EUROPEAN
COMMISSION

Brussels, 16.11.2016
COM(2016) 731 final

2016/0357 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

Background

Our overarching priority is to ensure the security of citizens in an open Europe. The pressures of the migration and refugee crises, alongside a series of terrorist attacks, have severely tested the EU migration and security frameworks. EU citizens expect the external borders of the Schengen area to be managed effectively to prevent irregular migration and ensure enhanced internal security.[1] The effectiveness of external border management is an essential precondition for free movement within the Schengen Area and for facilitating the crossing of EU external borders in a world of mobility. Every year, there are some 400 million crossings of the Schengen border by EU citizens, and 200 million by non-EU citizens.

Today, around 1,4 billion people from around 60 countries worldwide can benefit from visa-free travel to the European Union. This makes the EU the most welcoming destination in the industrialised world, and based on the principle of reciprocity, benefits also EU citizens by facilitating visa-free travel abroad. The number of visa-exempt third country nationals to the Schengen countries will continue to grow, with an expected increase of over 30% in the number of visa exempt third country nationals crossing the Schengen borders by 2020, from 30 million in 2014 to 39 million in 2020.[2] These figures demonstrate the need to put in place a system that is able to achieve objectives similar to the visa regime, namely to assess and manage the potential irregular migration and security risks represented by third country nationals visiting the EU, yet in a lighter and more visitor-friendly way, in line with the objectives of the EU's visa liberalisation policy.

The Commission confirmed in its Communication of 14 September 2016 'Enhancing security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders'[3] the need to strike the right balance between ensuring mobility and enhancing security, while facilitating legal entry into the Schengen area without the need for a visa. Visa liberalisation has proved an important tool in building partnerships with third countries, including as a means of ensuring effective systems of return and readmission, and to increase the attractiveness of the EU for business and tourism.

In comparison to visa-required third country nationals, the competent border and law enforcement authorities have little information on visa-exempt third country nationals as regards risks they may pose before their arrival at the Schengen border. Adding this missing layer of information and risk assessment on visa free visitors would bring significant added value to existing measures to maintain and strengthen the security of the Schengen area and will allow visa free visitors to fully enjoy their visa-free status.

Building an effective and integrated external border management based on new technologies by harnessing the full potential of interoperability was set out in the Communication *'Stronger and*

---

1 In a recent Eurobarometer survey, 71% of respondents called for more EU action in relation to external borders and 82% in relation to counter-terrorism (Special Eurobarometer of the European Parliament, June 2016).

2 Technical Study on Smart Borders, European Commission, DG HOME, 2014. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/index_en.htm Visa liberalisation dialogues with a number of countries in the EU's neighbourhood have been concluded (Commission proposals presented on Georgia, Ukraine, Turkey and Kosovo).

3 COM(2016) 602 final.

Smarter Information Systems for Borders and Security"[4], and applied in a revised legislative proposal for an EU Entry/Exit System (EES)[5]. The EES proposal aims to modernise the collection and registration of entry and exit records of non-EU citizens crossing the EU external borders. In parallel, the Commission launched a feasibility study[6] on establishing a European Travel Information and Authorisation System (ETIAS). ETIAS would collect information from visa free third country nationals, and ensure interoperability in terms of information and technological infrastructure with the EES and other EU information systems. To ensure maximum interoperability and resource sharing, the development and implementation of EES and ETIAS should be carried out together and in parallel. The importance of proposing swiftly a European Travel Information and Authorisation System was underlined by President Juncker in September's State of the Union address and the Commission announced that a legislative proposal for the establishment of this system would be adopted by November 2016.

In this context, and following the reference to ETIAS in the Bratislava Roadmap[7], the European Council in October 2016[8] invited the Commission to put forward a proposal for setting up ETIAS, stressing the need "*to allow for advance security checks on visa- exempt travellers and deny them entry where necessary*".

Rationale for the setting up of ETIAS

ETIAS will be an automated system created to identify any risks associated with a visa-exempt visitor travelling to the Schengen Area. Countries like the USA, Canada and Australia already use similar systems and consider these as an essential part of their security frameworks – as a result, these systems are now familiar to many Europeans.

ETIAS will gather information on these travellers prior to the start of their travel, to allow for advance processing. For the travellers, this will give them confidence that they would be able to cross the borders smoothly.

Strengthening integrated border management and enhancing internal security

At the moment, there is no advance information as regards visa exempt visitors coming to the Schengen external border. Both from a migration and from a security point of view, there is a clear necessity to conduct prior checks in order to identify any risks associated with a visa-exempt visitor travelling to the Schengen Area. At present border guards need to make the decision at the Schengen area external borders without the benefit of a prior assessment. In 2014, approximately 286,000 third country nationals were refused entry at the external borders of the EU-28. Most refusals were recorded at the external land borders (81%), followed by refusals at air borders (16 %). Approximately one-fifth of these refusals were due to the lack of a valid visa, but most cases were related to a negative assessment of the migration and/or security risk represented by the

---

4 COM(2016) 205 final.

5 Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union COM(2016) 194 final, and Proposal for a Regulation of the European Parliament and of the Council for a amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System.

6 Feasibility Study for a European Travel Information and Authorisation System (ETIAS), Final Report; http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents/docs/20161116/etias_feasability_study_en.pdf.

7 http://www.consilium.europa.eu/en/press/press-releases/2016/09/16-bratislava-declaration-and-roadmap/

8 EUCO 31/16 CO EUR 8, CONCL 4 www.consilium.europa.eu/en/.../european-council/2016/10/21-euco-conclusions_pdf/

third country national.[9] Europol and the European Border and Coast Guard risk assessments confirm[10] the existence of these risks both from an irregular migration and from a security point of view.

Therefore, the key function of ETIAS would consist in checking the information submitted by visa-exempt third country nationals, via an online application ahead of their arrival at EU external borders, if they pose certain risks for irregular migration, security or public health. This would be done by automatically processing each application submitted via a website or a mobile application against other EU information systems, a dedicated ETIAS watchlist and clearly defined screening rules. This examination would allow to determine that there are no factual indications or reasonable grounds to prevent a travel authorisation being issued.

Through the setting up of ETIAS, a mandate would be given to the European Border and Coast Guard to ensure via an ETIAS Central Unit the management of the ETIAS Central System that will be connected and integrated in the national border guard infrastructures. Applications rejected from the automatic processing would be transferred to an ETIAS Central Unit in the European Border and Coast Guard which will quickly verify the correctness of information provided and alerts identified. Applications subject to an alert or hit will be forwarded to the Member State(s) responsible. The Agency for the operational management of large-scale information systems in the area of freedom, security and justice ('eu-LISA') would develop the ETIAS Information System and ensure its technical management. Europol would give its input when it comes to security aspects.

By requiring a valid travel authorisation for all visa-exempt third country nationals, regardless of their mode of travelling or their point of entry, the EU will ensure that all visitors are checked prior to arrival while fully respecting their visa-free status. The system is however especially relevant for land borders as those visa-exempt third-country nationals travelling by land (foot, car, bus, truck, train) do not generate Advance Passenger Information (API) or Passenger Name Records (PNR) as is the case with air- and/or sea-travel.

Accordingly, ETIAS will reinforce EU internal security in two ways: first, through the identification of persons that pose a security risk before they arrive at the Schengen external border; and second, by making information available to national law enforcement authorities and Europol, where this is necessary in a specific case of prevention, detection or investigation of a terrorist offence, or other serious criminal offences.

Travel facilitation

ETIAS will also facilitate the crossing of the Schengen external border by visa-exempt third country nationals. An ETIAS authorisation would be obtained through an application process, which would be simple, cheap, fast and would in the vast majority of cases not require any further steps. According to the experience of other countries with similar systems for travel authorisations (US, Canada, Australia), an estimated 95% or more would result in a positive reply, which would be communicated to applicants within minutes. Fingerprints and other biometric data would not be collected. The authorisation would be valid for five years and for multiple travels and its application fee will only be € 5. The authorisation prior to travel would offer clarity to visa exempt third country nationals bound for the Schengen area. Once the applicants receive the travel authorisation, they would have a reliable early indication of admissibility into the Schengen area. This is a significant improvement for travellers compared to the current state of play.

---

9 http://ec.europa.eu/eurostat/statistics-explained/index.php/Statistics_on_enforcement_of_immigration_legislation

10 Europol TE-SAT 2016 https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report

Even if the final decision on allowing entry into the Schengen Area will still rest with the border guards at the external border in line with the Schengen Border Code, ETIAS will substantially reduce the number of cases of refusals of entry at the border crossing points. Border guards will be able to see if the person before them has obtained a travel authorisation or not before arriving at the border. ETIAS in this way will also reduce the costs for carriers to return passengers from sea and air borders. Persons having been denied authorisation will not waste time and money to travel to the Schengen area. Such decisions can be appealed in the Member State that has taken that decision and would not require launching lengthy and expensive visa application process as in the case of similar systems for travel authorisations.

Main elements of ETIAS

Definition

The proposed European Travel Information and Authorisation System (ETIAS) will be an EU system for visa-exempt third country nationals when crossing the external borders. The system would enable to determine whether the presence of such persons on the territory of the Member States would pose an irregular migration, security or public health risk.

For this purpose a travel authorisation would be introduced as a new condition for entering the Schengen area and the absence of a valid ETIAS travel authorisation would result in a refusal of entry into the Schengen area.

Moreover, where applicable, carriers would have to check that their passengers have a valid ETIAS travel authorisation before allowing them to board their transportation means bound to a Schengen country.

A valid travel authorisation would be a reliable indication to the visitor that the risk assessments performed in advance of arrival at a Schengen border crossing point makes him/her, a priori, eligible for entering the Schengen area. The border guard would still conduct the border control checks as provided under the Schengen Border Code and would take the final decision for granting or refusing entry.

The ETIAS would be composed of the ETIAS Information System, the ETIAS Central Unit and the ETIAS National Units.

The ETIAS Information System would be composed of a Central System to process the applications; a National Uniform Interface in each Member State based on the same technical specifications for all Member States, and connecting their national border infrastructures to the Central System; a secure Communication Infrastructure between the Central System and the National Uniform Interfaces; a public website and a mobile app for mobile devices; an email service; a secure account service enabling applicants to provide additional information and/or documentation, if deemed necessary; a carrier gateway; a web service enabling communication between the central system and external stakeholders, and a software enabling the ETIAS Central Unit and the ETIAS National Units to process the applications.

To the maximum extent possible and technically feasible, the ETIAS Information System will re-use the hardware and software components of the EES and its communication infrastructure. Interoperability would also be established with the other information systems to be consulted by ETIAS such as the VIS, the Europol data, the Schengen Information System (SIS), the Eurodac and the European Criminal Records Information System (ECRIS).

The ETIAS Central Unit will be established within the European Border and Coast Guard, and will be part of its legal and policy framework. Operating on a 24/7 basis, the ETIAS Central Unit

will have four central tasks: 1) ensuring that the data stored in the application files and the data recorded in the ETIAS Information System are correct and up to date, 2) where necessary, verifying the travel authorisation applications to remove any ambiguity about the applicant's identity in cases of a hit obtained during the automated process, 3) defining, testing, implementing, evaluating and revising specific risk indicators of the ETIAS screening rules after consultation of the ETIAS Screening Board, and 4) carrying out regular audits on the management of applications and on the implementation of the ETIAS screening rules, particularly as regards their impacts on fundamental rights and especially with regards to privacy and data protection.

ETIAS National Units would be established in each Member State, and would have the primary responsibility of conducting the risk assessment and deciding on travel authorization for applications rejected by the automated application process. They would need to have adequate resources to fulfil their tasks on a 24/7 basis. If necessary, they would consult other National Units and Europol and would issue opinions when consulted by other Member States. They would also act as national central access points regarding requests for access to the ETIAS data for law enforcement purposes in order to prevent, detect and investigate terrorist offences or other serious criminal offences falling under their competence.

An ETIAS Screening Board with an advisory function would also be established within the European Border and Coast Guard. It would be composed of a representative of each ETIAS National Unit and Europol, and would be consulted for the definition, evaluation and revision of the risk indicators as well as for the implementation of the ETIAS watchlist.

Scope

ETIAS will apply to visa-exempt third country nationals, including, and when it comes to checking the security and public health risk, to family members of European Union citizens and of nationals of a third country enjoying the right to free movement if they do not hold a residence card.

ETIAS will not apply to: holders of long-stay visas, holders of a local border traffic permits, citizens of the micro-states in the Schengen area, holders of diplomatic passports and crew members of ships or aircraft while on duty, third-country nationals who are family members of EU citizens or of a national of a third country enjoying the right of free movement under the Union law and hold a valid residence card and recognised refugees, stateless persons or other persons who reside and hold a travel document issued by a Member State.

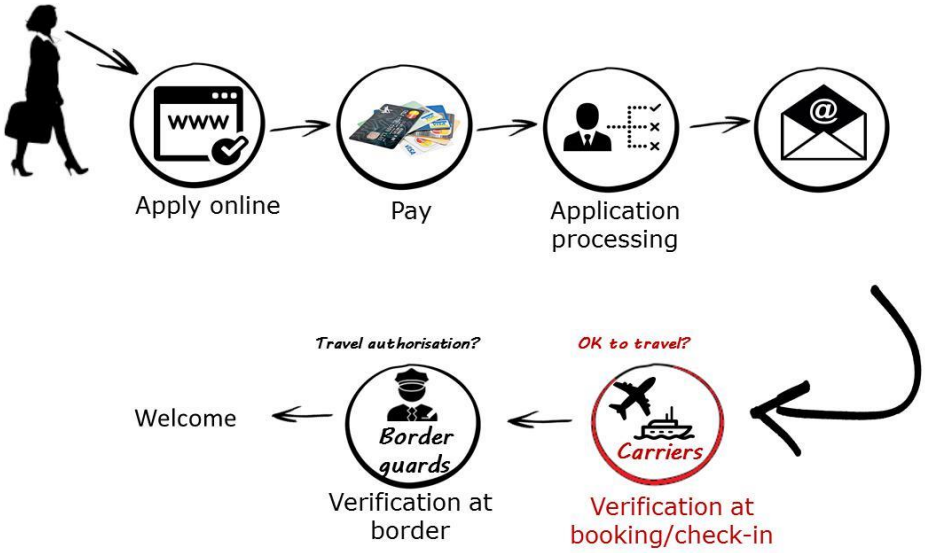
ETIAS does not apply to EU citizens. Consequently, third country nationals having multiple nationalities, including the nationality of an EU Member State must use the passport issued by an EU Member State for entering the Schengen area.

Local border traffic permit holders are excluded from the scope of the ETIAS Regulation, pending a thorough assessment of the security risks associated with this category of persons in accordance with Regulation (EC) No 1931/2006, which lays down rules on local border traffic at the external land borders of the Member States and amending the provisions of the Schengen Convention. The European Commission will examine the necessity of modifying Regulation (EC) No 1931/2006, to ensure that the conditions for issuing local border traffic permits, guarantee appropriate security risk assessments, while not prejudicing in any way the facilitations provided to local border traffic permit holders by Regulation (EC) No 1931/2006 and the Schengen Borders Code. The European Commission will also examine the security features of the permit itself.

Travel Authorisation Application and Issuance Process

The legislative proposal sets out in detail the practical steps and the process for issuing or refusing the travel authorisation. The figure below presents an overview of the process from the visa exempt third country national's perspective.

Figure 1: Traveller's journey with ETIAS



Online application

Prior to the intended travel, the applicant creates an on-line application, via a dedicated website or the mobile application.

To fill in the application, each applicant will be requested to provide the following data:

– Surname (family name), first name(s), surname at birth, usual name(s); date of birth, place of birth, country of birth, sex, current nationality, first names of the parents of the applicant; home address;

– Travel document;

– If applicable, any other nationality;

– Permanent residence information;

– Email address and phone number;

– Member State of intended first entry;

– Education and current occupation details;

– Answers to a set of ETIAS background questions (as regards conditions with epidemic potential or other infectious or contagious parasitic diseases; criminal records; presence in war zones; and any previous decision to return to borders or orders to leave the territory of an EU Member State),

– If the applicant is a minor, the identity of the person responsible for the minor,

– If the application is submitted by a person different of the applicant, the identity of the person and company that he or she represents (if applicable).

– For family members to EU citizens/third country nationals benefitting from free movement without residence cards: their status as family member; the identity details of the family member with whom the applicant has ties; their family ties.

Filling the application form online would in principle not take more than 10 minutes. Apart from having a valid passport, no further documentation would be required to reply to the questions asked.

ETIAS would accept applications introduced on behalf of the applicant in situations where visa exempt third country nationals cannot themselves create an application (for example, because of age, literacy- level, access to and inability to use information technology). In such cases, the application may be submitted by a third person provided this person's identity is included in the application.

Applicants intending to travel from far away would usually purchase a ticket online or through a travel agent. Both possibilities involve the use of information technology. Consequently, the applicant will have direct access to the technology required for introducing the ETIAS application or will have the possibility to request the travel agent to introduce the application on his/her behalf.

Payment of the fee

Once the application is ready, the payment of a fee of €5 per application will be required for all applicants above the age of 18. This would be an electronic payment in euro using a credit card or other payment methods. The payment methods available may be specified further at a later stage, in order to include additional and up to date means of payment, taking account of technological developments and their availability, in order not to hinder visa-free third country nationals who may not have access to certain payment means when applying for an ETIAS authorisation.

