Regulation (EU) 2019/818 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 police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816

CHAPTER IV

Common identity repository

Article 17

Common identity repository

1 A common identity repository (CIR), creating an individual file for each person that is registered in the EES, VIS, ETIAS, Eurodac or ECRIS-TCN containing the data referred to in Article 18, is established for the purpose of facilitating and assisting in the correct identification of persons registered in the EES, VIS, ETIAS, Eurodac and ECRIS-TCN in accordance with Article 20, of supporting the functioning of the MID in accordance with Article 21 and of facilitating and streamlining access by designated authorities and Europol to the EES, VIS, ETIAS and Eurodac, where necessary for the prevention, detection or investigation of terrorist offences or other serious criminal offences in accordance with Article 22.

2 The CIR shall be composed of:

a a central infrastructure that shall replace the central systems of respectively the EES, VIS, ETIAS, Eurodac and ECRIS-TCN to the extent that it shall store the data referred to in Article 18;

b a secure communication channel between the CIR, Member States and Union agencies that are entitled to use the CIR in accordance with Union and national law;

c a secure communication infrastructure between the CIR and the EES, VIS, ETIAS, Eurodac and ECRIS-TCN as well as with the central infrastructures of the ESP, the shared BMS and the MID.

3 eu-LISA shall develop the CIR and ensure its technical management.

4 Where it is technically impossible because of a failure of the CIR to query the CIR for the purpose of identifying a person pursuant to Article 20, for the detection of multiple identities pursuant to Article 21 or for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences pursuant to Article 22, the CIR users shall be notified by eu-LISA in an automated manner.

5 eu-LISA, in cooperation with Member States, shall implement an interface control document based on the UMF referred to in Article 38 for the CIR.

Article 18

The common identity repository data

1 The CIR shall store the following data, logically separated according to the information system from which the data have originated: the data referred to in Article 5(1)(b) and (2) and the following data listed in Article 5(1)(a) of Regulation (EU) 2019/816: surname

Status: Point in time view as at 31/01/2020.
Changes to legislation: There are outstanding changes not yet made to Regulation (EU) 2019/818 of the European Parliament and of the Council. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details)

(family name), first names (given names), date of birth, place of birth (town and country), nationality or nationalities, gender, previous names, if applicable, where available pseudonyms or aliases, as well as, where available, information on travel documents.

2 For each set of data referred to in paragraph 1, the CIR shall include a reference to the EU information systems to which the data belong.

3 The authorities accessing the CIR shall do so in accordance with their access rights under the legal instruments governing the EU information systems, and under national law and in accordance with their access rights under this Regulation for the purposes referred to in Articles 20, 21 and 22.

4 For each set of data referred to in paragraph 1, the CIR shall include a reference to the actual record in the EU information systems to which the data belong.

5 The storage of the data referred to in paragraph 1 shall meet the quality standards referred to in Article 37(2).

Article 19

Adding, amending and deleting data in the common identity repository

1 Where data are added, amended or deleted in Eurodac or ECRIS-TCN, the data referred to in Article 18 stored in the individual file of the CIR shall be added, amended or deleted accordingly in an automated manner.

2 Where a white or red link is created in the MID in accordance with Article 32 or 33 between the data of two or more of the EU information systems constituting the CIR, instead of creating a new individual file, the CIR shall add the new data to the individual file of the linked data.

Article 20

Access to the common identity repository for identification

1 Queries of the CIR shall be carried out by a police authority in accordance with paragraphs 2 and 5 only in the following circumstances:

a where a police authority is unable to identify a person due to the lack of a travel document or another credible document proving that person's identity;
b where there are doubts about the identity data provided by a person;
c where there are doubts as to the authenticity of the travel document or another credible document provided by a person;
d where there are doubts as to the identity of the holder of a travel document or of another credible document; or
e where a person is unable or refuses to cooperate.

Such queries shall not be allowed against minors under the age of 12 years old, unless in the best interests of the child.

2 Where one of the circumstances listed in paragraph 1 arises and a police authority has been so empowered by national legislative measures as referred to in paragraph 5, it may, solely for the purpose of identifying a person, query the CIR with the biometric data of that person

***Status:** Point in time view as at 31/01/2020.*
***Changes to legislation:** There are outstanding changes not yet made to Regulation (EU) 2019/818 of the European Parliament and of the Council. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details)*

taken live during an identity check, provided that the procedure was initiated in the presence of that person.

3 Where the query indicates that data on that person are stored in the CIR, the police authority shall have access to consult the data referred to in Article 18(1).

Where the biometric data of the person cannot be used or where the query with that data fails, the query shall be carried out with identity data of the person in combination with travel document data, or with the identity data provided by that person.

4 Where a police authority has been so empowered by national legislative measures as referred to in paragraph 6, it may, in the event of a natural disaster, an accident or a terrorist attack and solely for the purpose of identifying unknown persons who are unable to identify themselves or unidentified human remains, query the CIR with the biometric data of those persons.

5 Member States wishing to avail themselves of the possibility provided for in paragraph 2 shall adopt national legislative measures. When doing so, Member States shall take into account the need to avoid any discrimination against third-country nationals. Such legislative measures shall specify the precise purposes of the identification within the purposes referred to in Article 2(1)(b) and (c). They shall designate the competent police authorities and lay down the procedures, conditions and criteria of such checks.

