Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226

CHAPTER X

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

Article 50

Member States' designated authorities

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

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

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

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

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

3 At national level, each Member State shall keep a list of the operating units within the designated authorities that are authorised to request a consultation of data stored in the ETIAS Central System through the central access points.

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

Article 51

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

1 An operating unit referred to in Article 50(3) shall submit a reasoned electronic or written request for consultation of a specific set of data stored in the ETIAS Central System to a central access point referred to in Article 50(2). Where consultation of data referred to in point

(i) of Article 17(2) and points (a) to (c) of Article 17(4) is sought, the reasoned electronic or written request shall include a justification of the necessity to consult those specific data.

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

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

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

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

Article 52

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

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

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

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

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

[[F1]1a In cases where the designated authorities have launched a query of the CIR in accordance with Article 22 of Regulation (EU) 2019/817, they may access the application files stored in the ETIAS Central System in accordance with this Article for consultation where the reply received as referred to in Article 22(2) of Regulation (EU) 2019/817 reveals that data are stored in the application files stored in the ETIAS Central System.**]**

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

a surname (family name) and, if available, first name(s) (given names);

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

c number of the travel document;

d home address;
e email address;
f phone numbers;
g IP address.

3 Consultation of the ETIAS Central System with the data listed under paragraph 2 may be combined with the following data in the application file to narrow down the search:
a nationality or nationalities;
b sex;
c date of birth or age range.

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

Textual Amendments

F1 Inserted by Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA.

Article 53

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

1 For the purposes of Article 1(2), Europol may request to consult data stored in the ETIAS Central System and submit a reasoned electronic request to consult a specific set of data stored in the ETIAS Central System to the ETIAS Central Unit. Where consultation of data referred to in point (i) of Article 17(2) and points (a) to (c) of Article 17(4) is sought, the reasoned electronic request shall include a justification of the necessity to consult those specific data.

[[F1]1a In cases where Europol has launched a query of the CIR in accordance with Article 22 of Regulation (EU) 2019/817, it may access the application files stored in the ETIAS Central System in accordance with this Article for consultation where the reply received as referred to in Article 22(2) of Regulation (EU) 2019/817 reveals that data are stored in the application files stored in the ETIAS Central System.**]**

2 The reasoned request shall contain evidence that all the following conditions are met:
a the consultation is necessary to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences falling under Europol's mandate;

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

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

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

3 Europol requests for consultation of data stored in the ETIAS Central System shall be subject to prior verification by a specialised unit of duly empowered Europol officials, which shall examine in an efficient and timely manner whether the request fulfils all the conditions in paragraph 2.

4 Consultation of the ETIAS Central System shall, in the event of a hit with data stored in an application file, give access to the data referred to in points (a) to (g) and (j) to (m) of Article 17(2) as well as to the data added to the application file relating to the issue, refusal, annulment or revocation of a travel authorisation in accordance with Articles 39 and 43. Access to the data referred to in point (i) of Article 17(2) and points (a) to (c) of Article 17(4) added to the application file shall only be given if consultation of those data was explicitly requested by Europol. Consultation of the ETIAS Central System shall not give access to the data concerning education referred to in point (h) of Article 17(2).

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

Textual Amendments

F1 Inserted by Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA.

Changes to legislation:
There are currently no known outstanding effects for the Regulation (EU) 2018/1240 of the European Parliament and of the Council, CHAPTER X.