The payment would be managed by a bank or a financial intermediary. Data required for completing the payment would only be provided to the company operating the financial transaction and would not be processed by ETIAS in the context of the application.

Once the payment is received, the ETIAS application is automatically introduced.

Application processing

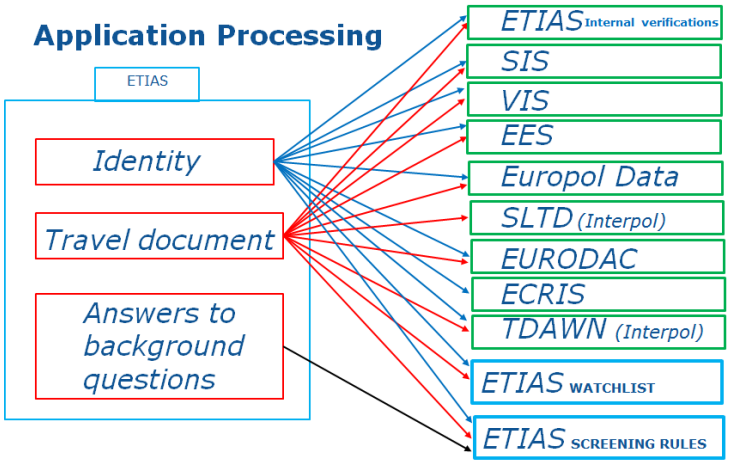
The process of assessing and deciding on an application would start immediately after the payment of the fee is confirmed.

The application would be automatically processed. Where applicable, the application would undergo manual processing by the ETIAS Central Unit and ETIAS National Unit(s).

Step 1 - Automated processing

This automated step will process data related to identity data, travel document, and the answers to the background questions. The central system will, within minutes, proceed to a fully automated cross-checking of the information provided by the applicant against other information systems, a watchlist established in ETIAS and against ETIAS' clearly defined screening rules.

Figure 2: Automated Application Processing



The objective of this automated process is to ensure that:

– no other valid travel authorisation already exists, the data provided in the application concerning the travel document do not correspond to another application for travel authorisation associated with different identity data, and the applicant or the associated travel document do not correspond to a refused, revoked or annulled application for travel authorisation (ETIAS);

– the applicant is not subject to a refusal of entry alert (SIS) and/or the travel document used for the application does not correspond to a travel document reported lost, stolen or invalidated (SIS and Interpol's SLTD);

– whether the applicant is not subject to an alert on the basis of a European Arrest Warrant or wanted for arrest for extradition purposes (SIS)

– the applicant has not been reported as an overstayer, at present or in the past, or has was refused entry (EES);

– the applicant had no visa application refused in Visa Information System (VIS – this would be valid for nationals of countries which were granted visa waiver status within five years or less and for applicants having more than one nationality);

– the applicant and the data provided in the application corresponds to information recorded in the Europol data;

– a risk assessment is conducted for irregular migration risks, particularly as to whether the applicant was subject to a return decision or a removal order issued following the withdrawal or rejection of the application for international protection (EURODAC[11]);

– no criminal record is recorded (ECRIS);

– the applicant and/or his/her travel document are not subject to an Interpol alert (TDAWN).

This automated process would also ensure that the applicant is not in the ETIAS watchlist and would verify if the applicant has replied affirmatively to any of the ETIAS background questions.

[11] COM(2016) 272 final.

Clearly defined screening rules within the ETIAS Central System will be used to assess the application file. These rules will consist of an algorithm which will compare the data recorded in an ETIAS application file, and specific risk indicators pointing to identified irregular migration, security or public health risks. The specific risk indicators will be established by the ETIAS Central Unit after consultation with the ETIAS Screening Board (see below).

The irregular migration, security or public health risks will be determined on the basis of:

– EES statistics on abnormal rates of overstays or refusals of entry for specific groups of third country nationals;

– ETIAS statistics on travel authorisation refusals due to irregular migration, security or public health risks associated with specific groups of third country nationals;

– Statistics generated by both EES and ETIAS showing correlations between the information collected through the ETIAS application form and overstays or refusals of entry.

– Information provided by Member States concerning specific security risk indicators or threats identified by those Member States.

– Information provided by Member States as well as the European Centre for Disease Prevention and Control (ECDC) concerning specific public health risks.

These screening rules and the irregular migration, security or public health risks will be targeted, proportionate and specific. The sets of data used for these rules will in no circumstances be based on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, sexual life or sexual orientation.

If the automatic process has not reported any hit or any element requiring additional analysis, the travel authorisation is issued automatically and the applicant is informed by email. Such a positive answer will concern the vast majority of applications (expected to exceed 95% of cases) and will be communicated to the applicant within minutes after payment.

If the automatic process has reported a hit or has identified elements requiring additional analysis, the application will be further assessed manually.

Step 2 (if necessary) - manual processing by the ETIAS Central Unit

If the automatic examination reports a hit from other information systems or the ETIAS watchlist or specific risk indicators, or is indecisive because there is uncertainty about the identity of the applicant a manual examination by the ETIAS Central Unit would follow. The ETIAS Central Unit will check the application to remove any ambiguity about the applicant's identity, using the information reported through the automatic process. This again may lead to a positive decision on the application, within 12 hours. If there is a confirmed hit, the application is transferred to the ETIAS National Unit of the Member State of first entry, as declared by the applicant during the application process.

It is expected that an additional 3-4% of applications would receive a positive decision after the verification of data done by the ETIAS Central Unit. This would leave the remaining 1-2% of ETIAS applications reporting a hit or hits to be transferred to ETIAS National Units for manual processing and a decision.

Step 3 (where applicable) – manual processing by the ETIAS National Unit of the Member State of intended first entry

If the automatic process by the ETIAS Central System detects a (confirmed) hit against any of the consulted databases or the ETIAS watchlist, and/or indicates that the applicant corresponds to the screening rules, the application will be transferred to the ETIAS National Units.

Attribution of the application by ETIAS to a specific Member State would be automated, and directed to the Member State of the traveller's intended first entry as declared in the application form.

Once the application has been transferred to the responsible ETIAS National Unit, the ETIAS National Unit would have to assess the application file and inform the applicant no later than 72 hours after lodging the application about the decision taken (negative or positive). The task of the responsible ETIAS National Unit would be to assess the irregular migration, security or public health risk and decide whether to issue or refuse a travel authorisation.

When the applicant receives a negative decision on his/her application, they will always have the right to appeal. Appeals would be launched in the Member State that has taken the decision on the application and in accordance with the national law of that Member State. In addition, a special procedure is foreseen in situations for humanitarian grounds, for reasons of national interest or because of international obligations where ETIAS National Units may issue a travel authorisation with limited territorial and temporal validity.

Where the information provided by the traveller in the application form does not allow the responsible ETIAS National Unit to decide whether to issue or refuse travel authorisation, more information and/or documentation may be requested from the applicant by the ETIAS National Unit. The request would be communicated to the applicant via email and would clearly indicate the missing information and/or documentation to be provided. This information would need to be provided within 7 working days, and the ETIAS National Unit would need to process this information no later than 72 hours after the date of submission by the traveller. In exceptional circumstances, the applicant may be invited via email for an interview at a consulate in his/her country of residence.

When manually assessing applications for which they are responsible, the ETIAS National Units are allowed to use information available in national databases or other decentralised systems to which they have access. In this process, the responsible authorities of other Member States and Europol would also be consulted and would receive access to the relevant additional information or documentation, if they are responsible for data having triggered a hit in the course of the cross-checking of other information systems. The ETIAS National Unit of the consulted Member States would then within 24 hours issue a reasoned opinion, either positive or negative, on the application, which would be recorded on the application file. When one or more ETIAS National Units consulted issue a negative opinion on the application, the responsible Member State would refuse the travel authorisation.

In the context of this manual processing, it is imperative that competent law enforcement authorities, have access to relevant and clearly defined information in ETIAS, when this is necessary to prevent, detect and investigate terrorist offences or other serious criminal offences. Access to data contained in the Visa Information System (VIS) for law enforcement purpose has already proven effective in helping investigators to make substantial progress in cases related to human being trafficking, terrorism or drug trafficking. The Visa Information System, however, does not contain data on visa-exempt third-country nationals.

In an era of globalised crime, information generated by ETIAS could be necessary to be accessed by law enforcement authorities in a specific investigation and in order to establish evidence and

information related to a person suspected of having committed a crime or be the a victim of a crime. 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 data for these purposes should only be granted following a reasoned request by the competent authorities giving reasons for its necessity. The request should be the subject of a prior review by a court or by an authority providing guarantees of full independence and impartiality. However, in situations of extreme urgency, it can be crucial for the law enforcement authorities to obtain immediately personal data necessary for preventing the commission of a serious crime or so that its perpetrators can be prosecuted. In these cases, the review of the personal data obtained from ETIAS takes place as swiftly as possible after access to such data has been granted to the competent authorities.

To prevent systematic searches of ETIAS by law enforcement authorities, the access to data stored in the ETIAS Central System would 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 crime. The designated authorities and Europol should only request access to ETIAS when they have reasonable grounds to believe that such access will provide information that will substantially assist them in preventing, detecting or investigating a terrorist offence or other serious criminal offence. The designated authorities and Europol should only request access to the ETIAS if prior searches in all relevant national databases of the Member State and databases at Europol did not lead to the requested information.

If the manual processing of the application is conducted as a result of a hit in the Europol data, the ETIAS National Unit of the responsible Member State would consult Europol in cases falling under Europol's mandate. In those cases, the ETIAS National Unit of that Member State would transmit to Europol the relevant data of the application file as well as the hit(s) which are necessary for the purpose the consultation, as well as the relevant additional information or documentation provided by the applicant. Europol would provide a reasoned opinion within 24 hours.

The ETIAS National Unit will upload the information concerning the final decision in the central system. When the system notifies the decision to the applicant he or she will be informed, where relevant, of which national authority was responsible for the processing and decision on his or her travel authorisation. The ETIAS Central System, Central Unit and National Unit will keep records of all data processing operations performed. Those records would show the date and time, the data used for the automated processing of the applications and the hits found while carrying out the verifications. The decision taken concerning the travel authorisation, positive or negative, would be justified and explained. The decision and the corresponding justification are recorded in the individual ETIAS application file by the entity having taken the decision.

In all cases a final decision shall be taken by the ETIAS National Unit within two weeks after receipt of the application by the central system.

Response to applicants

Applicants would receive an email with a valid travel authorisation and the authorisation's number, or a justification for the refusal. The validity of the travel authorisation would be 5 years (or until the expiry date of the passport). If the travel authorisation is refused, the applicant would be informed which national authority was responsible for the processing and decision on his or her travel authorisation, as well as information regarding the procedure to be followed in the event of an appeal.

Check by carriers

Prior to boarding, carriers have to verify if visa exempt third country nationals have a valid ETIAS travel authorisation. They could do this by means of an online interface, or through other mobile technical solutions.

If a traveller with a valid travel authorisation would be subsequently refused at entry, the carrier would remain liable for taking the traveller back to the initial point of embarkation but would not incur any penalty.

If a traveller who does not have a valid travel authorisation is authorised boarding and is subsequently refused entry, the carrier would not only remain liable for taking the traveller back to the initial point of embarkation but would also incur a penalty.

Arriving at the Schengen area border crossing point

When the traveller arrives at the border crossing point, the border guard will, as part of the standard border control process, electronically read the travel document data. This will trigger a query to different databases as provided under the Schengen Border Code including a query to ETIAS which would provide the up-to-date travel authorisation status. The ETIAS file itself would not be accessible to the border guard for border controls.

If there is no valid travel authorisation, the border guard would have to refuse entry to the Schengen area and complete the border control process accordingly. The traveller would be registered in EES, as well as the refusal of entry according to the EES Regulation.

If there is a valid travel authorisation, the border control process would be conducted as per the Schengen Border Code. As a result of this process, the traveller may be authorised to enter the Schengen area or refused access under the conditions defined in the Schengen Border Code.

Revocation or annulment of travel authorisations

An issued travel authorisation has to be annulled or revoked as soon as it becomes evident that the conditions for issuing it were not met at the time of issuing, or are no longer met, particularly when there are serious grounds for believing that the travel authorisation was fraudulently obtained. The revocation or annulment decision will in principle be taken by the authorities of the Member State that is in possession of the evidence leading to the revocation or annulment, or by the ETIAS National Unit of the Member State of first entry as declared by the applicant.

In particular, when a new SIS alert is created for a refusal of entry, the SIS will inform the ETIAS Central System, which would in turn verify whether this new alert corresponds to a valid travel authorisation. If that is the case, the Member State having created the alert will be immediately informed and will have to proceed to the revocation of the travel authorisation.

Role of Europol

Europol contributes to the added value that ETIAS will provide to EU internal security. This reflects Europol's role as EU information hub and core security cooperation tool within a reinforced regulatory framework. Data provided by applicants for an ETIAS authorisation will be cross-checked against data that is held by Europol related to persons who are suspected of having committed or taken part in a criminal offence, who have been convicted of such an offence, or regarding whom there are factual indications or reasonable grounds to believe that they will commit such an offence. Europol is in a unique position to combine information that is not available to individual Member States or in other EU databases.

This is why Europol will be involved in the definition of ETIAS screening rules through its participation in the ETIAS Screening Board. It will also manage the ETIAS watchlist within Europol data. Moreover, ETIAS National Units may consult Europol in the follow up to a hit that occurred during the ETIAS automated processing in cases falling under Europol's mandate. This will allow ETIAS National Units to benefit from relevant information that might be available at Europol when assessing an ETIAS application by a person that might pose a security threat. Finally, Europol may request consultation of data stored in the ETIAS Central System in a specific case where Europol supports action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences falling under Europol's mandate.

ETIAS technical infrastructure

The ETIAS would provide the technical infrastructure:

– For applicants to introduce the data required for each travel authorisation application online, with the appropriate guidance in case of doubt;

– For the ETIAS Central System to create, update and delete the travel authorisation application, and the information collected to handle the application, until the decision to grant or refuse authorisation is taken;

– For the ETIAS central system to process the personal data of the applicant to query specific databases and to retrieve the information they contain concerning the applicant, for the purpose of assessing the application;

– For border guards to access the travel authorisation status of an applicant from any Schengen border crossing point, by reading data on the travel document's machine readable zone or application number;

– For carriers to consult the travel authorisation status using only data on the travel document's machine readable zone or the application number;

– For staff in the ETIAS Central Unit and in ETIAS National Units to manage the process of handling the applications, including the exchanges with other Member State's competent authorities and the notifications to the applicants;

– For the ETIAS Central Unit as well as for staff and competent authorities in the ETIAS National Units to produce statistics using anonymised data, without enabling the identification of individuals by narrowing statistics to a very small group.

The technical infrastructure of ETIAS needs to provide timely responses to border control operations and to carriers on a 24/7 basis with an availability of 99,9%. The ETIAS Information System also needs to ensure the highest security protection mechanisms against intrusion, access and disclosure of data to non-authorised persons, corruption and loss of integrity of data. Compliance with this requirement will be sought by the adoption of a security plan as an implementing measure.

Data Retention period

As a general rule the duration for the storage of the ETIAS application data will be 5 years after the last use of the travel authorisation or from the last decision to refuse, revoke or annul a travel authorisation. This retention period corresponds to the retention period of an EES record with an entry authorisation granted on the basis of an ETIAS travel authorisation. This synchronisation of

retention periods ensures that both the entry record and the related travel authorisation are kept for the same duration and is an additional element of interoperability between ETIAS and EES. This synchronisation of data retention periods is necessary to allow the competent authorities performing the necessary risk analysis requested by the Schengen Borders Code and ETIAS. The retention period will also reduce the re-enrolment frequency and will be beneficial for all travellers. Beyond this period the ETIAS application file would be automatically and completely erased.

Interoperability and resource-sharing with EES

The proposed Regulation includes a general principle that ETIAS is built on the interoperability of information systems to be consulted (EES, SIS, VIS, Europol data, Eurodac and ECRIS) and on the re-use of components developed for those information systems, the EES in particular. This approach results also in significant cost saving for the set up and operation of ETIAS.

ETIAS and EES would share a common repository of personal data of third-country nationals, with additional data from the ETIAS application (e.g. residence information, answers to background questions, IP address) and the EES entry-exit records separately stored, but linked to this shared and single identification file. This approach is fully in line with the interoperability strategy proposed in the Communication on Stronger and Smarter Information Systems for Borders and Security of 6 April 2016, and would include all appropriate data protection safeguards.

The following components of EES are shared or re-used:

– the wide-area network (implemented as a virtual network and currently called Testa-ng that links Member State national domains with the central domain) has sufficient capacity to convey the ETIAS communications between national infrastructures and the central system;

– the National Uniform Interface which is a generic system developed and deployed by eu-LISA to provide a set of communication services between the national border control infrastructures and the central system will also be used for handling the ETIAS messages.

– the technical means that allow carriers to query the ETIAS status of visa exempt third country nationals travelling to the Schengen area will use the same service as provided for EES.

– the technical means that allow applicants to introduce requests to ETIAS (implemented as a web interface and mobile platform) will also use the infrastructure put in place in EES for allowing travellers to consult outstanding durations of authorised stay.

Costs of development phase and running phase

The cost for developing the ETIAS system is estimated at € 212,1 million and the average annual operations cost at € 85 million. The ETIAS would be financially self-sustaining as the annual operations costs would be covered by the fee revenue.

Existing provisions in the area of the proposal

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

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

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

Regulation (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).

Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) COM(2016) 194 final.

