard Agency in relation to their tasks pursuant to this Regulation, as well as any revenue allocated in accordance with Article 86;

(k) the use of ETIAS for law enforcement purposes on the basis of the information referred to in paragraph 8 of this Article;

(l) the number of applicants being invited for an interview and the percentage it represents of the total number of applicants, the reasons for requesting an interview, the number of remote interviews, the number of decisions where the travel authorisation has been granted, has been granted with a flag or has been refused, and the number of applicants invited to an interview who did not attend it, and if appropriate, an assessment of the need for a legislative proposal amending this Regulation.

The Commission shall transmit the evaluation report to the European Parliament, the Council, the European Data Protection Supervisor and the European Agency for Fundamental Rights.

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

7. eu-LISA and the ETIAS Central Unit shall provide the Commission with the information necessary to produce the evaluations referred to in paragraph 5.

8. While respecting the provisions of national law on the publication of sensitive information, each Member State and Europol shall prepare annual reports on the effectiveness of access to data stored in the ETIAS Central System for law enforcement purposes containing information and statistics on:

(a) the exact purpose of the consultation including the type of terrorist offence or other serious criminal offence;

(b) reasonable grounds given for the substantiated suspicion that the suspect, perpetrator or victim is covered by this Regulation;

(c) the number of requests for access to the ETIAS Central System for law enforcement purposes;

(d) the number and type of cases which have resulted in hits;

(e) the number and type of cases in which the urgency procedure referred to in Article 51(4) was used, including those cases where that urgency was not accepted by the *ex post* verification carried out by the central access point.

A technical solution shall be made available to Member States in order to facilitate the collection of those data pursuant to Chapter X for the purpose of generating statistics referred to in this paragraph. The Commission shall, by means of implementing acts, adopt the specifications of the technical solution. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 90(2).

Article 93

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. The practical handbook shall take into account relevant existing handbooks. The Commission shall adopt the practical handbook in the form of a recommendation.

Article 94

Ceuta and Melilla

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

Article 95

Financial contribution of the countries associated with the implementation, application and development of the Schengen acquis

Under the relevant provisions of their association agreements, arrangements shall be made in relation to the financial contributions of the countries associated with the implementation, application and development of the Schengen *acquis*.

Article 96

Entry into force and applicability

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall apply from the date determined by the Commission in accordance with Article 88, with the exception of Articles 6, 11, 12, 33, 34, 35, 59, 71, 72, 73, Articles 75 to 79, Articles 82, 85, 87, 89, 90, 91, Article 92(1) and (2), Articles 93 and 95, as well as the provisions related to the measures referred to in point (d) of Article 88(1), which shall apply from 9 October 2018.

The provisions relating to the consultation of Eurodac shall apply from the date the recast of Regulation (EU) No 603/2013 of the European Parliament and of the Council [1] becomes applicable.

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

Done at Strasbourg, 12 September 2018.

For the European Parliament	*For the Council*
The President	*The President*
A. TAJANI	K. EDTSTADLER

[1] Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 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 and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 180, 29.6.2013, p. 1).

ANNEX

List of criminal offences referred to in point (a) of Article 17(4)

1. terrorist offences,
2. participation in a criminal organisation,
3. trafficking in human beings,
4. sexual exploitation of children and child pornography,
5. illicit trafficking in narcotic drugs and psychotropic substances,
6. illicit trafficking in weapons, munitions and explosives,
7. corruption,
8. fraud, including that against the financial interests of the Union,
9. laundering of the proceeds of crime and counterfeiting of currency, including the euro,
10. computer-related crime/cybercrime,
11. environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties,
12. facilitation of unauthorised entry and residence,
13. murder, grievous bodily injury,
14. illicit trade in human organs and tissue,
15. kidnapping, illegal restraint and hostage-taking,
16. organised and armed robbery,
17. illicit trafficking in cultural goods, including antiques and works of art,
18. counterfeiting and piracy of products,
19. forgery of administrative documents and trafficking therein,
20. illicit trafficking in hormonal substances and other growth promoters,
21. illicit trafficking in nuclear or radioactive materials,
22. rape,
23. crimes within the jurisdiction of the International Criminal Court,
24. unlawful seizure of aircraft or ships,
25. sabotage,
26. trafficking in stolen vehicles,
27. industrial espionage,
28. arson,
29. racism and xenophobia.