Council of the European Union

Brussels, 6 February 2018
(OR. en)

5758/18

Interinstitutional File:
2017/0351 (COD)

LIMITE

COSI 25	**FAUXDOC 5**
FRONT 24	**COPEN 25**
ASIM 5	**JAI 77**
DAPIX 25	**CT 18**
ENFOPOL 49	**CSCI 15**
ENFOCUSTOM 20	**SAP 1**
SIRIS 7	**COMIX 44**
SCHENGEN 1	**CODEC 156**
DATAPROTECT 10	**IA 40**
VISA 16	

NOTE

From:	Presidency
To:	Delegations
Subject:	Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226 - Examination of Presidency revised text of Articles 1-32

Delegations will find below a Presidency revised text of the proposal for the aforementioned Regulation, based on the outcome of discussions on this proposal by DAPIX: interoperability of EU information systems on 8-9 January 2018 as well as the written drafting suggestions provided by 16 Member States and 1 Schengen Associated Country.

Changes to the Commission proposal are marked in ***bold italics*** and ~~strikethrough~~.

Delegations are invited to note that the corresponding recitals will be adjusted at a later stage.

ANNEX

2017/0351 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226[1]

(…)

CHAPTER I
General provisions

Article 1
Subject matter

1. This Regulation, together with [Regulation 2018/xx on interoperability police and judicial cooperation, asylum and migration], establishes a framework to ensure the interoperability between the Entry/Exit System (EES), the Visa Information System (VIS), [the European Travel Information and Authorisation System (ETIAS)], Eurodac, the Schengen Information System (SIS), and [the European Criminal Records Information System for third-country nationals (ECRIS-TCN)][2] in order for those systems and data to supplement each other.

2. The framework shall include the following interoperability components:

   (a) a European search portal (ESP);

   (b) a shared biometric matching service (shared BMS);

   (c) a common identity repository (CIR);

   (d) a multiple-identity detector (MID).

---

[1] General scrutiny reservations by: **CY, CZ, DE, EE, ES, FI, FR, IT, LT, LV, MT, NL, PL, PT, SE, SK, SI, UK, CH**
PL parliamentary reservation.

[2] **NL** scrutiny reservation on Articles relating to ECRIS-TCN in the interoperability solution.

3. This Regulation also lays down provisions on data quality requirements, on a Universal Message Format (UMF), on a central repository for reporting and statistics (CRRS) and lays down the responsibilities of the Member States and of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), with respect to the design and operation of the interoperability components.

4. This Regulation also adapts the procedures and conditions for Member State ~~law enforcement~~ ***designated*** authorities and for the European Union Agency for Law Enforcement Cooperation (Europol) access to ~~the Entry/Exit System (~~EES~~)~~, ~~the Visa Information System (~~VIS~~)~~, [~~the European Travel Information and Authorisation System (~~ETIAS~~),~~] and Eurodac for the purposes of the prevention, detection ~~and~~ ***or*** investigation of terrorist offences or of other serious criminal offences falling under their competence.

Article 2
Objectives ~~of interoperability~~

1. By ensuring interoperability, this Regulation ~~shall have~~ ***has*** the following objectives:

   (a) to improve the management of the external borders;

   (b) to contribute to preventing and combating irregular migration;

   (c) to contribute to a high level of security within the area of freedom, security and justice of the Union including the maintenance of public security and public policy and safeguarding the security in the territories of the Member States;

   (d) to improve the implementation of the common visa policy; and

   (e) to assist in examining application***s*** for international protection.

2. The objectives ~~of ensuring interoperability~~ ***referred to in paragraph 1*** shall be achieved ***in particular*** by:

   (a) ensuring the correct identification of persons;

   (b) contributing to fighting identity fraud;

   (c) improving and harmonising data quality requirements of the respective EU information systems;

   (d) facilitating the technical and operational implementation by Member States of existing and future EU information systems;

   (e) strengthening and simplifying and making more uniform the data security and data protection conditions that govern the respective EU information systems;

   (f) streamlining the conditions for ~~law enforcement~~ access ***by designated authorities*** to the EES, the VIS, [the ETIAS] and Eurodac;

   (g) supporting the purposes of the EES, the VIS, [the ETIAS], Eurodac, the SIS and [the ECRIS-TCN system].

Article 3
Scope

1. This Regulation applies to ~~[the Entry/Exit System (~~EES~~)]~~, ~~the Visa Information System (~~VIS~~)~~, [~~the European Travel Information and Authorisation System (~~ETIAS~~)~~] and ~~the Schengen Information System (~~SIS~~)~~.