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.

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

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

Regulation (EU) 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.

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.

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.

2. CONSULTATION OF INTERESTED PARTIES AND IMPACT ASSESSMENT

Consultation of interested parties

The ETIAS proposal was developed on the basis of a feasibility study. As part of this study, the Commission collected the views of Member State experts on border control and security. In addition the main elements of the ETIAS proposal were discussed in the framework of the High

Level Expert Group on Interoperability that was set up as a follow-up of the Communication on Stronger and Smarter Borders of 6 April 2016. Consultation took also place with representatives of the air, sea and rail carriers, as well as with representatives of EU Member States with external land borders. As part of the feasibility study, a consultation of the Fundamental Rights Agency was also undertaken.

Impact assessment

The ETIAS legal proposal is based on the results of the feasibility study conducted from June till October 2016.

3. LEGAL ELEMENTS OF THE PROPOSAL

Summary of the proposed actions

The purposes, functionalities and responsibilities for the ETIAS are defined in the legislative proposal. The proposal gives a mandate to the European Border and Coast Guard to ensure the creation and management of an ETIAS Central Unit. In addition, a mandate is given to the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) to develop and to ensure the technical operational management of the system. Europol is also given a significant role in terms of ensuring the security objectives of the ETIAS.

Therefore, consequential amendments to Regulation (EU) No 2016/399, Regulation (EU) No 2016/1624, to Regulation (EU) No 1077/2011, and Regulation (EU) 2016/794 are included in this proposal.

Consequential amendments to Regulations concerning the EU systems that will be queried by ETIAS shall be the object of separate Commission Proposals.

This legislative proposal establishes the elements of the ETIAS. The technical and operational details will be agreed at a later stage, in the framework of implementing decisions, where the Commission shall adopt further measures and rules on:

– the establishment and the high level design of the interoperability;

– the specifications and conditions for the website ;

– the entering the data;

– the definition of specific categories of data ;

– accessing the data ;

– determining the information systems to be consulted ;

– defining the screening rules;

– amending, deleting and advance deleting of data ;

– keeping and accessing the records ;

– performance requirements, including minimal specifications for technical equipment.

Legal basis

The proposal uses Article 77(2) (b) and (d) of the Treaty on the Functioning of the European Union as the legal basis for this Regulation. Article 77(2) (b) and (d) is the appropriate legal basis for further specifying the measures on the crossing of the external borders of the Member States, developing standards and procedures to be followed by Member States in carrying out checks on persons at such borders and specifying measures towards the gradual establishment of an integrated management system for external borders.

In addition, the proposal relies on Article 87(2) (a) as a legal basis to allow access for law enforcement purposes under strict conditions. This additional legal basis for law enforcement access involves the same ordinary legislative procedure applicable under Article 77(2) (b) and (d).

Finally, the proposal also relies on Article 88(2) (a) to the extent that it amends the list of tasks of Europol.

Subsidiarity principle

The proposed initiative falls within the scope of Article 77(2) (b) TFEU, where the European Union has competence to adopt measures relating to the checks on persons and the efficient monitoring of the crossing of external borders of the Member States.

The current EU framework on the crossing of the external borders of the Member States does not offer the possibility of automated, coordinated and homogenous prior screening of visa-exempt third country nationals. This does not enable Member States to apply the common Schengen rules in a harmonised and coordinated way. There is a clear cross-border problem as visa exempt third country nationals can freely choose the first point of entry into the Schengen area in order to avoid certain controls at certain border points. As for visa applicants, information should be available on visa-exempt third country nationals in order to enhance the effectiveness of security and immigration checks on persons and the overall quality of EU external border management.

These objectives cannot be sufficiently achieved by the Member States acting alone, and can better be achieved at Union level.

Proportionality principle

Article 5 of the Treaty on the European Union states that action by the Union shall not go beyond what is necessary to achieve the objectives of the Treaty. The proposed initiative constitutes a further development of the Schengen acquis in order to ensure that common rules at external borders are applied in the same way in all the Member States which have abolished controls at internal borders. It creates an instrument providing the European Union with the means to ensure that the rules to assess the irregular migration, security and public health risks from visa-exempt third country nationals are as consistently applied as for visa-required third country nationals by all Member States.

It also provides for consultation of data stored in the ETIAS Central System for law enforcement authorities where this is necessary in a specific case of the prevention, detection or investigation of terrorist offences or other serious criminal offences. In such a case and where prior searches in national and Europol databases did not lead to the requested information, ETIAS provides national law enforcement authorities and Europol with a timely, accurate, secure and cost-efficient way to investigate visa-exempt third-nationals who are suspects (or victims) of terrorism or of a serious crime. It enables competent authorities to consult the ETIAS application file of visa-exempt third-country nationals who are suspects (or victims) of such serious crimes.

The proposal includes all appropriate data protection safeguards and is proportionate in terms of the right to protection of personal data. It adheres to the data minimisation principle, includes strict data security provisions, and does not require the processing of data for a longer period than is absolutely necessary to allow the system to function and meet its objectives. All safeguards and mechanisms required for the effective protection of the fundamental rights of third country nationals, will be foreseen and implemented fully (see the section below on Fundamental Rights).

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

Choice of instrument

Proposed instruments: Regulation.

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

The present proposal will set up a centralised system through which Member States cooperate with each other on Schengen external border management, something which requires a common architecture and common operating rules. It will lay down rules on risk assessment checks on irregular migration, security and public health for visa exempt third country nationals prior to their arrival at the external borders and on access to the system including for the purpose of law enforcement, which are uniform for all Member States. Moreover, the Central System will be managed by the European Border and Coast Guard. As a consequence, only a Regulation can fully achieve these objectives and should be chosen as a legal instrument.

Fundamental rights

The proposed Regulation has an impact on fundamental rights, notably on right to dignity (Article 1 of the Charter of Fundamental Rights of the EU); right to liberty and security (Article 6 of the Charter), respect for private and family life (Article 7 of the Charter), the protection of personal data (Article 8 of the Charter), right to asylum (Article 18 of the Charter) and protection in the event of removal, expulsion or extradition (Article 19 of the Charter), the right to non-discrimination (Article 21 of the Charter), the rights of the child (Article 24 of the Charter) and the right to an effective remedy (Article 47 of the Charter).

The legitimate public interest of ensuring a high level of security is positively affected by the implementation of an ETIAS. A better and more accurate identification of the security risk of visa-exempt third country nationals crossing the external border of the Schengen area supports the detection of trafficking in human beings (particularly in the case of minors) and cross border criminality, and it more generally facilitates the identification of persons whose presence in the Schengen area would pose a security threat. ETIAS thus contributes to improving the security of the citizens present in the Schengen area and enhancing internal security in the EU.

ETIAS guarantees non-discriminatory access to all visa exempt third country nationals to the applications process, ensuring that the decisions taken will in no circumstances be based on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, sexual life or sexual orientation. ETIAS provides guarantees ensuring information for the person who submitted an application and effective remedies.

Concerning the right to protection of personal data, the proposal contains all appropriate safeguards as regards personal data, in particular regarding access, which should be strictly limited only to the purpose of this Regulation. It also foresees individuals' rights of redress, particularly as regards the right to a judicial remedy and the supervision of processing operations by public independent

authorities. The limitation of the retention period of data referred to above also contributes to the respect for protection of personal data as a fundamental right.

The proposal provides for consultation by national law enforcement authorities and Europol to the ETIAS Central System for the prevention, detection or investigation of terrorist offences or other serious criminal offences. As stipulated by Article 52(1) of the Charter, any limitation to the right to the protection of personal data must be appropriate for attaining the objective pursued and not going beyond what is necessary to achieve it. Article 8(2) of the European Convention of Human Rights also recognises that interference by a public authority with a person's right to privacy may be justified as necessary in the interest of national security, public safety or the prevention of crime, as it is the case in the current proposal. The Court of Justice has also recognised that the fight against terrorism and serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern information technologies and investigation techniques and hence, access to personal data granted for those specific purposes could be justified if considered necessary. Therefore, the proposal fully complies with the Charter of Fundamental Rights of the European Union as regards the right to the protection of personal data, and is also in line with Article 16 TFEU, which guarantees everyone the right to protection of personal data concerning them.

The proposal provides for access to the ETIAS for the prevention, detection or investigation of terrorist offences or other serious criminal offences for the purpose of accessing data submitted by visa-exempt third-country nationals when applying for a travel authorisation. Although similar data exist in the VIS on visa holders or applicants, such data on visa exempt nationals are not available in any other EU database. The globalisation of criminality follows the globalisation of economics.[12] International criminal organisations are developing their activities across borders.[13] Criminal activities such as trafficking in human beings, smuggling of people or the smuggling of illicit goods involve numerous border crossings. Information stored in the VIS is an important source of information for criminal investigations against third-country nationals who are involved in criminal activity, as indicated by the increasing use of the VIS for law enforcement purposes as well as by the effectiveness and usefulness of the system.[14] However, such information is currently not available for visa-exempt third-country nationals.

Providing for consultation of data stored in the ETIAS Central System for the prevention, detection or investigation of terrorist offences or other serious criminal offences thus addresses an information gap concerning visa-exempt third-country nationals and allows, where necessary, to link with information stored in an ETIAS application file. Moreover, as a travel authorisation will generally be valid for a period of five years, consultation by national law enforcement authorities or Europol of data stored in the ETIAS Central System might be necessary when information related

---

[12] "Criminals capitalise on new opportunities to generate profit, especially when they are able to rely on existing infrastructures, personnel and contacts. This is particularly true for the groups involved in the transportation and distribution of illicit commodities. The ease of international travel and transport, the global emergence of the internet and other technological advances have made geographic considerations less relevant. Criminals act undeterred by geographic boundaries and the most significant groups are now global in terms of their range of activities, operating areas, levels of cooperation and nationality of membership.": Europol's EU Organised Crime Threat Assessment 2013 (OCTA 2013), p. 37.

[13] "Analysis of the nationality of criminals and the countries of main activities has demonstrated that criminal groups are becoming increasingly international. For example, both Belgium and Portugal reported criminal groups consisting of more than 60 nationalities of criminals. These two countries also reported criminal groups whose main criminal activities extend to more than 35 countries. This clearly indicates a significant level of international criminal cooperation, mobility and reach.": idem, p. 34.

[14] See Commission Staff Working Document accompanying the Report on the implementation of Regulation (EC) No 767/2008, SWD(2016) 328 final.

to a person and an act of terrorism or other serious crimes becomes available after that person was granted a travel authorisation.

Consultation of the ETIAS Central System for the prevention, detection or investigation of terrorist offences or other serious criminal offences constitutes a limitation of the right to the protection of personal data. The proposal provides for effective safeguards to mitigate this limitation:

– Clear scope of discretion conferred on the competent authorities and the manner of its exercise: Consultation of data stored in the ETIAS Central System for law enforcement purposes may only be granted for the prevention, detection or investigation of criminal offences or other serious criminal offences as defined in Council Framework Decisions 2002/475/JHA on combatting terrorism and 2002/584/JHA on the European arrest warrant, and only if it is necessary for a specific case. This excludes both the access to ETIAS for crimes that are not serious and a systematic or mass comparison of data.

– Reasoned justification of requests for access for law enforcement purposes: Designated national law enforcement authorities and Europol may only request consultation of data stored in the ETIAS Central System if there are reasonable grounds to consider that such access will substantially contribute to the prevention, detection or investigation of the criminal offence in question.

– Independent verification prior to the consultation of data: Requests for consultation of data stored in the ETIAS Central System in a specific case of prevention, detection or investigation of terrorist offences or other serious criminal offences are subject to an independent verification of whether the strict conditions for requesting consultation of data stored in the ETIAS Central System for law enforcement purposes are fulfilled. Such independent verification is to be conducted a prior by a court or by an authority providing guarantees of full independence and impartiality, and which is free from any direct or indirect external influence.

– Data minimisation to limit the extent of processing to the minimum necessary in relation to its purposes: Not all data stored in an ETIAS application file will be available for the prevention, detection or investigation of terrorist offences or other serious criminal offences. Some data elements will not be available at all given their limited relevance for criminal investigations (e.g. information regarding a person's education or whether or not he or she may pose a public health risk). Other data elements will only be available if the necessity of consulting such specific data element is explicitly justified in the reasoned request for law enforcement consultation and confirmed by independent verification (e.g. data concerning the current occupation).

– Consultation of data stored in the ETIAS Central System as measure of last resort: National law enforcement authorities and Europol can only request consultation of data stored in the ETIAS Central System if prior searches in all relevant national databases of the Member State and Europol databases did not lead to the requested information.

4. BUDGETARY IMPLICATIONS

Following the feasibility study, the current proposal is based on the preferred option for the ETIAS system and the amount needed has been assessed as € 212,1 million which takes also into account the purpose of law enforcement access.

This financial support will cover not only the costs of central components for the entire MFF period (€ 113,4 million – at EU level, both development and operational cost via indirect management) but

also the costs for the integration of the existing national border infrastructures in Member States with the ETIAS via the National Uniform Interfaces (NUI) (€ 92,3 million - via shared management). Providing financial support for national integration costs will ensure that difficult economic circumstances at national level do not jeopardise or delay the projects. During the development phase (2018-2020) the Commission will spend a total amount of € 4,2 million (via shared management) for the expenses related to the operations in the Member States.

From 2020, when the new system will be operational, future operational costs in the Member States could be supported by their national programmes in the framework of the ISF (shared management). However, the operation will start after the end of the current MFF and their funding should consequently be considered during the discussions concerning the next Multiannual Financial Framework.

Both eu-LISA and the European Border and Coast Guard will require additional human and financial resources to carry out their new tasks under the ETIAS Regulation. For eu-LISA, the development phase will start as of 2018, while European Border and Coast Guard will need to be equipped to handle the operational phase, which requires a phasing in of resources starting in the second half of 2020.

As set out in Section 1 above, from 2020 the ETIAS System will generate fee revenue, which in view of its specific character is proposed to be treated as external assigned revenue. Based on the current estimates of the number of applications, the fee revenue will more than cover the direct development and running cost of the ETIAS. In turn, this will allow the financing of related expenditure in the field of Smart Borders.

5. ADDITIONAL INFORMATION

Participation

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

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

Given that this Regulation builds upon the Schengen acquis, Denmark shall, in accordance with Article 4 of that Protocol decide within a period of six months after the Council has decided on this Regulation whether it will implement it in its national law.

United Kingdom and Ireland: In accordance with Articles 4 and 5 of the Protocol integrating the Schengen acquis into the framework of the European Union and Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland, and Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen acquis, the United Kingdom and Ireland do not take part in Regulation (EU) 2016/399 (Schengen Borders Code) nor in any other of the legal instruments which are commonly known as the "Schengen acquis", viz. the legal instruments organising and supporting the abolition of controls at internal borders and the flanking measures regarding the controls at external borders.

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

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

Iceland and Norway: The procedures laid down in the Association Agreement concluded by the Council and the Republic of Iceland and the Kingdom of Norway concerning the latter's association with the implementation, application and development of the Schengen acquis are applicable, since the present proposal builds on the Schengen acquis as defined in Annex A of this Agreement.[15]

Switzerland: This Regulation constitutes a development of the provisions of the Schengen acquis, as provided for by the Agreement between the European Union, the European Community and the Swiss Confederation on the latter's association with the implementation, application and development of the Schengen acquis.[16]

Liechtenstein: This Regulation constitutes a development of the provisions of the Schengen acquis, as provided for by the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis.[17]

Croatia, Cyprus, Bulgaria and Romania: This Regulation establishing the ETIAS builds on the conditions of entry as described in Article 6 of Regulation (EU) 2016/399. This provision was to be applied by the acceding Member States upon accession to the European Union.

[15] OJ L 176, 10.7.1999, p. 36.
[16] OJ L 53, 27.2.2008, p. 52.
[17] OJ L 160, 18.6.2011, p. 19.

2016/0357 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty of the Functioning of the European Union, and in particular, Article 77(2)(b) and (d), Article 87(2)(a) and Article 88(2)(a) thereof,

Having regard to the proposal from the European Commission,

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

After consulting the European Data Protection Supervisor,

Having regard to the opinion of the European Economic and Social Committee[18],

Having regard to the opinion of the Committee of the Regions[19],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The Communication of the Commission of 6 April 2016 entitled 'Stronger and Smarter Information Systems for Borders and Security'[20] outlined the need for the EU to strengthen and improve its IT systems, data architecture and information exchange in the area of border management, law enforcement and counter-terrorism. It emphasises the need to improve the interoperability of information systems. Importantly, it sets out possible options for maximising the benefits of existing information systems and, if necessary, developing new and complementary ones to address still existing information gaps**.**

(2) Indeed, the Communication of 6 April 2016 identified a series of information gaps. Amongst them the fact that border authorities at external Schengen borders have no information on travellers exempt from the requirement of being in possession of a visa when crossing the external borders. The Communication of 6 April 2016 announced that the Commission would launch a study on the feasibility of establishing a European Travel Information and Authorisation System (ETIAS). Such an automated system would determine the eligibility

[18] OJ C , , p. .
[19] OJ C , , p. .
[20] COM(2016) 205 final.

of visa-exempt third country nationals prior to their travel to the Schengen Area, and whether such travel poses a security or irregular migration 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'[21] confirms the priority of securing external borders and presents concrete initiatives to accelerate and broaden the EU response in continuing to strengthen the management of external borders.