6 Member States wishing to avail themselves of the possibility provided for in paragraph 4 shall adopt national legislative measures laying down the procedures, conditions and criteria.

Article 21

Access to the common identity repository for the detection of multiple identities

1 Where a query of the CIR results in a yellow link in accordance with Article 28(4), the authority responsible for the manual verification of different identities in accordance with Article 29 shall have access, solely for the purpose of that verification, to the data referred to in Article 18(1) and (2) stored in the CIR connected by a yellow link.

2 Where a query of the CIR results in a red link in accordance with Article 32, the authorities referred to in Article 26(2) shall have access, solely for the purposes of combating identity fraud, to the data referred to in Article 18(1) and (2) stored in the CIR connected by a red link.

Article 22

Querying the common identity repository for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences

1 In a specific case, where there are reasonable grounds to believe that consultation of EU information systems will contribute to the prevention, detection or investigation of terrorist offences or other serious criminal offences, in particular where there is a suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offences is a person whose data are stored in Eurodac, the designated authorities and Europol may consult the CIR in order to obtain information on whether data on a specific person are present in Eurodac.

2 Where, in reply to a query the CIR indicates that data on that person are present in Eurodac, the CIR shall provide to designated authorities and Europol a reply in the form of a

***Status:** Point in time view as at 31/01/2020.*
***Changes to legislation:** There are outstanding changes not yet made to Regulation (EU) 2019/818 of the European Parliament and of the Council. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details)*

reference as referred to in Article 18(2) indicating that Eurodac contains matching data. The CIR shall reply in such a way that the security of the data is not compromised.

The reply indicating that data on that person are present in Eurodac shall be used only for the purposes of submitting a request for full access subject to the conditions and procedures laid down in the legal instrument governing such access.

In the event of a match or multiple matches, the designated authority or Europol shall make a request for full access to at least one of the information systems from which a match was generated.

Where exceptionally, such full access is not requested, the designated authorities shall record the justification for not making the request, which shall be traceable to the national file. Europol shall record the justification in the relevant file.

3 Full access to the data contained in Eurodac for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences remains subject to the conditions and procedures laid down in the legal instrument governing such access.

Article 23

Data retention in the common identity repository

1 The data referred to in Article 18(1), (2) and (4) shall be deleted from the CIR in an automated manner in accordance with the data retention provisions of Regulation (EU) 2019/816.

2 The individual file shall be stored in the CIR only for as long as the corresponding data are stored in at least one of the EU information systems whose data are contained in the CIR. The creation of a link shall not affect the retention period of each item of the linked data.

Article 24

Keeping of logs

1 Without prejudice to Article 29 of Regulation (EU) 2019/816, eu-LISA shall keep logs of all data processing operations in the CIR in accordance with paragraphs 2, 3 and 4 of this Article.

2 eu-LISA shall keep logs of all data processing operations pursuant to Article 20 in the CIR. Those logs shall include the following:

a the Member State or Union agency launching the query;
b the purpose of access of the user querying via the CIR;
c the date and time of the query;
d the type of data used to launch the query;
e the results of the query.

3 eu-LISA shall keep logs of all data processing operations pursuant to Article 21 in the CIR. Those logs shall include the following:

a the Member State or Union agency launching the query;
b the purpose of access of the user querying via the CIR;
c the date and time of the query;

d where a link is created, the data used to launch the query and the results of the query indicating the EU information system from which the data were received.

4 eu-LISA shall keep logs of all data processing operations pursuant to Article 22 in the CIR. Those logs shall include the following:

a the date and time of the query;

b the data used to launch the query;

c the results of the query;

d the Member State or Union agency querying the CIR.

The logs of such access shall be regularly verified by the competent supervisory authority in accordance with Article 41 of Directive (EU) 2016/680 or by the European Data Protection Supervisor in accordance with Article 43 of Regulation (EU) 2016/794, at intervals not exceeding six months, to verify whether the procedures and conditions set out in Article 22(1) and (2) of this Regulation are fulfilled.

5 Each Member State shall keep logs of queries that its authorities and the staff of those authorities duly authorised to use the CIR make pursuant to Articles 20, 21 and 22. Each Union agency shall keep logs of queries that its duly authorised staff make pursuant to Articles 21 and 22.

In addition, for any access to the CIR pursuant to Article 22, each Member State shall keep the following logs:

a the national file reference;

b the purpose of access;

c in accordance with national rules, the unique user identity of the official who carried out the query and of the official who ordered the query.

6 In accordance with Regulation (EU) 2016/794, for any access to the CIR pursuant to Article 22 of this Regulation, Europol shall keep logs of the unique user identity of the official who carried out the query and of the official who ordered the query.

7 The logs referred to in paragraphs 2 to 6 may be used only for data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, and for ensuring data security and integrity. Those logs shall be protected by appropriate measures against unauthorised access and erased one year after their creation. If, however, they are required for monitoring procedures that have already begun, they shall be erased once the monitoring procedures no longer require the logs.

8 eu-LISA shall store the logs related to the history of the data, in individual files. eu-LISA shall erase such logs in an automated manner, once the data are erased.

Status:
Point in time view as at 31/01/2020.

Changes to legislation:
There are outstanding changes not yet made to Regulation (EU) 2019/818 of the European Parliament and of the Council. Any changes that have already been made to the legislation appear in the content and are referenced with annotations.