

ETIAS consequential amendments: borders and visa

2019/0002(COD) - 07/06/2021 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted a legislative resolution on the proposal for a regulation of the European Parliament and of the Council establishing the conditions for accessing other EU information systems for ETIAS purposes and amending Regulation (EU) 2018/1240, Regulation (EC) No 767/2008, Regulation (EU) 2017/2226 and Regulation (EU) 2018/1861.

The European Parliament's position adopted at first reading under the ordinary legislative procedure amends the Commission's proposal as follows:

Access from the ETIAS Central Unit to other EU information systems, Europol data and Interpol databases

Regulation (EU) 2018/1240 of the European Parliament and of the Council established the European Travel Information and Authorisation System (ETIAS) for third-country nationals exempt from the visa requirement when crossing the external borders of the Union. ETIAS makes it possible to assess whether the presence of such third-country nationals on the territory of the Member States would pose a security or illegal immigration risk or a high epidemic risk.

This Regulation amends Regulations of the European Parliament and of the Council (EU) 2018/1240, (EC) No 767/2008, (EU) 2017/2226, (EU) and 2018/1861 in order to enable the ETIAS central system to carry out checks against the Schengen Information System (SIS), the Visa Information System (VIS) the Entry/Exit System (EES), Eurodac and the database on criminal records of third-country nationals (ECRIS-TCN), as well as Europol data and the Interpol databases on Stolen and Lost Travel Documents (SLTD) and Travel Documents Associated with Notices (TDAWN).

The amending regulation allows the connection of the ETIAS Central System to these databases and defines the data that can be accessed for ETIAS purposes, as well as the **conditions and rights of access** of the ETIAS Central Unit and the ETIAS National Units. Access to the relevant data in these systems should enable the authorities to assess the security or immigration risk of applicants and to decide whether to issue or refuse a travel authorisation.

Access by Member States, through the ETIAS National Units, to other EU information systems should be in accordance with their participation in the various legal instruments.

Application form and personal data of the applicant

The amended text specifies that the applicant will have to answer the questions by indicating whether he or she has been convicted in the previous 25 years of a terrorist offence or in the previous 15 years of any other criminal offence listed in the Annex, and if so when and in which country.

Automated processing

The ETIAS Central System should send an automated notification to the ETIAS Central Unit.

The **European Search Portal (ESP)**, established by Regulation (EU) 2019/817 and Regulation (EU) 2019/818 of the European Parliament and of the Council, should enable the data stored in ETIAS and the data stored in the other EU information systems concerned to be queried in parallel.

The ETIAS Central System should verify:

- whether the travel document used for the application corresponds to a travel document reported lost, stolen, misappropriated or invalidated in SIS;
- whether the applicant is subject to a refusal of entry and stay alert entered in SIS;
- whether the applicant is currently reported as an overstayer or whether he or she has been reported as an overstayer in the past in the EES;
- whether the applicant is subject to an alert in respect of persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant or wanted for arrest for extradition purposes in SIS.

Where there are doubts about the identity of the applicant or where the automated verifications have reported a hit, the application should be processed manually by the competent authorities.

The ETIAS Central Unit should provide periodical reports to the Commission and eu-LISA on false hits that are generated during the automated checks.

Refusal of authorisation

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.

During the appeal procedure, the appellant should be given access to the information in the application file in accordance with the data protection rules of this Regulation. The ETIAS National Unit of the Member State responsible should provide applicants with information regarding the appeal procedure. That information should be provided in one of the official languages of the countries listed in Annex II to Regulation (EC) No 539/2001 of which the applicant is a national.

Fallback procedures in case of technical impossibility of access to data by carriers

Where technical difficulties make it impossible for carriers to access the ETIAS Information System through the carrier gateway, the ETIAS Central Unit should provide operational support to carriers in order to limit the impact on passenger travel and carriers to the extent possible.

Implementation

The Commission may adopt delegated acts concerning the definition of the conditions for matching data contained in a record, alert or file of other EU information systems consulted with data contained in an ETIAS application file.

It may adopt implementing acts (i) to establish the technical arrangements for the implementation of certain data retention provisions and to further specify the rules concerning the support to be provided to carriers by the ETIAS Central Unit and (ii) to lay down the details of fallback procedures in case of technical impossibility for carriers to access the data and to further specify the rules concerning the support to be provided to carriers by the ETIAS Central Unit.