(4) It is necessary to specify the objectives of the European Travel Information and Authorisation System (ETIAS), to define its technical architecture, to set up the ETIAS Central Unit, the ETIAS National Units and the ETIAS Screening Board, to lay down rules concerning the operation and the use of the data to be entered into the system by the applicant, to establish rules on the issuing or refusal of the travel authorisations, to lay down the purposes for which the data are to be processed, to identify the authorities authorised to access the data and to ensure protection of personal data.

(5) The ETIAS should apply to third country nationals who are exempt from the requirement of being in possession of a visa when crossing the external borders.

(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[22] applies or of a national of a third country enjoying the right of free movement under Union law and who do not hold a residence card referred to under Directive 2004/38/EC. Article 21(1) of the Treaty on the Functioning of the European Union stipulates that every citizen of the Union shall have the right to move and reside freely within the territory of the Member States, subject to the limitations and conditions laid down in the Treaties and by the measures adopted to give them effect. The respective limitations and conditions are to be found in Directive 2004/38/EC on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States.

(7) As confirmed by the Court of Justice of the European Union[23], such family members have the right to enter the territory of the Member State and to obtain an entry visa for that purpose. Consequently, also family members exempted from the visa obligation should have the right to obtain a travel authorisation. Member States should grant such persons every facility to obtain the necessary travel authorisation which must be issued free of charge.

(8) The right to obtain a travel authorisation is not unconditional as it can be denied to those family members who represent a risk to public policy, public security or public health pursuant to Directive 2004/38/EC. Against this background, family members can be required to provide their personal data related to their identification and their status only insofar these are relevant for assessment of the security threat they could represent. Similarly, examination of their travel authorisation applications should be made exclusively against the security concerns, and not those related to migration risks.

---

21 COM(2016) 602 final.

22 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.

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

(9) The ETIAS should establish a travel authorisation for third country nationals exempt from the requirement to be in possession of a visa when crossing the external borders ('the visa requirement') enabling to determine whether their presence in the territory of the Member States does not pose an irregular migration, security or public health risk. Holding a valid travel authorisation should be a new entry condition for the territory of the Member States, however mere possession of a travel authorisation should not confer an automatic right of entry.

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

(11) ETIAS should contribute to the facilitation of border checks performed by border guards at the external borders crossing points and ensure a coordinated and harmonised assessment of third country nationals subject to the travel authorisation requirement intending at visiting the Schengen area. In addition it should enable to better inform applicants of their eligibility to visit the Schengen area. Moreover, the ETIAS should also contribute to the facilitation of border checks by reducing the number of refusals of entry at the external borders.

(12) The ETIAS should also support the objectives of the Schengen Information System (SIS) related to the alerts in respect of persons wanted for arrest or for surrender or extradition purposes, on missing persons, on persons sought to assist with a judicial procedure and on persons for discreet checks or specific checks. For this purpose the ETIAS should carry out an automated processing of the application files against the relevant alerts in the SIS. This processing will be carried for the purpose of supporting the SIS. Accordingly, any hit resulting from this comparison should be stored in the SIS.

(13) The ETIAS should consist of a large-scale information system, the ETIAS Information System, a central team, the ETIAS Central Unit and national teams, the ETIAS National Units.

(14) The ETIAS Central Unit should be part of the European Border and Coast Guard Agency. The ETIAS Central Unit should be responsible for verifying travel authorisations' applications rejected from the automated process in order to determine whether the applicant personal data corresponds to the personal data of the person having triggered a hit, for the screening rules, and for carrying out regular audits on the processing of applications. The ETIAS Central Unit should work in 24/7 regime.

(15) Each Member State should establish an ETIAS National Unit mainly responsible for the examination and decision on whether to issue or refuse a travel authorisation. The ETIAS National Units should cooperate among themselves and with Europol for the purpose of the assessment of the applications. The ETIAS National Unit should work in 24/7 regime.

(16) To meet its objectives, the ETIAS should provide an online application form that the applicant should fill in with declarations relating to his or her identity, travel document, residence information, contact details, education and current occupation, his or her condition of family member to EU citizens or third country nationals benefiting from free movement not holding a residence card, if the applicant is minor, identity of the responsible person and answers to a set of background questions (whether or not the applicant is subject to any disease with epidemic potential as defined by the International Health Regulations of the World Health Organisation or other infectious or contagious parasitic diseases, criminal records, presence in war zones, decision to return to borders/orders to leave territory).

Access to the applicants' health data should only be allowed to determine whether they represent a threat to public health.

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

(18) In order to finalise the application, all applicants above the age of 18 should be required to pay a fee. The payment should be managed by a bank or a financial intermediary. Data required for securing the electronic payment should only be provided to the bank or financial intermediary operating the financial transaction and are not part of the ETIAS data.

(19) Most of the travel authorisations should be issued within minutes, however a reduced number could take up to 72 hours. For exceptional cases, where a request for additional information or documentation is notified to the applicant, the procedure could last up to two weeks.

(20) The personal data provided by the applicant should be processed by the ETIAS for the sole purposes of verifying in advance the eligibility criteria laid down in Regulation (EU) 2016/399[24] and assessing whether the applicant is likely to irregularly migrate, whether the entry of the applicant in the Union could pose a threat to security or to public health in the Union.

(21) The assessement of such risks cannot be carried out without processing the personal data listed in recital (16). Each item of personal data in the applications should be compared with the data present in a record, file or alert registered in an information system (the Schengen Information System (SIS), the Visa Information System (VIS), the Europol data, the Interpol Stolen and Lost Travel Document database (SLTD), the Entry/Exit System (EES), the Eurodac, the European Criminal Records Information System (ECRIS) and/or the Interpol Travel Documents Associated with Notices database (Interpol TDAWN)) or against the ETIAS watchlists, or against specific risk indicators. The categories of personal data that should be used for comparison should be limited to the categories of data present in the queried information systems, the ETIAS watchlist or the specific risk indicators.

(22) The comparison should take place by automated means. Whenever such comparison reveals that a correspondence (a 'hit') exists with any of the personal data or combination thereof in the applications and a record, file or alert in the above information systems, or with personal data in the ETIAS watchlist, or with risk indicators, the application should be processed manually by an operator in the ETIAS National Unit of the Member State of declared first entry. The assessment performed by the ETIAS National Unit should lead to the decision to issue or not the travel authorisation.

(23) The automated processing may result in the issuing of authorisation. It is expected that the vast majority of applications will obtain a positive answer by automated means. No denial of a travel authorisation should be based only on the automated processing of personal data in the applications. For this reason, the applications for which a hit was generated should be assessed manually by an operator in an ETIAS National Unit.

---

[24] 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).

(24) Applicants who have been refused a travel authorisation should have the right to appeal. Appeals should be conducted in the Member State that has taken the decision on the application and in accordance with the national law of that Member State.

(25) The screening rules should be used to analyse the application file by enabling a comparison between the data recorded in an application file of the ETIAS Central System and specific risk indicators corresponding to previously identified security, irregular migration or public health risk. The criteria used for defining the specific risk indicators should in no circumstances be based on a applicant's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, sexual life or sexual orientation.

(26) An ETIAS watchlist should be established for identifying connections between data in an ETIAS application file and information related to persons who are suspected of having committed an act of serious crime or terrorism, or regarding whom there are factual indications or reasonable grounds to believe that they will commit an act of serious crime or terrorism. The ETIAS watchlist should be part of the data processed by Europol in accordance with Article 18(2)(a) of Regulation (EU) 2016/794 and Europol's Integrated Data Management Concept implementing that Regulation. When providing information to Europol, Member States should be able to determine the purpose or purposes for which it is to be processed, including the possibility to limit this processing to the ETIAS watchlist.

(27) The continuous emergence of new forms of security threats, new patterns of irregular migration and public health threats requires effective responses and needs to be countered with modern means. Since these means entail the processing of important amounts of personal data, appropriate safeguards should be introduced to keep the interference with the right to protection of private life and to the right of protection of personal data limited to what is necessary in a democratic society.

(28) Personal data in ETIAS should therefore be kept secure; access to it should be limited to strictly authorised personnel and in no circumstance it should be used to reach decisions based on any form of discrimination. The personal data stored should be kept securely in eu-LISA's facilities in the Union.

(29) Issued travel authorisations should be annulled or revoked as soon as it becomes evident that the conditions for issuing it were not or are no longer met. In particular, when a new SIS alert is created for a refusal of entry or for a reported lost or stolen travel document, the SIS should inform the ETIAS which should verify whether this new alert corresponds to a valid travel authorisation. In such a case, the ETIAS National Unit of the Member State having created the alert should be immediately informed and revoke the travel authorisation. Following a similar approach, new elements introduced in the ETIAS watchlist shall be compared with the application files stored in the ETIAS in order to verify whether this new element corresponds to a valid travel authorisation. In such a case, the ETIAS National Unit of the Member State of first entry should assess the hit and, where necessary, revoke the travel authorisation. A possibility to revoke the travel authorisation at the request of the applicant should also be provided.

(30) When, in exceptional cirmcumstances, a Member State considers necessary to allow a third country national to travel to its territory on humanitarian grounds, for reasons of national interest or because of international obligations, it should have the possibility to issue a travel authorisation with limited territorial and temporal validity.

(31) Prior to boarding, air and sea carriers, as well as carriers transporting groups overland by coach should have the obligation to verify if travellers have all the travel documents

required for entering the territory of the Member States pursuant to the Schengen Convention[25]. This should include verifying that travellers are in possession of a valid travel authorisation. The ETIAS file itself should not be accessible to carriers. A secure internet access, including the possibility using mobile technical solutions, should allow carriers to proceed with this consultation using travel document data.

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

(33) In the fight against terrorist offences and other serious criminal offences and given the globalisation of criminal networks, it is imperative that law enforcement authorities have the necessary information to perform their tasks effectively. Access to data contained in the Visa Information System (VIS) for law enforcement purpose has already proven effective in helping investigators to make substantial progress in cases related to human being trafficking, terrorism or drug trafficking. The Visa Information System does not contain data on visa-exempt third-country nationals.

(34) Access to the information contained in ETIAS is necessary to prevent, detect and investigate terrorist offences as referred to in Council Framework Decision 2002/475/JHA[26] or other serious criminal offences as referred to in Council Framework Decision 2002/584/JHA[27]. In a specific investigation and in order to establish evidence and information related to a person suspected of having committed a crime or a victim of a crime, law enforcement authorities may need access to the data generated by ETIAS. The data stored in ETIAS may also be necessary to identify the perpetrator of a terrorist offence or other serious criminal offences, especially when urgent action is needed. Access to the ETIAS for the purpose of preventing, detecting or investigating terrorist offences or other serious criminal offences constitutes an interference with the fundamental rights to respect for the private life of individuals and to protection of personal data of persons whose personal data are processed in the ETIAS. Therefore, the data in ETIAS should be retained and made available to the designated authorities of the Member States and the European Police Office ('Europol'), subject to the strict conditions set out in this Regulation in order for such access to be limited to what is strictly necessary for the prevention, detection and investigation of terrorist offences and serious criminal offences in accordance with the requirements notably laid down in the jurisprudence of the Court, in particular in the Digital Rights Ireland case[28].

---

[25] 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.

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

[27] 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).

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

(35) In particular, access to ETIAS data for the purpose of preventing, detecting or investigating terrorist offences or other serious criminal offences should only be granted following a reasoned request by the competent authorities giving reasons for its necessity. Member States should ensure that any such request for access to data stored in ETIAS be the subject of a prior review by a court or by an authority providing guarantees of full independence and impartiality, and which is free from any direct or indirect external influence. However, in situations of extreme urgency, it can be crucial for the competent authorities to obtain immediately personal data necessary for preventing the commission of a serious crime or so that its perpetrators can be prosecuted. In such cases it should be accepted that the review of the personal data obtained from ETIAS takes place as swiftly as possible after access to such data has been granted to the competent authorities.

(36) It is therefore necessary to designate the competent authorities of the Member States that are authorised to request such access for the specific purposes for the prevention, detection or investigation of terrorist offences or of other serious criminal offences.

(37) The ETIAS National Units should act as the central access point and should verify that the conditions to request access to the ETIAS Central System are fulfilled in the concrete case at hand.

(38) Europol is the hub for information exchange in the Union and it plays a key role with respect to cooperation between Member States' authorities in the field of cross-border crime investigation in supporting Union-wide crime prevention, analyses and investigation. Consequently, Europol should also have access to the ETIAS Central System within the framework of its tasks and in accordance with Regulation (EU) 2016/794[29] in specific cases where this is necessary for Europol to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences.

(39) To exclude systematic searches, the processing of data stored in the ETIAS Central System should take place only in specific cases and only when it is necessary for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences. The designated authorities and Europol should only request access to ETIAS when they have reasonable grounds to believe that such access will provide information that will substantially assist them in preventing, detecting or investigating a terrorist offence or other serious criminal offence. The law enforcement authorities and Europol should only request access to the ETIAS if prior searches in all relevant national databases of the Member State and databases at Europol did not lead to the requested information.

(40) The personal data recorded in the ETIAS should be kept for no longer than is necessary for its purposes. In order for the ETIAS to function, it is necessary to keep the data related to applicants for the period of validity of the travel authorisation. In order to assess the security, irregular migration and public health risks posed by the applicants it is necessary to keep the personal data for five years from the last entry record of the applicant stored in the EES. In fact, the ETIAS should rely on accurate preliminary assessments of the security, public health and irregular migration risks, notably through the use of the screening rules. In order to constitute a reliable basis for the manual risk assessment by the Member States, and reduce to the minimum the occurrence of hits not corresponding to real risks ('false positives'), the hits resulting from screening rules based on statistics generated by ETIAS data itself need to be representative of a sufficiently broad population. This cannot be

[29] OJ L 119, 4.5.2016, p. 132-149.

achieved exclusively on the basis of the data of the travel authorisations in their validity period. The retention period should start from the last entry record of the applicant stored in the EES, since that constitutes the last actual use of the travel authorisation. A retention period of five years corresponds to the retention period of an EES record with an entry authorisation granted on the basis of an ETIAS travel authorisation or a refusal of entry. This synchronisation of retention periods ensures that both the entry record and the related travel authorisation are kept for the same duration and is an additional element ensuring the future interoperability between ETIAS and EES. This synchronisation of data retention periods is necessary to allow the competent authorities to perform the risk analysis requested by the Schengen Borders Code. A decision to refuse, revoke or annul a travel authorisation could indicate a higher security or irregular migration risk posed by the applicant. Where such a decision has been issued, the 5 years retention period for the related data should start from its date of issuance, in order for ETIAS to be able to take accurately into account the higher risk possibly posed by the applicant concerned. After the expiry of such period, the personal data should be deleted.

(41) Precise rules should be laid down as regards the responsibilities of the Agency for the operational management of large-scale information systems in the area of freedom, security and justice (eu-LISA) for the designing, development and technical management of the ETIAS Information System, the responsabilities of the European Coast and Border Guard Agency, the responsibilities of the Member States and the responsabilities of Europol.

(42) Regulation (EC) No 45/2001 of the European Parliament and the Council[30] applies to the activities of eu-LISA and the European Coast and Border Guard Agency when carrying out the tasks entrusted to them in this Regulation.

(43) [Regulation (EU) 2016/679][31] applies to the processing of personal data by the Member States in application of this Regulation unless such processing is carried out by the designated or verifying authorities of the Member States for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences.

(44) The processing of personal data by the authorities of the Member States for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences pursuant to this Regulation should be subject to a standard of protection of personal data under their national law which complies with [Directive (EU) 2016/680][32].

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

---

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

31 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).

32 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.

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

(47) Strict access rules to the ETIAS Central System and the necessary safeguards should be established. It is also necessary to provide for individuals' rights of access, correction, deletion and redress, in particular the right to a judicial remedy and the supervision of processing operations by public independent authorities.

(48) In order to assess the security, irregular migration or public health risk which could be posed by a traveller, interoperability between the ETIAS Information System and other information systems consulted by ETIAS such as the Entry/Exit System (EES), the Visa Information System (VIS), the Europol data, the Schengen Information System (SIS), the Eurodac and the European Criminal Records Information System (ECRIS) should have to be established. However this interoperability can only be fully ensured once the proposals to establish the EES[33], the ECRIS[34] and the recast proposal of the Eurodac Regulation[35] have been adopted.

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

(50) In order to establish the technical measures needed for the application of this Regulation, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission:

- to adopt a predetermined list of answers concerning the questions on the level and field of education, the current occupation and the job title to be indicated in the application for a travel authorisation,
- to specify the content and format of the additional questions which can be put to an applicant for a travel authorisation,
- to lay down the payment methods and process for the travel authorisation fee taking into account the technological developments and their availability and to amend the amount of the fee,
- to extend the duration of the period of grace during which no travel authorisations is required,

---

[33] Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) COM(2016) 194 final.

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

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

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

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

(52) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to adopt detailed rules on the conditions for operation of the public website and the mobile app for mobile devices and on the data protection and security rules applicable to the public website and the mobile app for mobile devices, as well as an authentication scheme reserved exclusively to carriers and to specify the details of the fall back procedures to be followed in the case of technical impossibility to access ETIAS. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[36].

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

(54) The projected costs for the development of the ETIAS Information System and for the establishment of the ETIAS Central Unit and the ETIAS National Units are lower than the remaining amount on the budget earmarked for Smart Borders in Regulation (EU) No 515/2014 of the European Parliament and the Council[37]. Accordingly, this Regulation, pursuant to Article 5(5)(b) of Regulation (EU) No 515/2014, should, re-allocate the amount currently attributed for developing IT systems supporting the management of migration flows across the external borders.