2. This Regulation applies to persons in respect of whom personal data may be processed in the EU information systems referred to in paragraph 1.

Article 4
Definitions

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

(1) ‘external borders’ means external borders as defined in Article 2(2) of Regulation (EU) 2016/399;

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

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

(4) ‘supervisory authorities’ means the supervisory authority established in accordance with Article 51(1) of Regulation (EU) 2016/679 and the supervisory authority established in accordance with Article 41(1) of Directive (EU) 2016/680;

(5) ‘verification’ means the process of comparing sets of data to establish the validity of a claimed identity (one-to-one check);

(6) ‘identification’ means the process of determining a person’s identity through a database search against multiple sets of data (one-to-many check);

(7) ‘third-country national’ means a person who is not a citizen of the Union within the meaning of Article 20(1) of the Treaty, or a stateless person or a person whose nationality is unknown;

(8) ‘alphanumeric data’ means data represented by letters, digits, special characters, spaces and punctuation marks;

(9) ‘identity data’ means the data referred to in Article 27(3)(a) to (h);

(10) ‘fingerprint data’ means the data relating to the fingerprints of an individual;

(11) ‘facial image’ means digital image~~s~~ of the face;

(12) ‘biometric data’ means fingerprint data ~~and/~~or facial image;

(13) ‘biometric template’ means a mathematical representation obtained by feature extraction from biometric data limited to the characteristics necessary to perform identifications and verifications;

(14) ‘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;

(15) ‘travel document data’ means the type, number and country of issuance of the travel document, the date of expiry of the validity of the travel document and the three-letter code of the country issuing the travel document;

~~(16) ‘travel authorisation’ means travel authorisation as defined in Article 3 of the [ETIAS Regulation];~~

~~(17) ‘short-stay visa’ means visa as defined in Article 2(2)(a) of Regulation (EC) No 810/2009;~~

(18) ‘EU information systems’ means the large-scale IT systems managed by eu-LISA;

(19) ‘Europol data’ means personal data provided to Europol for the purpose referred to in Article 18(2)(a) of Regulation (EU) 2016/794;

(20) ‘Interpol databases’ means the Interpol Stolen and Lost Travel Document database (SLTD) and the Interpol Travel Documents Associated with Notices database (Interpol TDAWN);

(21)[3] ‘match’ means the existence of a correspondence established by comparing two or more occurrences of personal data recorded or being recorded in an information system or database;

(22)[4] ‘hit’ means the confirmation of one match or several matches;

(23) 'police authority' means 'competent authority' as defined in Article 3(7) of Directive 2016/680;

(24) ‘designated authorities’ means the Member State designated authorities referred to in Article 29(1) of Regulation (EU) 2017/2226, Article 3(1) of Council Decision 2008/633/JHA, [Article 43 of the ETIAS Regulation] and [Article 6 of the Eurodac Regulation];

---

[3] *NB: This definition is to be aligned with the final definition in the new SIS Regulations.*

[4] *NB: This definition is to be aligned with the final definition in the new SIS Regulations.*

(25) ‘terrorist offence’ means an offence under national law which corresponds or is equivalent to one of the offences referred to in Directive (EU) 2017/541;

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

(27) ***'Entry/Exit System' (***'EES'**)** means the Entry/Exit System as referred to in Regulation (EU) 2017/2226;

(28) ***'Visa Information System' (***'VIS'***)*** means the Visa Information System as referred to in Regulation (EC) No 767/2008;

(29) [***'the European Travel Information and Authorisation System' (***'ETIAS'***)*** means the European Travel Information and Authorisation System as referred to in the ETIAS Regulation];

(30) 'Eurodac' means Eurodac as referred to in the [Eurodac Regulation];

(31) ***'Schengen Information System' (***'SIS'***)*** means the Schengen Information System as referred to [in the Regulation on SIS in the field of border checks, Regulation on SIS in the field of law enforcement and Regulation on SIS in the field of illegal return];

(32) ['ECRIS-TCN System' means ~~the European Criminal Records Information System~~ ***the centralised system for the identification of Member States*** holding conviction information on third-country national***s*** and stateless persons as referred to in the ECRIS-TCN System Regulation];

(33) ***'European search portal' (***'ESP'***)*** means the European search portal as referred to in Article 6;

(34) ***'shared biometric matching service' (***'shared BMS'***)*** means the shared biometric matching service as referred to in Article ~~15~~ ***12***;

(35) ***'common identity repository' (***'CIR'***)*** means the common identity repository as referred to in Article 17;

(36) ***'multiple-identity detector' (***'MID'***)*** means the multiple-identity detector as referred to in Article 25;

(37) ***'central repository for reporting and statistics' (***'CRRS'***)*** means the central repository for reporting and statistics as referred to in Article 39.