(55) The revenue generated by the payment of travel authorisation fees should be assigned to cover the recurring operational and maintenance costs of the ETIAS Information System, of the ETIAS Central Unit and of the ETIAS National Units. In view of the specific character of the system, it is appropriate to treat the revenue as external assigned revenue.

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

(57) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European

---

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

[37] 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).

Union, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Given that this Regulation builds upon the Schengen *acquis*, Denmark shall, in accordance with Article 4 of that Protocol, decide within a period of six months after the Council has decided on this Regulation whether it will implement it in its national law.

(58) This Regulation constitutes a development of the provisions of the Schengen acquis in which the United Kingdom does not take part, in accordance with Council Decision 2000/365/EC[38]; the United Kingdom is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(59) This Regulation constitutes a development of the provisions of the Schengen *acquis* in which Ireland does not take part, in accordance with Council Decision 2002/192/EC[39]; Ireland is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(60) As regards Iceland and Norway, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latters' association with the implementation, application and development of the Schengen acquis[40] which fall within the area referred to in Article 1, point A of Council Decision 1999/437/EC[41] .

(61) As regards Switzerland, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*[42] which fall within the area referred to in Article 1, point A of Council Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/146/EC[43] and with Article 3 of Council Decision 2008/149/JHA[44].

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

---

38 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).

39 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).

40 OJ L 176, 10.7.1999, p. 36.

41 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).

42 OJ L 53, 27.2.2008, p. 52.

43 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).

44 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).

Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*[45] which fall within the area referred to in Article 1, point A of Council Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU[46] and with Article 3 of Council Decision 2011/349/EU.[47]

(63) This Regulation constitutes an act building upon, or otherwise relating to, the Schengen *acquis* within, respectively, the meaning of Article 3(2) of the 2003 Act of Accession, Article 4(2) of the 2005 Act of Accession and Article 4(2) of the 2011 Act of Accession.

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

---

45 OJ L 160, 18.6.2011, p. 21.

46 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).

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

HAVE ADOPTED THIS REGULATION:

CHAPTER 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 to determine whether their presence in the territory of the Member States does not pose an irregular migration, security or public health risk. For this purpose a travel authorisation and the conditions and procedures to issue or refuse it are introduced.

2. This Regulation lays down the conditions under which Member States' law enforcement authorities and the European Police Office (Europol) may consult data stored in the ETIAS Central System for the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences falling under their competence.

Article 2
Scope

1. This Regulation applies to the following categories of third country nationals exempt from the visa requirement:

   (a) nationals of third countries listed in Annex II to Council Regulation (EC) No 539/2001[48] who are exempt from the visa requirement for airports transits or intended stays in the territory of the Member States of a duration of no more than 90 days in any 180 day period;

   (b) refugees and stateless persons where the third country in which they reside and which issued their travel document is one of the third countries listed in Annex II to Regulation (EC) No 539/2001 and who are exempted from the visa requirement pursuant to Article 4(2)(b) of that Regulation;

   (c) third country nationals who fulfil the following conditions:

      i) they are family members of a Union citizen to whom Directive 2004/38/EC applies or of a national of a third country enjoying the right of free movement under Union law; and

      ii) they do not hold a residence card referred to under Directive 2004/38/EC.

2. This Regulation does not apply to:

[48] OJ L 81, 21.3.2001, p. 1.

(a) refugees or stateless persons or other persons who do not hold the nationality of any country who reside in a Member State and who are holders of a travel document issued by that Member State;

(b) third country nationals who are members of the family of a Union citizen to whom Directive 2004/38/EC applies and who hold a residence card pursuant to that Directive;

(c) third country nationals who are members of the family of nationals of a third country enjoying the right of free movement under Union law and who hold a residence card pursuant to Directive 2004/38/EC;

(d) holders of residence permits referred to in point 16 of Article 2 of Regulation (EU) 2016/399 of the European Parliament and of the Council[49]other than those covered by points (b) and (c) of this paragraph;

(e) holders of long-stay visas;

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

(g) the nationals of third countries listed in Annex I and II to Regulation (EC) No 539/2001 who are holders of a local border traffic permit issued by the Member States pursuant to Regulation (EC) No 1931/2006[50] when these holders exercise their right within the context of the Local Border Traffic regime;

(h) persons or categories of persons referred to in Article 4(1) and (3) of Regulation (EC) No 539/2001.

Article 3
Definitions

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

(a) ‘external borders' mean external borders as defined in Article 2(2) of Regulation (EU) 2016/399;

(b) ‘border checks’ means border checks as defined in Article 2(11) of Regulation (EU) 2016/399;

(c) ‘border guard’ means border guard as defined in Article 2(14) of Regulation (EU) 2016/399;

(d) 'travel authorisation' means a decision issued in accordance with this Regulation indicating that there are no factual indications or reasonable grounds to conclude that the presence of the person on the territory of the Member States poses an irregular migration, security or public health risk and

[49] Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ L 077 23.3.2016, p. 1).
[50] OJ L 405, 20.12.2006, p. 1.

which is a requirement for third country nationals referred to in Article 2 to fulfil the entry condition laid down in Article 6(1)(b) of Regulation (EU) 2016/399.

(e) 'public health risk' means threat to public health as defined in Article 2(21) of Regulation (EU) 2016/399;

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

(g) ‘travel document’ means a passport or other equivalent document, entitling the holder to cross the external borders and to which a visa may be affixed;

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

(i) ‘overstayer’ means a third country national who does not fulfil, or no longer fulfils the conditions relating to the duration of a short stay on the territory of the Member States;

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

(k) 'hit' means the existence of a correspondence established by comparing the personal data recorded in an application file of the ETIAS Central System with the personal data stored in a record, file or alert registered in an information system queried by the ETIAS Central System, in the ETIAS watchlist or with the specific risk indicators referred to in Article 28;

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

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

(n) 'Europol data' means personal data provided to Europol for the purpose referred to in Article 18(2)(a) of Regulation (EU) 2016/794.

2. The definitions set out in Article 2 of Regulation (EC) 45/2001 shall apply in so far as personal data are processed by the European Border and Coast Guard Agency and eu-LISA

3. The definitions set out in Article 4 of [Regulation (EU) 2016/679] shall apply in so far as personal data are processed by the authorities of Member States.

4. The definitions set out in Article 3 of [Directive (EU) 2016/680] shall apply in so far as personal data are processed by the authorities of the Member States for law enforcement purposes.

Article 4
Objectives of the ETIAS

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

(a) contribute to a high level of security by providing for a thorough security risk assessment of applicants, prior to their arrival at the external borders crossing points, in order to determine whether there are factual indications or reasonable grounds to conclude that the presence of the person on the territory of the Member States poses a security risk;

(b) contribute to the prevention of irregular migration by providing for an irregular migration risk assessment of applicants prior to their arrival at the external borders crossing points;

(c) contribute to the protection of public health by providing for an assessment of whether the applicant poses a public health risk within the meaning of Article 3(1)(e) prior to their arrival at the external borders crossing points;

(d) enhance the effectiveness of border checks;

(e) support the objectives of the Schengen Information System (SIS) related to the alerts in respect of persons wanted for arrest or for surrender or extradition purposes, on missing persons, on persons sought to assist with a judicial procedure and on persons for discreet checks or specific checks;

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

Article 5
General structure of ETIAS

The ETIAS consists of:

(a) the ETIAS Information System as referred to in Article 6;

(b) the ETIAS Central Unit as referred to in Article 7;

(c) the ETIAS National Units as referred to in Article 8.

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

1. The Agency for the operational management of large-scale information systems in the area of freedom, security and justice ('eu-LISA') shall develop the ETIAS Information System and ensure its technical management.

2. The ETIAS Information System shall be composed of:

(a) a Central System;

(b) a National Uniform Interface (NUI) in each Member State based on common technical specifications and identical for all Member States enabling the Central System to connect to the national border infrastructures in Member States;

(c) a secure Communication Infrastructure between the Central System and the National Uniform Interfaces;

(d) a secure Communication Infrastructure between the ETIAS Central System and the information systems referred to in Article 10;

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

(f) an email service;

(g) a secure account service enabling applicants to provide additional information and/or documentation, if necessary;

(h) a carrier gateway;

(i) a web service enabling communication between the Central System , on the one hand and the public website, the mobile app, the email service, the secured account service, the carrier gateway, the payment intermediary and the international systems (Interpol systems/databases), on the other hand;

(j) a software enabling the ETIAS Central Unit and the ETIAS National Units to process the applications;

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

Article 7
Set up of the ETIAS Central Unit

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

2. The ETIAS Central Unit working in 24/7 regime shall be in charge of:

(a) ensuring that the data stored in the applications files and in the ETIAS Central System is correct and up to date;

(b) verifying travel authorisations' applications rejected from the automated process in order to determine whether the applicant personal data corresponds to the personal data of the person having triggered a hit in one of the consulted information systems/databases or the specific risk indicators referred to in Article 28;

(c) defining, testing, implementing, evaluating and revising the specific risk indicators as referred to in Article 28 after consultation of the ETIAS Screening Board;

(d) carrying out regular audits on the processing of applications and on the implementation of the provisions of Article 28 including regularly assessing their impact on fundamental rights, in particular with regard to privacy and personal data protection.

Article 8
Set up of the ETIAS National Units

1. Each Member State shall designate a competent authority as the ETIAS National Unit.

2. The ETIAS National Units shall be responsible for:

   (a) ensuring that the data stored in the applications files and in the ETIAS Central System is correct and up to date;

   (b) examining and deciding on travel authorisations' applications rejected by the automated application process, and carrying out the manual risk assessment referred to in Article 22;

   (c) ensuring coordination between ETIAS National Units and Europol concerning the consultation requests referred to in Articles 24 and 25;

   (d) providing applicants with information regarding the procedure to be followed in the event of an appeal in accordance with Article 31(2);

   (e) acting as central access point for the consultation of the ETIAS Central System for the purpose laid down in Article 1(2) and in accordance with Article 44.

3. Member States shall provide the ETIAS National Units with adequate resources for them to fulfil their tasks in 24/7 regime.

Article 9
The ETIAS Screening Board

1. An ETIAS Screening Board with an advisory function is hereby established within the European Border and Coast Guard Agency. It shall be composed of a representative of each ETIAS National Unit and Europol.

2. The ETIAS Screening Board shall be consulted on:

   (a) the definition, evaluation and revision of the specific risk indicators referred to in Article 28;

   (b) the implementation of the ETIAS watchlist referred to in Article 29.

3. For the purpose referred to in paragraph 1, the ETIAS Screening Board shall issue opinions, guidelines, recommendations and best practices.

4. The ETIAS Screening Board shall meet whenever necessary, and at least twice a year. The costs and servicing of its meetings shall be borne by the European Border and Coast Guard Agency.

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

Article 10
Interoperability with other information systems

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

Article 11
Access to data stored in the ETIAS

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

2. Access by border guards to the ETIAS Central System in accordance with Article 41 shall be limited to searching the ETIAS Central System to obtain the travel authorisation status of a traveller present at an external border crossing point.

3. Access by carriers to the ETIAS Central System by in accordance with Article 39, shall be limited to searching the ETIAS Central System to obtain the travel authorisation status of a traveller.

Article 12
Non-discrimination

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

CHAPTER II
Application

Article 13
Practical arrangements for lodging an application

1. Applicants shall lodge an application by filling in the online application form via the dedicated public website or via the mobile app for web devices sufficiently in advance of any intended travel.

2. Applications may be lodged by the applicant or by a person or a commercial intermediary authorised by the applicant to lodge the application in his or her behalf.

Article 14
The public website and mobile app for mobile devices

1. The public website and the mobile app for mobile devices shall enable third country nationals subject to the travel authorisation requirement to launch a travel authorisation

application, to provide the data required in the application form in accordance with Article 15 and to pay the travel authorisation fee.

2. The public website and the mobile app for mobile devices shall make the application form widely available and easily accessible to applicants free of charge.

3. The public website and the mobile app for mobile devices shall be available in all the official languages of the Member States.

4. Where the official language(s) of the countries listed in Annex II of Council Regulation (EC) No 539/2001 do not correspond to the languages referred to in paragraph 3, factsheets with information concerning the content and the use of the public website and the mobile app for mobile devices and explanatory information shall be made available in at least one of the official languages of the countries referred to.

5. The public website and the mobile app for mobile devices shall inform applicants of the languages which may be used when filling in the application form.

6. The public website and the mobile app for mobile devices shall provide the applicant with an account service enabling applicants to provide additional information and/or documentation, where required.

7. The Commission shall adopt detailed rules on the conditions for operation of the public website and the mobile app for mobile devices, and on the data protection and security rules applicable to the public website and the mobile app for mobile devices. Those implementing measures shall be adopted in accordance with the examination procedure referred to in Article 79(2).

Article 15
Application form and personal data of the applicant

1. Each applicant shall submit a completed application form including a declaration of authenticity, completeness and reliability of the data submitted and a declaration of veracity and reliability of the statements made. 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));

(c) other nationalities (if any);

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

(e) 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) e-mail address, phone number;

(h) education (level and field);

(i) current occupation;

(j) Member State of first intended entry;

(k) for minors, surname and first name(s) of the applicant's parental authority or legal guardian;

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

i) their status of family member;

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

iii) their family ties with that family member in accordance with Article 2(2) of Directive 2004/38/EC;

(m) in the case of applications filled in by a person other than the applicant, the surname, first name(s), name of firm, organization if applicable, e-mail address, mailing address, phone number; relationship to the applicant and an electronically signed representative declaration.

3. The applicant shall choose the level and field of education, the current occupation and the job title from a predetermined list. The Commission shall be empowered to adopt delegated acts in accordance with Article 78 to lay down these predetermined lists.

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

(a) whether the applicant is subject to any disease with epidemic potential as defined by the International Health Regulations of the World Health Organisation or other infectious or contagious parasitic diseases;

(b) whether he or she has ever been convicted of any criminal offence in any country;

(c) regarding any stay in a specific war or conflict zone over the last ten years and the reasons for the stay;

(d) regarding any decision requiring him or her to leave the territory of a Member State or of any other country or whether he or she was subject to any return decision issued over the last ten years.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 78 specifying the content and format of those questions.

6. The applicant shall provide answers to those questions. Where the applicant answers affirmatively to any of the questions, he or she shall be required to provide answers to additional questions on the application form aimed at collecting further information via providing answers to a predetermined list of questions. The Commission shall be empowered to adopt delegated acts in accordance with Article 78 to lay down the content

and format of those additional questions and the predetermined list of answers to those questions.

7. The data referred to in paragraphs 2 and 4 shall be introduced by the applicant in Latin alphabet characters without diacritics.

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

Article 16
Travel authorisation fee

1. A travel authorisation fee of EUR 5 shall be paid by the applicant for each application.

2. The travel authorisation fee shall be waived for children under eighteen years.

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

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 78 on the payment methods and process for the travel authorisation fee and on changes to the amount of that fee.

CHAPTER III
Creation of the application file and examination of the application by the ETIAS Central System

Article 17
Admissibility and creation of the application file

1. The ETIAS Central System shall automatically verify whether, following submission of an application:

   (a) all the fields of the application form are filled in and contain all the items referred to in Article 15(2) and (4),

   (b) the travel authorisation fee has been collected.

2. When the application is deemed admissible pursuant to paragraph 1, the ETIAS Central System shall automatically create an application file without delay and assign it an application number.

3. Upon creation of the application file, the ETIAS Central System shall record and store the following data:

   (a) the application number;

   (b) status information, indicating that a travel authorisation has been requested;

   (c) the personal data referred to in Article 15(2) and (4) including the three letter code of the country issuing the travel document;

(d) the data referred to in Article 15(5);

(e) the date and the time the application form was submitted as well as a reference to the successful payment of the travel authorisation fee and the unique reference number of the payment.

4. Upon creation of the application file, the ETIAS Central System shall determine whether the applicant already has another application file in the ETIAS Central System by comparing the data referred to in Article 15(2)(a) with the personal data of the application files stored in the ETIAS Central System. In such a case, the ETIAS Central System shall link the new application file to any previous existing application file created for the same applicant.

Article 18
Automated processing

1. The application files shall be automatically processed by the ETIAS Central System to identify hit(s). The ETIAS Central System shall examine each application file individually.

2. The ETIAS Central System shall compare the relevant data referred to in Article 15(2)(a),(b),(d),(f),(g),(m) and (8) to the data present in a record, file or alert registered in the ETIAS Central System, the Schengen Information System (SIS), [the Entry/Exit System (EES)], the Visa Information System (VIS), [the Eurodac], [the European Criminal Records Information System (ECRIS)], the Europol data, the Interpol Stolen and Lost Travel Document database (SLTD) and the Interpol Travel Documents Associated with Notices database (Interpol TDAWN).

In particular, the ETIAS Central System shall verify:

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

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

(c) whether the applicant is subject to a refusal of entry alert recorded in the SIS;

(d) whether the applicant is subject to an alert in respect of persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant or wanted for arrest for extradition purposes in the SIS;

(e) whether the applicant and the travel document correspond to a refused, revoked or annulled application for travel authorisation in the ETIAS Central System;

(f) whether the data provided in the application concerning the travel document correspond to another application for travel authorisation associated with different identity data in the ETIAS Central System;

(g) [whether the applicant is currently reported as overstayer, whether he has been reported as overstayer in the past through consultation of the EES;]

(h) [whether the applicant was refused entry through consultation of the EES;]

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

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

(k) [whether the applicant was subject to a return decision or a removal order issued following the withdrawal or rejection of the application for internal protection in the Eurodac;]

(l) [whether the applicant corresponds to a person whose data is recorded in the ECRIS;]

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

3. The ETIAS Central System shall verify whether the applicant has replied affirmatively to any of the questions listed in Article 15(4) and whether the applicant has not provided a home address but only his city and country of residence, as referred to in Article 15(2)(f).