(38) 'Universal Message Format' ('UMF') means Universal Message Format as referred to in Article 38.

Article 5
Non-discrimination

Processing of personal data for the purposes of this Regulation shall not result in discrimination against persons on any grounds such as 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
European Search Portal

Article 6
European search portal

1. A European search portal (ESP) is established for the purposes of ensuring that Member State authorities and EU bodies have fast, seamless, efficient, systematic and controlled access to the EU information systems, the Europol data and the Interpol databases that they need to perform their tasks in accordance with their access rights and of supporting the objectives of the EES, the VIS, [the ETIAS], Eurodac, the SIS, [the ECRIS-TCN system] and the Europol data.

2. The ESP shall be composed of:

   (a) a central infrastructure, including a search portal enabling the simultaneous querying of the EES, the VIS, [the ETIAS], Eurodac, the SIS, [the ECRIS-TCN system] as well as of the Europol data and the Interpol databases;

   (b) a secure communication channel between the ESP, Member States and EU bodies that are entitled to use the ESP in accordance with Union law;

   (c) a secure communication infrastructure between the ESP and the EES, the VIS, [the ETIAS], Eurodac, the Central-SIS, [the ECRIS-TCN system], the Europol data and the Interpol databases as well as between the ESP and the central infrastructures of the common identity repository (CIR) and the multiple-identity detector ***(MID)***.

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

Article 7
Use of the European search portal

1. The use of the ESP shall be reserved to the Member State authorities and EU bodies having access to the EES, [the ETIAS], the VIS, the SIS, Eurodac and [the ECRIS-TCN system], to the CIR and the ~~multiple-identity detector~~ ***MID*** as well as the Europol data and the Interpol databases in accordance with Union or national law governing such access.

2. The authorities referred to in paragraph 1 shall use the ESP to search data related to persons or their travel documents in the central systems of the EES, the VIS and [the ETIAS] in accordance with their access rights under Union and national law. They shall also use the ESP to query the CIR in accordance with their access rights under this Regulation for the purposes referred to in Articles 20, 21 and 22.

3. The Member State authorities referred to in paragraph 1 may use the ESP to search data related to persons or their travel documents in the Central SIS referred to in the [Regulation on SIS in the field of border checks ~~and of the Regulation on SIS in the field of law enforcement~~] ***in accordance with their access rights under Union and national law.*** Access to the Central SIS via the ESP shall be established through the national system (N.SIS) of each Member State in accordance with [Article 4(2) of the Regulation on SIS in the field of border checks and of the Regulation on SIS in the field of law enforcement].

4. The EU bodies shall use the ESP to search data related to persons or their travel documents in the Central SIS.

5. The authorities referred to in paragraph 1 may use the ESP to search data related to ~~persons or their~~ travel documents in the Interpol databases in accordance with their access rights under Union and national law.

Article 8
Profiles for the users of the European search portal

1. For the purposes of enabling the use of the ESP, eu-LISA ***in cooperation with Member States*** shall create a profile for each category of user of the ESP in accordance with the technical details and access rights referred to in paragraph 2, including, in accordance with Union and national law:

   (a) the fields of data ~~to be~~ used for querying;

   (b) the EU information systems, the Europol data and the Interpol databases that shall and may be consulted and that shall provide a reply to the user; and

   (c) the ***fields of*** data provided in each reply.

2. The Commission shall adopt delegated acts in accordance with Article 63 to specify the technical details of the profiles referred to in paragraph 1 for the users of the ESP referred to in Article 7(1) in accordance with their access rights.

Article 9
Queries

1. The users of the ESP shall launch a query by introducing ***alphanumeric or biometric*** data in the ESP ~~in accordance with their user profile and access rights~~. Where a query has been launched, the ESP shall query simultaneously, with the data introduced by the user of the ESP ***and in accordance with the user profile and access rights***, the EES, [the ETIAS], the VIS, the SIS, Eurodac, [the ECRIS-TCN system] and the CIR as well as the Europol data and the Interpol databases.

2. The fields of data used to launch a query via the ESP shall correspond to the fields of data related to persons or travel documents that may be used to query the various EU information systems, the Europol data and the Interpol databases in accordance with the legal instruments governing them.

3. eu-LISA***, after consulting the Member States*** shall implement an interface control document (ICD) based on the UMF referred to in Article 38 for the ESP.

4. The EES, [the ETIAS], the VIS, the SIS, Eurodac, [the ECRIS-TCN system], the CIR and the multiple-identity detector, as well as the Europol data *and the Interpol databases*, shall provide the data that they contain resulting from the query of the ESP.

5. When querying the Interpol databases, the design of the ESP shall ensure that the data used by the user of the ESP to launch a query is not shared with the owners of Interpol data.

6. ~~The reply to the~~ ***The*** user of the ESP shall ~~be unique~~ ***receive one reply*** ~~and~~ ***that*** shall contain all the data to which the user has access under Union ***and national*** law. ~~Where necessary, the reply provided by the ESP shall indicate to which information system or database the data belongs~~.

7. The Commission shall adopt a delegated act in accordance with Article 63 to specify the ~~content and~~ format of the ESP replies.

Article 10
Keeping of logs

1. Without prejudice to ~~[~~Article 46 of the ~~EES~~ Regulation ***(EU) 2017/2226***~~]~~, Article 34 of Regulation (EC) No 767/2008, [Article 59 of the ETIAS proposal] and Articles 12 and 18 of the Regulation on SIS in the field of border checks, eu-LISA shall keep logs of all data processing operations within the ESP. Those logs shall include, in particular, the following:

   (a) the Member State authority ***or EU body*** and the ~~individual user of the ESP, including the~~ ESP profile used as referred to in Article 8;

   (b) the date and time of the query;

   (c) the EU information systems and the Interpol databases queried;

   ~~(d) in accordance with national rules or when applicable, Regulation (EU) 45/2001, the identifying mark of the person who carried out the query~~.

2. The logs 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 pursuant to Article 42. Those logs shall be protected by appropriate measures against unauthorised access ***and modifications*** and erased one year after their creation, unless they are required for monitoring procedures that have already begun.

Article 11

Fall-back procedures in case of technical impossibility to use the European search portal

1. Where it is technically impossible to use the ESP to query one or several EU information systems referred to in Article 9(1) or the CIR, because of a failure of the ESP, the users of the ESP shall be notified ***automatically*** by eu-LISA.

2. Where it is technically impossible to use the ESP to query one or several EU information systems referred to in Article 9(1) or the CIR, because of a failure of the national infrastructure in a Member State, that Member State~~'s competent authority~~ shall notify eu-LISA and the Commission.

3. In both scenarios, and until the technical failure is addressed, the obligation referred to in Article 7(2) and (4) shall not apply and Member States ~~may~~ ***shall*** access the information systems referred to in Article 9(1) or the CIR directly using their respective national uniform interfaces or national communication infrastructures.

4. Where it is technically impossible to use the ESP to query one or several EU information systems referred to in Article 9(1) or the CIR, because of a failure of the infrastructure of a EU body, that EU body shall notify eu-LISA and the Commission.

CHAPTER III
Shared Biometric Matching Service

Article 12
Shared biometric matching service

1. A shared biometric matching service (shared BMS) storing biometric templates and enabling querying with biometric data across several EU information systems is established for the purposes of supporting the ***Common Identity Repository (***CIR***)*** and the multiple-identity detector ***(MID)*** and the objectives of the EES, the VIS, Eurodac, the SIS and [the ECRIS-TCN system].

2. The shared BMS shall be composed of:

   (a) a central infrastructure, including a search engine and the storage of the data referred to in Article 13;

   (b) a secure communication infrastructure between the shared BMS, Central-SIS and the CIR.

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

Article 13
Data stored in the shared biometric matching service

1. The shared BMS shall store the biometric templates that it shall obtain from the following biometric data:

   (a) the data referred to in Article 16(1)(d) and Article 17(1)(b) and (c) ***and Article 18(2)(a), (b) and (c) of*** Regulation (EU) 2017/2226;

   (b) the data referred to in Article 9(6) of Regulation (EC) No 767/2008;

   (c) [the data referred to in Article 20(2)(w) and (x) of the Regulation on SIS in the field of border checks;

   (d) ***[***the data referred to in Article 20(3)(w) and ~~(x)~~***(y)*** of the Regulation on SIS in the field of law enforcement***]***;

   (e) ***[***the data referred to in Article 4(3)(t) and (u) of the Regulation on SIS in the field of illegal return];

   (f) [the data referred to in ***Article 12(a) and (b),*** Article 13***(2)***(a) ***and (b) and 14(2)(a) and (b)*** of the Eurodac Regulation;]

   (g) [the data referred to in Article 5(1)(b) and Article 5(2) of the ECRIS-TCN Regulation.]