4. The ETIAS Central System shall compare the relevant data referred to in Article 15(2)(a), (b), (d), (f), (g), (i), (m) and (8) to the data present in the ETIAS watchlist referred to in Article 29.

5. The ETIAS Central System shall compare the relevant data referred to in Article 15(2)(a), (f), (h) and (i) and the specific risk indicators referred to in Article 28.

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

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

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

(b) an alert in respect of missing persons;

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

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

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

Article 19
Results of the automated processing

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

2. Where the automated processing laid down in Article 18(2) to (5) reports one or several hit(s), the application shall be assessed in accordance with the procedure laid down in Article 22.

3. Where the automated processing laid down in Article 18(2) to (5) is inconclusive because the ETIAS Central System is not in a position to certify that the data recorded in the application file correspond to the data triggering a hit, the application shall be assessed in accordance with the procedure laid down in Article 20.

Article 20
Verification by the ETIAS Central Unit

1. Where the ETIAS Central System is not in a position to certify that the data recorded in the application file corresponds to the data triggering a hit during the automated processing pursuant to Article 18(2) to (5) the ETIAS Central System shall automatically consult the ETIAS Central Unit.

2. Where consulted, the ETIAS Central Unit shall have access to the application file and the linked application file(s), if any, as well as to all the hits triggered during the automated processing pursuant to Article 18(2) to (5).

3. The ETIAS Central Unit shall verify whether the data recorded in the application file corresponds to the data present in one of the consulted information systems/databases, the ETIAS watchlist referred to in Article 29 or the specific risk indicators referred to in Article 28.

4. Where the data do not correspond, and no other hit has been reported during the automated processing pursuant to Article 18(2) to (5), the ETIAS Central Unit shall delete the false hit from the application file and the ETIAS Central System shall automatically issue a travel authorisation in accordance with Article 30.

5. Where the data correspond to or where doubts remain concerning the identity of the applicant, the application shall be assessed in accordance with the procedure laid down in Article 22.

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

Article 21
Specific rules for family members of EU citizens or of other third country nationals enjoying the right of free movement under Union law

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

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

   (a) the applicant shall provide the additional personal data referred to in Article 15(2)(l);

   (b) the applicant shall not reply to the question referred to in Article 15(4)(d);

   (c) the fee referred to in Article 16 shall be waived.

3. [When processing an application for a travel authorisation for a third country national referred to in Article 2(1)(c), the ETIAS Central Systems shall not verify whether:

(a) the applicant is currently reported as overstayer, whether he or she has been reported as overstayer in the past through consultation of the EES as referred to in Article 18(2)(g);

(b) the applicant corresponds to a person whose data is recorded in the Eurodac as referred to in Article 18(2)(j).]

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

4. An application for a travel authorisation shall not be refused on the ground of an irregular migration risk as referred to in Article 31(1)(b).

5. The following rules shall also apply:

(a) in the notification laid down in Article 32(1) the applicant shall receive information regarding the fact that he or she needs to be able to prove when crossing the external border his or her status as family member of a citizen exercising the right of free movement as referred to in Article 15(2)(l), which shall also include a reminder that the family member of a citizen exercising the right of free movement who is in possession of a travel authorisation only has a right to enter if the family member accompanies or joins the citizen exercising its right of free movement;

(b) an appeal as referred to in Article 32 shall be made in accordance with Directive 2004/38/EC;

(c) the retention period of the application file referred to in Article 47(1) shall be:

i) the period of validity of the travel authorisation;

ii) [one year from the last entry record of the applicant stored in the EES, where that period of one year ends on a later date than the period of validity of the travel authorisation; or]

iii) five years from the last decision to refuse, revoke or annul the travel authorisation in accordance with Articles 31, 34 and 35.

CHAPTER IV
Examination of the application by the ETIAS National Units

Article 22
Manual processing of applications by the ETIAS National Units

1. The Member State responsible for the manual processing of applications pursuant to this Article (the 'responsible Member State') shall be the Member State of first entry as declared by the applicant in accordance with Article 15(2)(j).

2. Where the automated processing laid down in Article 18(2) to (5) reported one or several hit(s), the application shall be processed manually by the ETIAS National Unit of the responsible Member State. The ETIAS National Unit shall have access to the application file and the linked application file(s), if any, as well as to all the hits triggered during the automated processing laid down in Article 18(2) to (5).

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

   (a) issue a travel authorisation; or

   (b) refuse a travel authorisation.

4. Where the automated processing laid down in Article 18(2) has reported a hit, the ETIAS National Unit of the responsible Member State shall:

   (a) where the hit corresponds to one or several of the categories laid down in Article 18(2)(a) to (c), refuse a travel authorisation.

   (b) where the hit corresponds to one or several of the categories laid down in Article 18(2)(d) to (m), assess the security or irregular migration risk and decide whether to issue or refuse a travel authorisation.

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

6. Where the automated processing laid down in Article 18(4) has reported a hit, the ETIAS National Unit of the responsible Member State shall assess the security risk and decide whether to issue or refuse a travel authorisation.

7. Where the automated processing laid down in Article 18(5) has reported a hit, the ETIAS National Unit of the responsible Member State shall assess the irregular migration, security or public health risk and decide whether to issue or refuse a travel authorisation.

Article 23
Request for additional information or documentation from the applicant

1. Where the information provided by the applicant in the application form does not allow the ETIAS National Unit of the responsible Member State to decide whether to issue or refuse a travel authorisation, that ETIAS National Unit may request the applicant for additional information or documentation.

2. The request for additional information or documentation shall be notified to the contact e-mail address recorded in the application file. The request for additional information or documentation shall clearly indicate the information or documentation that the applicant is required provide. The applicant shall provide the additional information or documentation directly to the ETIAS National Unit through the secure account service referred to in Article 6(2)(g) within 7 working days of the date of receipt of the request.

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

4. In exceptional circumstances, the ETIAS National Unit may invite the applicant for an interview at a consulate in his or her country of residence.

5. The invitation shall be notified to the applicant by the ETIAS National Unit of the Member and shall be notified to the contact e-mail address recorded in the application file.

6. Where the applicant fails to reply to the invitation within the deadline or where the applicant fails to attend the interview, the application shall be refused in accordance with Article 31(1) and the ETIAS National Unit of the responsible Member State shall inform the applicant without delay.

7. The ETIAS National Unit shall resume the examination of the application from the moment the applicant provides the additional information or documentation.

Article 24
Consultation of other Member States

1. For the purpose of carrying out the assessment referred to in Article 22(4)(b) the ETIAS National Unit of the responsible Member State shall consult the authorities of the Member State(s) responsible for the data having triggered a hit pursuant to Article 18(2)(d),(e),(g),(h),(i) or (k).

2. For the purpose of carrying out the assessment referred to in Article 22(4)(b), (6) and (7) the ETIAS National Unit of the responsible Member State may consult the authorities of one or several Member States.

3. Where the responsible Member State consults with one or several Member States during the manual processing of an application, the ETIAS National Units of those Member States shall have access to the relevant data of the application file as well as to the hits obtained by the automated system pursuant to Article 18 (2), (4) and (5) which are necessary for the purpose the consultation. The ETIAS National Units of the Member States consulted shall also have access to the relevant additional information or documentation provided by the applicant following a request from the responsible Member State in relation to the matter for which they are being consulted.

4. The ETIAS National Unit of the Member States consulted shall:

   (a) provide a reasoned positive opinion on the application; or

   (b) provide a reasoned negative opinion on the application.

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

5. The ETIAS National Unit of the Member States consulted shall reply within 24 hours from the date of the notification of the consultation. The failure by Member States to reply within the deadline shall be considered as a positive opinion on the application.

6. Where several Member States are consulted, the ETIAS National Unit of the responsible Member State shall ensure the coordination.

7. During this consultation process, the consultation request and the replies thereto shall be transmitted through the ETIAS Communication Infrastructure.

8. Where one or several Member States consulted provide a negative opinion on the application, the responsible Member State shall refuse the travel authorisation pursuant to Article 31.

Article 25
Consultation of Europol

1. For the purpose of carrying out the assessment of security risks following a hit pursuant to Article 18(2)(j) and (4), the ETIAS National Unit of the responsible Member State shall consult Europol in cases falling under Europol's mandate. The consultation shall take place through existing communication channels between the Member State and Europol as established under Article 7 of Regulation (EU) 2016/794.

2. Where the responsible Member State consults Europol, the ETIAS National Unit of that Member State shall transmit to Europol the relevant data of the application file as well as the hit(s) which are necessary for the purpose of the consultation. The ETIAS National Unit may transmit to Europol the relevant additional information or documentation provided by the applicant in relation to the request for travel authorisation for which Europol is consulted.

3. In any case, Europol shall not have access to the personal data concerning the education of the applicant as referred to in Article 15(2)(h) and the health of the applicant as referred to in Article 15(4)(a).

4. Where consulted in accordance with paragraph 1, Europol shall provide a reasoned opinion on the application. Europol's opinion shall be recorded in the application file by the responsible Member State.

5. Europol shall reply within 24 hours of the date of the notification of the consultation. The failure by Europol to reply within the deadline shall be considered as a positive opinion on the application.

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

Article 26
Deadlines for notification to the applicant

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

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

(b) if additional information or documentation is requested.

Article 27
Decision on the application

1. Applications shall be decided on no later than 72 hours after the lodging of an application which is admissible in accordance with Article 17.

2. Exceptionally, when a request for additional information or documentation is notified, the period laid down in paragraph 1 shall be extended in accordance with Article 23. Such application shall in all cases be decided on no later than 72 hours after the submission of the additional information or documentation by the applicant .

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

(a) issue a travel authorisation in accordance with Article 30; or

(b) refuse a travel authorisation in accordance with Article 31;

CHAPTER V
The ETIAS screening rules and the ETIAS watchlist

Article 28
The ETIAS screening rules

1. The ETIAS screening rules shall be an algorithm enabling the comparison between the data recorded in an application file of the ETIAS Central System and specific risk indicators pointing to irregular migration, security or public health risks. The ETIAS screening rules shall be registered in the ETIAS Central System.

2. The irregular migration, security or public health risks shall be determined on the basis of:

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

(b) statistics generated by the ETIAS in accordance with Article 73 indicating abnormal rates of refusals of travel authorisations due to an irregular migration, security or public health risk associated with a specific group of travellers;

(c) [statistics generated by the ETIAS in accordance with Article 73 and the EES indicating correlations between information collected through the application form and overstay or refusals of entry;]

(d) information provided by Member States concerning specific security risk indicators or threats identified by that Member State;

(e) information provided by Member States concerning abnormal rates of overstayers and refusals of entry for a specific group of travellers for that Member State;

(f) information concerning specific public health risks provided by Member States as well as epidemiological surveillance information and risk assessments provided by the European Centre for Disease Prevention and Control (ECDC).

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

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

(a) age range, sex, current nationality;

(b) country and city of residence;

(c) education level;

(d) current occupation.

5. The specific risk indicators shall be targeted and proportionate. They shall in no circumstances be based on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, sexual life or sexual orientation.

6. The specific risk indicators shall be defined, modified, added and deleted by the ETIAS Central Unit after consultation of the ETIAS Screening Board.

Article 29
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 criminal offence or persons regarding whom there are factual indications or reasonable grounds to believe that they will commit criminal offences.

2. The ETIAS watchlist shall be established on the basis of:

(a) the United Nations list of war criminals;

(b) information related to terrorist offences or other serious criminal offences provided by Member States;

(c) information related to terrorist offences or other serious criminal offences obtained through international cooperation.

3. On the basis of the information referred to in paragraph 2 and relevant Europol data, Europol shall establish the ETIAS watchlist composed of items consisting of one or more of the following data elements:

(a) surname, first name(s), surname at birth; date of birth, place of birth, country of birth, sex, nationality;

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

(c) a travel document (type, number and country of issuance of the travel document);

(d) home address;

(e) e-mail address, phone number;

(f) the name, e-mail address, mailing address, phone number of a firm or organization;

(g) IP address.

CHAPTER VI
Issuing, refusal, annulment or revocation of a travel authorisation

Article 30
Issuing of a travel authorisation

1. Where the examination of an application pursuant to the procedures laid down in Chapters III, IV and V indicates that there are no factual indications or reasonable grounds to conclude that the presence of the person on the territory of the Member States poses an irregular migration, security or public health risk, a travel authorisation shall be issued by the ETIAS Central System or the ETIAS National Unit of the responsible Member State.

2. A travel authorisation shall be valid for five years or until the end of validity of the travel document registered during application, whichever comes first, and shall be valid for the territory of the Member States.

3. A travel authorisation shall not confer an automatic right of entry.

Article 31
Refusal of a travel authorisation

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

   (a) presents a travel document which is reported as lost, stolen or invalidated;

   (b) poses an irregular migration risk;

   (c) poses a security risk;

   (d) poses a public health risk;

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

   (f) fails to reply to a request for additional information or documentation within the deadlines referred to in Article 23.

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

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

Article 32

Notification on the issuing or refusal of a travel authorisation

1. Where a travel authorisation has been issued, the applicant shall immediately receive a notification via the e-mail service, including:

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

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

   (c) where applicable, a reminder of the calculation of the duration of authorised short stay (90 days in any 180-day period) and of the rights derived from an issued travel authorisation pursuant to Article 30(3); and

   (d) a link to the ETIAS public website containing information on the possibility for the applicant to revoke the travel authorisation.

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

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

   (b) a reference to the authority that refused the travel authorisation and its location;

   (c) the ground(s) for refusal of the travel authorisation, as laid down in Article 31(1);

   (d) information on the procedure to be followed for an appeal.

Article 33

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

Where a decision has been taken to issue or refuse a travel authorisation, the ETIAS Central System or, where relevant, the ETIAS National Units of the responsible Member State shall add the following data to the application file:

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

(b) a reference to the authority that issued or refused the travel authorisation and its location;

(c) place and date of the decision to issue or refuse the travel authorisation;

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

(e) the ground(s) for refusal of the travel authorisation as laid down in Article 31(1).

Article 34
Annulment of a travel authorisation

1. A travel authorisation shall be annulled where it becomes evident that the conditions for issuing it were not met at the time it was issued. The travel authorisation shall be annulled on the basis of one or more of the grounds for refusal of the travel authorisation laid down in Article 31(1).

2. Where a Member State is in possession of evidence that the conditions for issuing a travel authorisation were not met at the time it was issued, the ETIAS National Unit of that Member State shall annul the travel authorisation.

3. A person whose travel authorisation has been annulled shall have the right to appeal. Appeals shall be conducted in the Member State that has taken the decision on the annulment in accordance with the national law of that Member State.

Article 35
Revocation of a travel authorisation

1. A travel authorisation shall be revoked where it becomes evident that the conditions for issuing it are no longer met. The travel authorisation shall be revoked on the basis of one or more of the grounds for refusal of the travel authorisation laid down in Article 31(1).

2. Where a Member State is in possession of evidence that the conditions for issuing the travel authorisation are no longer met, the ETIAS National Unit of that Member State shall revoke the travel authorisation.

3. Without prejudice to paragraph 2, where a new refusal of entry alert or a travel document as lost, stolen or invalidated is reported in the SIS, the SIS shall inform the ETIAS Central System. The ETIAS Central System shall verify whether this new alert corresponds to a valid travel authorisation. Where this is the case, the ETIAS Central System shall transfer the application file to the ETIAS National Unit of the Member State having created the alert which shall revoke the travel authorisation.

4. New elements introduced by Europol in the ETIAS watchlist shall be compared to the data of the application files in the ETIAS Central System. Where the comparison results in a hit, the ETIAS National Unit of the Member State of first entry as declared by the applicant in accordance with Article 15(2)(j) shall assess the security risk and, where it concludes that the conditions for granting are no longer met, it shall revoke the travel authorisation.

5. An applicant whose travel authorisation has been revoked shall have the right to appeal. Appeals shall be conducted in the Member State that has taken the decision on the revocation and in accordance with the national law of that Member State.

6. A travel authorisation may be revoked at the request of the applicant.

Article 36
Notification on the annulment or revocation of a travel authorisation

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

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

(b) a reference to the authority that annulled or revoked the travel authorisation and its location;

(c) the ground(s) for the annulment or revocation of the travel authorisation, as laid down in Article 31(1);

(d) information on the procedure to be followed for an appeal.

Article 37

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

1. Where a decision has been taken to annul or to revoke a travel authorisation, the Member State responsible for the revocation or annulment of the travel authorisation shall add the following data to the application file:

(a) status information indicating that the travel authorisation has been annulled or revoked;

(b) a reference to the authority that revoked or annulled the travel authorisation and its location;

(c) place and date of the decision.

2. The application file shall also indicate the ground(s) for annulment or revocation as laid down in Article 31(1).

Article 38

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

1. A travel authorisation with limited territorial validity may be issued exceptionally, when the Member State concerned considers it necessary on humanitarian grounds, for reasons of national interest or because of international obligations notwithstanding the fact that the manual assessment process pursuant to Article 22 is not yet completed or that a travel authorisation has been refused, annulled or revoked.