2. The shared BMS shall include in each biometric template a reference to the information systems in which the corresponding biometric data is stored.

3.[5] Biometric templates shall only be entered in the shared BMS following an automated quality check of the biometric data added to one of the information systems performed by the shared BMS to ascertain the fulfilment of a minimum data quality standard[6].

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

Article 14
Searching biometric data with the shared biometric matching service

In order to search the biometric data stored within the CIR and the SIS, the CIR and the SIS shall use the biometric templates stored in the shared BMS. Queries with biometric data shall take place in accordance with the purposes provided for in this Regulation and in ~~the EES~~ Regulation ***(EU) 2017/2226***, ~~the VIS~~ Regulation ***(EC) No 767/2008***, the Eurodac Regulation, the [SIS Regulations] and [the ECRIS-TCN Regulation].

Article 15

Data retention in the shared biometric matching service

The data referred to in Article 13***(1) and (2)*** shall be stored in the shared BMS for as long as the corresponding biometric data is stored in the CIR or the SIS ***and shall be deleted in an automated manner in accordance with the data retention provisions of Regulation (EU) 2017/2226, Regulation (EC) No 767/2008 and [the SIS Regulation in the field of border management] respectively.***

Article 16
Keeping of logs

1. Without prejudice to ~~[~~Article 46 of ~~the EES~~ Regulation~~]~~ ***(EU) 2017/2226***, Article 34 of Regulation (EC) No 767/2008 and [Article 12 and 18 of the Regulation on SIS in the field of ~~law enforcement~~ ***border checks***], eu-LISA shall keep logs of all data processing operations within the shared BMS. Those logs shall include, in particular, the following:

   (a) the history related to the creation and storage of biometric templates;

   (b) a reference to the EU information systems queried with the biometric templates stored in the shared BMS;

   (c) the date and time of the query;

---

[5] **NL** scrutiny reservation.

[6] *NB: this provision could be further clarified in a recital.*

(d) the type of biometric data used to launch the query;

~~(e) the length of the query;~~

(f) the results of the query and date and time of the result;

(g) ~~in accordance with national rules or, when applicable, Regulation (EU) 45/2001, the identifying mark of the person who carried out the query~~ ***the name of the authority searching biometric data***.

2. The logs 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 pursuant to Article 42. Those logs shall be protected by appropriate measures against unauthorised access ***and modifications*** and erased one year after their creation, unless they are required for monitoring procedures that have already begun. The logs referred to in paragraph 1(a) shall be erased once the data is erased.

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 recorded in the EES, the VIS, [the ETIAS], Eurodac or [the ECRIS-TCN system] containing the data referred to in Article 18, is established for the purpose of facilitating and assisting the correct identification of persons registered in the EES, the VIS, [the ETIAS], the Eurodac and [the ECRIS-TCN system], of supporting the functioning of the multiple-identity detector and of facilitating and streamlining access by ~~law enforcement~~ ***designated*** authorities ***and Europol*** to non-law enforcement information systems at EU level, where necessary for the prevention, ~~investigation,~~ detection ***or investigation*** ~~or prosecution~~ ***of terrorist offences or other*** ~~of~~ serious ~~crime~~ ***criminal offences***.

2. The CIR shall be composed of:

   (a) a central infrastructure that shall replace the central systems of respectively the EES, the VIS, [the ETIAS], Eurodac and [the ECRIS-TCN system] 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 EU bodies that are entitled to use the ~~European search portal (ESP)~~ ***CIR*** in accordance with Union law;

   (c) a secure communication infrastructure between the CIR and the EES, [the ETIAS], the VIS, Eurodac and [the ECRIS-TCN system] as well as with the central infrastructures of the ESP, the shared BMS and the ~~multiple-identity detector~~ ***MID***.

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

4. eu-LISA shall implement an interface control document (ICD) 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 was originated:

   (a) the data referred to in ~~[~~Article 16(1)(a) to (d) and Article 17(1)(a) to (c) ***and Article 18(2)*** of the ~~EES~~ Regulation ***(EU) 2017/2226***~~]~~;

   (b) the data referred to in Article 9(4)(a) to (c), (5) and (6) of Regulation (EC) No 767/2008;

   (c) [the data referred to in Article 15(2)(a) to (e) of the [ETIAS Regulation;]

~~(d) – (not applicable)~~

~~(e) – (not applicable)~~

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 belongs.