2. For the purposes of paragraph 1, the applicant may apply for a travel authorisation with limited territorial validity to the Member State to which he or she intends to travel. He or she and shall indicate the humanitarian grounds, the reasons of national interest or the international obligations in his or her application.

3. The Member State to which the third country national intends to travel shall be the Member State responsible for deciding whether to issue or refuse a travel authorisation with limited territorial validity.

4. A travel authorisation with limited territorial validity shall be valid for the territory of the issuing Member State and for a maximum of 15 days.

5. Where a travel authorisation with territorial validity is issued, the following data shall be entered in the application file:

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

(b) the territory in which the travel authorisation holder is entitled to travel;

(c) the authority of the Member State that issued the travel authorisation with territorial validity;

(d) a reference to the humanitarian grounds, the reasons of national interest or the international obligations.

Chapter VII
Use of ETIAS by carriers

Article 39
Access to data for verification by carriers

1. In accordance with Article 26 of the Convention Implementing the Schengen Agreement carriers shall consult the ETIAS Central System in order to verify whether or not third country nationals subject to the travel authorisation requirement are in possession of a valid travel authorisation.

2. A secure internet access to the carrier gateway, including the possibility to use mobile technical solutions, referred to in Article 6(2)(h) shall allow carriers to proceed with the consultation referred to in paragraph 1 prior to the boarding of a passenger. For this purpose, the carrier shall be permitted to consult the ETIAS Central System using the data contained in the machine readable zone of the travel document.

The ETIAS Central System shall respond by indicating whether or not the person has a valid travel authorisation. Carriers may store the information sent and the answer received.

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

Article 40
Fall-back procedures in case of technical impossibility to access data by carriers

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

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

CHAPTER VIII
Use of ETIAS by border authorities at the external borders

Article 41
Access to data for verification at the external borders

1. For the sole purpose of verifying whether the person has a valid travel authorisation the authorities competent for carrying out checks at external border crossing points in accordance with Regulation (EU) 2016/399 shall be permitted to consult the ETIAS Central System using the data contained in the machine readable zone of the travel document.

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

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

1. Where it is technically impossible to proceed with the consultation referred to in Article 41(1), because of a failure of the ETIAS Information System, the Member State's authorities competent for carrying out checks at external border crossing points shall be notified by the ETIAS Central Unit.

2. Where it is technically impossible to perform the search referred to in Article 41(1) because of a failure of the national border infrastructure in a Member State, that Member State's competent authority shall notify eu-LISA, the ETIAS Central Unit and the Commission.

3. In both scenarios, the Member State's competent authorities for carrying out checks at external border crossing points shall follow their national contingency plans.

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

Article 43
Member States' designated law enforcement authorities

1. Member States shall designate the law enforcement authorities which are entitled to request consultation of data recorded in the ETIAS Central System in order to prevent, detect and investigate terrorist offences or other serious criminal offences.

2. At national level, each Member State shall keep a list of the contact points within the designated authorities that are authorised to request a consultation of data stored in the ETIAS Central System through the central access point(s).

Article 44

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

1. The competent authorities shall submit a reasoned electronic request for consultation of a specific set of data stored in the ETIAS Central System to the central access points referred to in Article 8(2)(c). Where consultation of data referred to in Article 15(2)(i) and (4)(b) to (d) is sought, the reasoned electronic request shall include a justification of the necessity to consult those specific data.

2. Each Member State shall ensure prior to accessing ETIAS Central System that according to its national law and procedural law a request for consultation undergoes an independent, efficient and timely verification whether the conditions referred to in Article 45 are fulfilled, including whether any request for consultation of data referred to in Article 15(2)(i) and (4)(b) to (d) is justified.

3. If the conditions referred to in Article 45 are fulfilled, the central access point shall process the requests. The data stored in the ETIAS Central System accessed by the central access point shall be transmitted to the contact points referred to in Article 43(2) in such a way as to not compromise the security of the data.

4. In an exceptional case of urgency, where there is a need to immediately obtain personal data necessary for preventing the commission of a serious crime or for prosecuting its perpetrators, the central access point shall process the request immediately and without the independent verification provided in paragraph 2. An ex post independent verification shall take place without undue delay after the processing of the request, including whether an exceptional case of urgency actually existed.

5. Where an ex post independent verification determines that the consultation of and access to the data recorded in the ETIAS Central System were not justified, all the authorities that accessed and/or consulted such data shall erase the data originating from the ETIAS Central System and shall inform the central access point of the erasure.

Article 45

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

1. Designated authorities may request consultation of data stored in the ETIAS Central System if all the following conditions are met:

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

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

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

   (d) prior consultation of all relevant national databases and the Europol data did not lead to the requested information.

2. Consultation of the ETIAS Central System shall be limited to searching with the following data recorded in the application file:

(a) surname (family name); first name(s) (given names);

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

(c) number of the travel document;

(d) home address;

(e) e-mail address; phone number;

(f) IP address.

3. Consultation of the ETIAS Central System with the data listed under paragraph 2 may be combined with the following data in the application file to narrow down the search:

(a) nationality or nationalities;

(b) sex;

(c) date of birth or age range.

4. Consultation of the ETIAS Central System shall, in the event of a hit with data recorded in an application file, give access to the data referred to in Article 15(2)(a) to (g) and (j) to (m) as recorded in that application file as well as to data entered in that application file in respect of the issuing, refusal, revocation or annulment of a travel authorisation in accordance with Articles 33 and 37. Access to the data referred to in Article 15(2)(i) and in (4) (b) to (d) as recorded in the application file shall only be given if consultation of that data was explicitly requested by the operating units in the reasoned electronic request submitted under Article 44(1) and approved by the independent verification. Consultation of the ETIAS Central System shall not give access to data concerning the education as referred to in Article 15(2)(h) or on whether or not the applicant may pose a public health risk as referred to in Article 15(4)(a).

Article 46

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

1. For the purposes of Article 1(2), Europol may request consultation of data stored in the ETIAS Central System and submit a reasoned electronic request for consultation of a specific set of data stored in the ETIAS Central System to the ETIAS Central Unit.

2. The reasoned request shall contain evidence that the following conditions are met:

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

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

(c) the consultation shall be limited to searching with data referred to in Article 45(2);

(d) reasonable grounds exist to consider that the consultation may substantially contribute to the prevention, detection or investigation of any of the criminal offences in question;

(e) prior consultation of the database at Europol did not lead to the requested information.

3. Europol requests for consultation of data stored in the ETIAS Central System shall be subject to prior verification by the EDPS, where appropriate in accordance with the procedure of Article 44 of Regulation (EU) 2016/794, which shall examine in an efficient and timely manner whether the request fulfils all conditions of paragraph 2.

4. Consultation of the ETIAS Central System shall, in the event of a hit with data stored in an application file, give access to the data referred to in Article 15(2)(a) to (g) and (j) to (m) as well as to the data entered in the application file in respect to the issuing, refusal, revocation or annulment of a travel authorisation in accordance with Articles 33 and 37. Access to the data referred to in Article 15(2)(i) and in (4)(b) to (d) as stored in the application file shall only be given if consultation of that data was explicitly requested by Europol.

5. Where the EDPS has approved the request, the ETIAS Central Unit shall process the request for consultation of data stored in the ETIAS Central System.

CHAPTER X
Retention and amendment of the data

Article 47
Data retention

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

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

(b) [five years from the last entry record of the applicant stored in the EES; or]

(c) five years from the last decision to refuse, revoke or annul the travel authorisation in accordance with Articles 31, 34 and 35.

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

Article 48
Amendment of data and advance data deletion

1. The ETIAS Central Unit and the ETIAS National Units shall have the obligation to update the data stored in the ETIAS Central System and ensure that it is correct. The ETIAS Central Unit and the ETIAS National Units shall not have the right to modify data entered in the application form directly by the applicant pursuant to Article 15(2) or (4).

2. Where the ETIAS Central Unit has evidence that data recorded in the ETIAS Central System by the ETIAS Central system are factually inaccurate or that data were processed in the ETIAS Central System in contravention of this Regulation, it shall check the data concerned and, if necessary, amend or erase them without delay from the ETIAS Central System.

3. Where the responsible Member State has evidence that data recorded in the ETIAS Central System are factually inaccurate or that data were processed in the ETIAS Central System in contravention of this Regulation, its ETIAS National Unit shall check the data concerned and, if necessary, amend or erase them without delay from the ETIAS Central System.

4. If a Member State different from the responsible Member State has evidence to suggest that data stored in the ETIAS Central System are factually inaccurate or that data were processed in the ETIAS Central System in contravention of this Regulation, it shall contact the ETIAS Central Unit or the ETIAS National Unit of the responsible Member State within a time limit of 14 days. The ETIAS Central Unit or the competent ETIAS National Unit shall check the accuracy of the data and the lawfulness of its processing within a time limit of one month and, if necessary, amend or erase the data from the ETIAS Central System without delay.

5. Where a third country national has acquired the nationality of a Member State or has fallen under the scope of Article 2(2)(a) to (e), the authorities of that Member State shall verify whether that person has a valid travel authorisation and, where relevant, shall delete the application file without delay from the ETIAS Central System. The authority responsible for deleting the application file shall be the:

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

   (b) the ETIAS National Unit of the Member State the nationality of which he or she has acquired;

   (c) the ETIAS National Unit of the Member State that issued the residence permit or card;

   (d) the ETIAS National Unit of the Member State that issued the long-stay visa.

6. Where a third country national has fallen under the scope of Article 2(2)(f) to (h), he or she shall inform the competent authorities of the Member State he or she next enters of this change. That Member State shall contact the ETIAS Central Unit within a time limit of 14 days. The ETIAS Central Unit shall check the accuracy of the data within a time limit of one month and, if necessary erase the application file and the data contained within from the ETIAS Central System without delay. The individual shall have access to an effective judicial remedy to ensure the data is deleted.

CHAPTER XI
Data protection

Article 49
Data Protection

1. Regulation (EC) No 45/2001 shall apply to the processing of personal data by the European Border and Coast Guard Agency and eu-LISA.

2. [Regulation 2016/679] shall apply to the processing of personal data by the ETIAS National Units.

3. [Directive (EU) 2016/680] shall apply to the processing by Member States designated authorities for the purposes of Article 1(2).

4. Regulation (EU) 2016/794 shall apply to the processing of personal data by Europol pursuant to Articles 24 and 46.

Article 50
Data controller

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

2. In relation to the processing of personal data in the ETIAS Central System by a Member State, the ETIAS National Unit is to be considered as controller in accordance with Article 4(7) of [Regulation (EU) 2016/679] which shall have central responsibility for the processing of personal data in ETIAS Central System by this Member State.

Article 51
Data processor

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

2. eu-LISA shall ensure that the ETIAS Information System is operated in accordance with this Regulation.

Article 52
Security of processing

1. Both eu-LISA and the ETIAS National Units shall ensure the security of processing of personal data takes place pursuant to the application of this Regulation. eu-LISA and the ETIAS National Units shall cooperate on security related tasks.

2. Without prejudice to Article 22 of Regulation (EC) No 45/2001, eu-LISA shall take the necessary measures to ensure the security of the Central System, the Communication

Infrastructure between the Central System and the National Uniform Interface, the public website and mobile app, the email service, the secure account service, the carrier gateway, the web service and the software enabling to process the applications;

3. Without prejudice to Article 22 of Regulation (EC) No 45/2001 and Articles 32 and 34 of [Regulation (EU) 2016/679], both eu-LISA and the ETIAS National Units shall adopt the necessary measures, including a security plan and a business continuity and disaster recovery plan, in order to:

(a) physically protect data, including by making contingency plans for the protection of critical infrastructure;

(b) deny unauthorised persons access to the secure website that carries out operations in accordance with the purposes of the ETIAS;

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

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

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

(f) ensure that persons authorised to access the ETIAS Information System have access only to the data covered by their access authorisation, by means of individual user identities and confidential access modes only;

(g) ensure that all authorities with a right of access to the ETIAS Information System create profiles describing the functions and responsibilities of persons who are authorised to enter, amend, delete, consult and search the data and make their profiles available to the supervisory authorities;

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

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

(j) prevent the unauthorised reading, copying, modification or deletion of personal data during the transmission of personal data to or from the ETIAS Central System or during the transport of data media, in particular by means of appropriate encryption techniques;

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

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

Article 53
Self-monitoring

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

Article 54
Right of information, access, correction and erasure

1. Without prejudice to the right of information in Articles 11 and 12 of Regulation (EC) 45/2001, applicants whose data are stored in the ETIAS Central System shall be informed, at the time their data are collected, on the procedures for exercising the rights under Articles 13, 14, 15 and 16 of Regulation (EC) 45/2001 and on the contact details of the data protection officer of the European Border and Coast Guard Agency, of the European Data Protection Supervisor and of the national supervisory authority of the responsible Member State.

2. In order to exercise their rights under Articles 13, 14, 15 and 16 of Regulation (EC) 45/2001 and Article 15, 16, 17 and 18 of [Regulation (EU) 2016/679] any applicant shall have the right to address him or herself to the ETIAS Central Unit or to the ETIAS National Unit responsible for the application, who shall examine and reply to the request.

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

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

3. Where the ETIAS Central Unit or the ETIAS National Unit of the Member State responsible for the application do not agree that data stored in the ETIAS Central System are factually inaccurate or have been recorded unlawfully, the ETIAS Central Unit or the ETIAS National Unit of the Member State responsible for the application shall adopt an administrative decision explaining in writing to the person concerned without delay why it is not prepared to correct or delete data relating to him.

4. This decision shall also provide the person concerned with information explaining the possibility to challenge the decision taken in respect of the request referred in paragraph 2 and where relevant, information on how to bring an action or a complaint before the

competent authorities or courts and any assistance, including from the competent national supervisory authorities.

5. Any request made pursuant to paragraph 2 shall contain the necessary information to identify the person concerned. That information shall be used exclusively to enable the exercise of the rights referred to in paragraph 2 and shall be erased immediately afterwards.

6. The ETIAS Central Unit or the ETIAS National Unit of the Member State responsible for the application shall keep a record in the form of a written document that a request referred to in paragraph 2 was made and how it was addressed and shall make that document available to competent data protection national supervisory authorities without delay.

Article 55
Communication of personal data to third countries, international organisations and private parties

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

2. Personal data accessed from the ETIAS Central System by a Member State or by for the purposes referred to in Article 1(2) shall not be transferred or made available to any third country, international organisation or private entity established in or outside the Union. The prohibition shall also apply if those data are further processed at national level or between Member States.

Article 56
Supervision by the national supervisory authority

1. The supervisory authority or authorities designated pursuant to Article 51 of [Regulation 2016/679] shall ensure that an audit of the data processing operations by the ETIAS National Units is carried out in accordance with relevant international auditing standards at least every four years.

2. Member States shall ensure that their supervisory authority has sufficient resources to fulfil the tasks entrusted to it under this Regulation.

3. Each Member State shall supply any information requested by the supervisory authorities and shall, in particular, provide them with information on the activities carried out in accordance with their responsabilities as laid down in this Regulation. Each Member State shall grant the supervisory authorities access to their records and allow them access at all times to all their ETIAS related premises.

Article 57
Supervision by the European Data Protection Supervisor

The European Data Protection Supervisor shall ensure that an audit of eu-LISA's and the ETIAS Central Unit personal data processing activities is carried out in accordance with relevant international auditing standards at least every four years. A report of that audit

shall be sent to the European Parliament, the Council, eu-LISA, the Commission and the Member States. eu-LISA and the European Border and Coast Guard Agency shall be given an opportunity to make comments before their reports are adopted.

Article 58
Cooperation between national supervisory authorities and the European Data Protection Supervisor

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

2. In cases referred to under paragraph 1, the European Data Protection Supervisor and the national supervisory authorities competent for data protection supervision may, each acting within the scope of their respective competences, exchange relevant information, assist each other in carrying out audits and inspections, examine difficulties over the interpretation or application of this Regulation, study problems related to the exercise of independent supervision or the exercise of the rights of the data subject, draw up harmonised proposals for joint solutions to any problems and promote awareness of data protection rights, as necessary.

3. The supervisory authorities and the European Data Protection Supervisor shall meet for that purpose at least twice a year as part of the Board established by [Regulation (EU) 2016/679]. The costs of these meetings shall be borne by the Board established by [Regulation (EU) 2016/679]. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary.

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

Article 59
Keeping of records

1. eu-LISA shall keep records of all data processing operations performed within the ETIAS Information System. Those records shall show the purpose of the access, the date and time of each operation, the data used for the automated processing of the applications, the hits found while carrying out the automated processing laid down in Article 18, the data used for verification of the identity regarding the ETIAS Central System or other information systems and databases, the results of the verification process referred to in Article 20 and the staff having performed it.

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

3. The ETIAS National Unit of the responsible Member State shall keep records in the ETIAS Information System of all data processing operations while carrying out the

assessment referred to in Article 22. Those records shall show the date and time of each operation, the data used for interrogation of other information systems and databases, the data linked to the hit received, the staff having performed the risk assessment and the justification behind the decision to issue, refuse, revoke or annul a travel authorisation.

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

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

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

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

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

Article 60
Keeping of records, logs and documentation for requests for consultation of data for law enforcement access

1. eu-LISA shall keep records of all data processing operations performed within the ETIAS Central System concerning the access by central access points for the purposes of Article 1(2). Those records shall show the date and time of each operation, the data used for launching the search, the data transmitted by the ETIAS Central System and the name of the authorised staff of the central access points entering and retrieving the data.

2. In addition, each Member State and Europol shall keep records of all data processing operations within the ETIAS Central System resulting from requests to consult of or access to data stored in the ETIAS Central System for the purposes laid down in Article 1(2). The records shall include logs and documentation of all data processing operations.

3. The records shall show:

(a) the exact purpose of the request for consultation of or access to data stored in the ETIAS Central System, including the terrorist offence or other serious criminal offence concerned and, for Europol, the exact purpose of the request for consultation;

(b) the decision taken with regard to the admissibility of the request;

(c) the national file reference;

(d) the date and exact time of the request for access made by the National Access Point to the ETIAS Central System;

(e) where applicable, the use of the urgent procedure referred to in Article 44(4) and the decision taken with regard to the ex-post verification;

(f) which of data or set of data referred to in Article 45(2) and (3) have been used for consultation;

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

4. The records referred to in paragraphs 1 and 2 shall be used only to check the admissibility of the request, monitor the lawfulness of data processing and to ensure data integrity and security. Only records containing non-personal data may be used for the monitoring and evaluation referred to in Article 81. The European Data Protection Supervisor and the competent supervisory authorities responsible for monitoring the lawfulness of the data processing and data integrity and security shall have access to those records at their request for the purpose of fulfilling their duties. The authority responsible for checking the admissibility of the request shall also have access to those records for this purpose. Other than for such purposes, personal data, as well as the records of the consultation requests of data stored in the ETIAS Central System shall be erased in all national and Europol files after a period of one month, unless those data and records are required for the purposes of the specific ongoing criminal investigation for which they were requested by a Member State or by Europol.

CHAPTER XII
Public awareness

Article 61
Information to the general public

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

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

(b) information concerning the website and the mobile application for a web device where the application can be launched;

(c) the deadlines for deciding on an application provided for in Article 27;

(d) that decisions on applications must be notified to the applicant, that such decisions must state, where relevant, the reasons for refusal on which they are based and that applicants whose applications are refused have a right to appeal, with information regarding the procedure to be followed in the event of an appeal, including the competent authority, as well as the time limit for lodging an appeal;

(e) that mere possession of a travel authorisation does not confer an automatic right of entry and that the holders of a travel authorisation are requested to present proof that

they fulfil the entry conditions at the external border, as provided for in Article 6 of Regulation (EU) 2016/399.

Article 62
Information campaign

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

CHAPTER XIII
Responsibilities

Article 63
Responsibilities of eu-LISA during the designing and development phase

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

2. The infrastructures supporting the public website, the mobile app and the carrier gateway shall be hosted in eu-LISA' sites or in Commission sites. These infrastructures shall be geographically distributed to provide the functionalities laid down in this Regulation in accordance with the conditions of security, availability, quality and speed laid down in paragraph 3.

3. eu-LISA shall be responsible for the development of the ETIAS Information System, for any development required for establishing interoperability between the ETIAS Central System and the information systems referred to in Article 10.

   eu-LISA shall define the design of the physical architecture of the system including its Communication Infrastructure as well as the technical specifications and their evolution as regards the Central System, the Uniform Interfaces, which shall be adopted by the Management Board, subject to a favourable opinion of the Commission. eu-LISA shall also implement any necessary adaptations to the EES, SIS, Eurodac, ECRIS or VIS deriving from the establishment of interoperability with the ETIAS.

   eu-LISA shall develop and implement the Central System, the National Uniform Interfaces, and the Communication Infrastructure as soon as possible after the entry into force of this Regulation and the adoption by the Commission of the measures provided for in Article 15(2) and (4), Article 16(4), Article 28(5), Article 39(3), Article 40(2) and Article 72(1) and (4).

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

4. During the designing and development phase, a Programme Management Board composed of a maximum of 10 members shall be established. It shall be composed of six members

appointed by eu-LISA's Management Board from among its members or its alternates, the Chair of the ETIAS-EES Advisory Group referred to in Article 80, a member representing eu-LISA appointed by its Executive Director, a member representing the European Border and Coast Guard Agency appointed by its Executive Director and one member appointed by the Commission. The members appointed by eu-LISA's Management Board shall be elected only from those Member States which are fully bound under Union law by the legislative instruments governing the development, establishment operation and use of all the large-scale IT systems managed by eu-LISA and which will participate in the ETIAS. The Programme Management Board will meet once a month. It shall ensure the adequate management of the design and development phase of the ETIAS. The Programme Management Board shall submit written reports every month to the Management Board on progress of the project. It shall have no decision-making power nor any mandate to represent the members of the Management Board.

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

(a) chairmanship;

(b) meeting venues;

(c) preparation of meetings;

(d) admission of experts to the meetings;

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

The chairmanship shall be held by the Member State holding the Presidency, provided it is fully bound under Union law by the legislative instruments governing the development, establishment operation and use of all the large-scale IT systems managed by eu-LISA or, if this requirement is not met, by the Member State which shall next hold the Presidency and which meets that requirement.

All travel and subsistence expenses incurred by the members of the Programme Management Board shall be paid by the Agency and Article 10 of the eu-LISA Rules of Procedure shall apply mutatis mutandis. The Programme Management Board's secretariat shall be ensured by eu-LISA.

The EES-ETIAS Advisory Group referred to in Article 80 shall meet regularly until the start of operations of the ETIAS. It shall report after each meeting to the Programme Management Board. It shall provide the technical expertise to support the tasks of the Programme Management Board and shall follow-up on the state of preparation of the Member States.

Article 64

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

1. Following the entry into operations of the ETIAS, eu-LISA shall be responsible for the technical management of the Central System and the National Uniform Interfaces. It shall ensure, in cooperation with the Member States, at all times the best available technology, subject to a cost-benefit analysis. eu-LISA shall also be responsible for the technical management of the Communication Infrastructure between the Central system and the

National Uniform Interfaces as well as for the public website, the mobile app for mobile devices, the email service, the secure account service, the carrier gateway, the web service and the software to process the applications referred to in Article 6.

Technical management of the ETIAS shall consist of all the tasks necessary to keep the ETIAS Information System functioning 24 hours a day, 7 days a week in accordance with this Regulation, in particular the maintenance work and technical developments necessary to ensure that the system functions at a satisfactory level of technical quality, in particular as regards the response time for interrogation of the central database in accordance with the technical specifications.

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

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

Article 65
Responsibilities of the European Coast and Border Guard Agency

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

   (a) the setting up and operation of the ETIAS Central Unit;

   (b) the automated processing of applications;

   (c) the screening rules.

2. Before being authorised to process data recorded in the ETIAS Central System, the staff of the ETIAS Central Unit having a right to access the ETIAS Central System shall be given appropriate training about data security and data protection rules, in particular on relevant fundamental rights.

Article 66
Responsibilities of Member States

1. Each Member State shall be responsible for:

   (a) the connection to the National Uniform Interface;

   (b) the organisation, management, operation and maintenance of the ETIAS National Units for the examination of and decision on travel authorisations' applications rejected during the automated processing of applications;

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

   (d) the management and arrangements for access of duly authorised staff of the competent national authorities to the ETIAS Information System in accordance with

this Regulation and to establish and regularly update a list of such staff and their profiles;

(e) the set up and operation of the ETIAS National Units.

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

3. Before being authorised to process data recorded in the ETIAS Central System, the staff of the ETIAS National Units having a right to access the ETIAS Information System shall be given appropriate training about data security and data protection rules, in particular on relevant fundamental rights.

Article 67
Responsibilities of Europol

1. Europol shall ensure processing of the queries referred to in Article 18(2)(j) and (4) and accordingly adapting its information system.

2. Europol shall be responsible for the establishment of the ETIAS watchlist pursuant to Article 29.

3. Europol shall be responsible for providing an opinion following a consultation request pursuant to Article 26.

CHAPTER XIV
Amendments to other Union instruments

Article 68
Amendments to Regulation (EU) 515/2014

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

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

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

Article 69
Amendments to Regulation (EU) 2016/399

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

1. Article 6 is amended as follows:

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

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

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

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

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

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

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

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

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

Article 70
Amendments to Regulation (EU) 2016/794

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

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

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

2. Article 21 is amended as follows:

(a) the title is replaced by the following:

"Article 21

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

(b) the following paragraph 1a is inserted:

"Europol shall take all appropriate measures to enable the European Borders and Coast Guard Agency, within its mandate and for the purposes of Regulation [Regulation establishing a European Travel Information and Authorisation System (ETIAS)], to have indirect access on the basis of a hit/no hit system to information provided for the purposes of point (a) of Article 18(2) without prejudice to any restrictions indicated by the Member

State, Union body, third country or international organisation providing the information in question, in accordance with Article 19(2).

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

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

Article 71
Amendments to Regulation (EU) 2016/1624

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

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

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

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

"Section 5

The ETIAS

Article 33a
Creation of the ETIAS Central Unit

1. An ETIAS Central Unit is hereby established.

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

CHAPTER XV
Final provisions

Article 72
Transitional period and transitional measures

1. For a period of six months from the date ETIAS commences operations, the utilisation of ETIAS shall be optional and the requirement to be in possession of a valid travel authorisation shall not apply. The Commission may adopt a delegated act in accordance with Article 78 to extend that period for a maximum of a further six months.

2. During this six month period, the border guards shall inform third country nationals subject to the travel authorisation requirement crossing the external borders of the requirement to have a valid travel authorisation from the expiry of the six month period. For this purpose, the border guards shall distribute a common leaflet to this category of travellers.

3. The common leaflet shall be drawn up and set up by the Commission. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 79(2) and shall contain at a minimum the information referred to in Article 61. The leaflet shall be clear and simple and available in a language version the person concerned understands or is reasonably assumed to understand.

4. A period of grace may be established following the end of the period defined in paragraph 1. During such period, the requirement to be in possession of a valid travel authorisation shall apply. During the period of grace the border guards shall exceptionally allow third country nationals subject to the travel authorisation requirement who are not in possession of a travel authorisation to cross the external borders where they fulfil all the remaining conditions of Article 6(1) of Regulation (EU) 2016/399 provided that they cross the external borders of the Member States for the first time since the end of the period referred to in paragraph 1 of this Article. Border guards shall notify the third country nationals subject to the travel authorisation requirement of the requirement to be in possession of a valid travel authorisation in accordance with Article 6(1)(b) of Regulation (EU) 2016/399.

5. The Commission shall adopt delegated acts on the duration of the period of grace referred to in paragraph 4. That period shall not exceed twelve months from the end of the period defined in paragraph 1.

Article 73
Use of data for reporting and statistics

1. The duly authorised staff of the competent authorities of Member States, the Commission, eu-LISA and the ETIAS Central Unit shall have access to consult the following data, solely for the purposes of reporting and statistics without allowing for individual identification:

   (a) status information;

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

   (c) the country of residence;

   (d) education;

   (e) current occupation (domain), job title;

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

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

   (h) the validity period of the travel authorisation;

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

2. For the purpose of paragraph 1, eu-LISA shall establish, implement and host a central repository containing the data referred to in paragraph 1 which would not allow for the identification of individuals and would allow the authorities listed in paragraph 1 to obtain customisable reports and statistics to improve the assessment of the irregular migration, security and health risks, to enhance the efficiency of border checks, to help the ETIAS Central Unit processing the travel authorisation applications and to support evidence-based Union migration policymaking. The repository shall also contain daily statistics on the data referred to in paragraph 4. Access to the central repository shall be granted by means of secured access through S-TESTA with control of access and specific user profiles solely for the purpose of reporting and statistics.

Detailed rules on the operation of the central repository and the data protection and security rules applicable to the repository shall be adopted in accordance with the examination procedure referred to in Article 79(2).

3. The procedures put in place by eu-LISA to monitor the development and the functioning of the ETIAS Information System referred to in Article 81(1) shall include the possibility to produce regular statistics for ensuring that monitoring.

4. Every quarter, eu-LISA shall publish statistics on the ETIAS Information System showing in particular the number and nationality of applicants whose travel authorisation was refused, including the grounds for refusal, and of third country nationals whose travel authorisation were annulled or revoked.

5. At the end of each year, statistical data shall be compiled in the form of quarterly statistics for that year.

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

Article 74
Costs

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

The following costs shall be excluded:

(a) Member States' project management office (meetings, missions, offices);

(b) hosting of national systems (space, implementation, electricity, cooling);

(c) operation of national systems (operators and support contracts);

(d) customisation of existing border checks;

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

Article 75
Revenues

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

Article 76
Notifications

1. Member States shall notify the Commission of the authority which is to be considered as controller referred to in Article 50.

2. The ETIAS Central Unit and the Member States shall notify eu-LISA of the competent authorities referred to in Article 11 which have access to the ETIAS Information System.

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

3. Member States shall notify the Commission of their designated authorities referred to in Article 43 and shall notify without delay any amendments thereto.

4. eu-LISA shall notify the Commission of the successful completion of the test referred to in Article 77(1)(b).

5. The Commission shall make the information notified pursuant to paragraph 1 available to the Member States and the public by a constantly updated public website.

Article 77
Start of operations

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

   (a) the measures referred to in Article 15(3) and (4), Article 16(4), Article 28(3), Article 39(3), Article 40(2), Article 72(1) and (5) and Article 73(2) have been adopted;

   (b) eu-LISA has declared the successful completion of a comprehensive test of the ETIAS;

   (c) eu-LISA and the ETIAS Central Unit have validated the technical and legal arrangements to collect and transmit the data referred to in Article 15 to the ETIAS Central System and have notified them to the Commission;

   (d) the Member States and the ETIAS Central Unit have notified to the Commission the data concerning the various authorities referred to in Article 76(1) and (3).

2. The test of the ETIAS referred to in point (b) of paragraph 1 shall be conducted by eu-LISA in cooperation with the Member States and the ETIAS Central Unit.

3. The Commission shall inform the European Parliament and the Council of the results of the test carried out pursuant to point (b) of paragraph 1.

4. The Commission decision referred to in paragraph 1 shall be published in the *Official Journal of the European Union*.

5. The Member States and the ETIAS Central Unit shall start using the ETIAS from the date determined by the Commission in accordance with paragraph 1.

Article 78
Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 15(3) and (4), Article 16(4), Article 28(3) and Article 72(1) and (5) shall be conferred on the Commission for an indeterminate period of time from [*the date of entry into force of this Regulation*].

3. The delegation of power referred to in Article 15(3) and (4), Article 16(4), Article 28(3) and Article 72(1) and (5) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to Article 15(2) and (4), Article 16(4), Article 28(3) and Article 72(1) and (4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of [two months] of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by [two months] at the initiative of the European Parliament or of the Council.

Article 79
Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Article 80
Advisory group

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

Article 81
Monitoring and evaluation

1. eu-LISA shall ensure that procedures are in place to monitor the development of the ETIAS Information System in light of objectives relating to planning and costs and to monitor the functioning of the ETIAS in light of objectives relating to the technical output, cost-effectiveness, security and quality of service.

2. By [*Six months after the entry into force of this Regulation* – OPOCE, please replace with the actual date] and every six months thereafter during the development phase of the ETIAS Information System, eu-LISA shall submit a report to the European Parliament and the Council on the state of play of the development of the Central System, the Uniform Interfaces and the Communication Infrastructure between the Central System and the Uniform Interfaces. Once the development is finalised, a report shall be submitted to the European Parliament and the Council explaining in detail how the objectives, in particular relating to planning and costs, were achieved as well as justifying any divergences.

3. For the purposes of technical maintenance, eu-LISA shall have access to the necessary information relating to the data processing operations performed in the ETIAS Information System.

4. For the first time two years after the start of operations of the ETIAS and every two years thereafter, eu-LISA shall submit to the European Parliament, the Council and the Commission a report on the technical functioning of ETIAS Information System, including the security thereof.

5. Three years after the start of operations of the ETIAS and every four years thereafter, the Commission shall evaluate ETIAS and shall make any necessary recommendations to the European Parliament and the Council. This evaluation shall include:

   (a) the results achieved by the ETIAS having regard to its objectives, mandate and tasks;

   (b) the impact, effectiveness and efficiency of the ETIAS performance and its working practices in relation to its objectives, mandate and tasks;

   (c) the rules of the automated application processor used for the purpose of risk assessment;

   (d) the possible need to modify the mandate of the ETIAS Central Unit;

   (e) the financial implications of any such modification;

   (f) the impact on fundamental rights.

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

6. The Member States and Europol shall provide eu-LISA, the ETIAS Central Unit and the Commission with the information necessary to draft the reports referred to in paragraphs 4 and 5. This information shall not jeopardise working methods or include information that reveals sources, staff members or investigations of the designated authorities.

7. eu-LISA and the ETIAS Central Unit shall provide the Commission with the information necessary to produce the evaluations referred to in paragraph 5.

8. While respecting the provisions of national law on the publication of sensitive information, each Member State and Europol shall prepare annual reports on the effectiveness of access to data stored in the ETIAS Central System for law enforcement purposes containing information and statistics on:

(a) the exact purpose of the consultation including the type of terrorist or serious criminal offence;

(b) reasonable grounds given for the substantiated suspicion that the suspect, perpetrator or victim is covered by this Regulation;

(c) the number of requests for access to the ETIAS Central System for law enforcement purposes;

(d) the number and type of cases which have ended in successful identifications;

(e) the need and use made of the exceptional case of urgency including those cases where that urgency was not accepted by the ex post verification carried out by the central access point.

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

Article 82
Entry into force and applicability

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

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

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*