2a. 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 belongs.

3. 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 is added, amended or deleted in the EES, the VIS and [the ETIAS], 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 ~~the multiple-identity detector creates~~ a white or red link ***is created in the MID*** in accordance with Articles 32 ~~and~~ ***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. Where a Member State police authority has been so empowered by national legislative measures as referred to in paragraph 2, it may, solely for the purpose of identifying a person, query the CIR with the biometric data of that person taken during an identity check.

   Where the query indicates that data on that person is stored in the CIR, the Member States 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.

2. Member States wishing to avail themselves of the possibility provided for in this Article shall adopt national legislative measures. Such legislative measures shall specify the precise purposes of identity checks within the purposes referred to in Article 2(1)(b) and (c). They shall designate the police authorities competent and lay down the procedures, conditions and criteria of such checks.

Article 21

Access to the common identity repository for the detection of multiple identities[7]

1. Where a query of the CIR results in a yellow link in accordance with Article 28(4), the authority responsible for the verification of different identities determined in accordance with Article 29 shall have access, solely for the purpose of that verification, to the identity data stored in the CIR belonging to the various information systems connected to 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 fighting identity fraud, to the identity data stored in the CIR belonging to the various information systems connected to a red link.

Article 22

Querying the common identity repository for ~~law enforcement~~ purposes ***of preventing, detecting and investigating terrorist offences or other serious criminal offences***

1. For the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences in a specific case and in order to obtain information on whether data on a specific person is present in the EES, the VIS and [the ETIAS] ~~or~~ the Member State designated authorities and Europol may consult the CIR.

2. Member State designated authorities and Europol shall not be entitled to consult data belonging to [the ECRIS-TCN] when consulting the CIR for the purposes listed in paragraph 1.

3. Where, in reply to a query the CIR indicates data on that person is present in the EES, the VIS and [the ETIAS] the CIR shall provide to Member States' designated authorities and Europol a reply in the form of a reference indicating which of the information systems contains matching data referred to in Article 18(2). The CIR shall reply in such a way that the security of the data is not compromised.

4. Full access to the data contained in the EU information systems for the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences remains subject to the conditions and procedures laid down in the respective legislative instruments governing such access.

[7] **NL** scrutiny reservation.

Article 23
Data retention in the common identity repository

1. ***Without prejudice to paragraph 3,*** ~~T~~***t***he data referred to in Article 18(1)***,*** ~~and~~ (2) ***and (2a)*** shall be deleted from the CIR ***in an automated manner*** in accordance with the data retention provisions of ~~[the EES~~ Regulation ***(EU) 2017/2226***~~]~~, ~~the VIS~~ Regulation ***(EC) No 767/2008*** and [the ETIAS Regulation] respectively.

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

3. Where a red link is stored in the MID in accordance with Article 32, the linked data referred to in Article 18(1), (2) and (2a) shall be stored in the CIR for as long as the corresponding data is stored in at least one of the information systems from which the linked data originates.

Article 24
Keeping of logs

1. Without prejudice to ~~[~~Article 46 of ~~the EES~~ Regulation***(EU) 2017/2226***, Article 34 of Regulation (EC) No 767/2008 and [Article 59 of the ETIAS proposal], eu-LISA shall keep logs of all data processing operations within the CIR in accordance with paragraphs 2, 3 and 4.

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

   (a) the purpose of access of the user querying via the CIR;

   (b) the date and time of the query;

   (c) the type of data used to launch the query;

   (d) the results of the query;

   (e) ~~in accordance with national rules or with Regulation (EU) 2016/794 or, when applicable, Regulation (EU) 45/2001, the identifying mark of the person who carried out the query~~ ***the name of the authority querying the CIR***.

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

   (a) the purpose of access of the user querying via the CIR;

   (b) the date and time of the query;

   (c) where ~~relevant~~ ***a link is created***, the data used to launch the query;

(d) where ~~relevant~~ ***a link is created***, the results of the query;

(e) ~~in accordance with national rules or with Regulation (EU) 2016/794 or, when applicable, Regulation (EU) 45/2001, the identifying mark of the person who carried out the query~~ ***the name of the authority querying the CIR***.

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

(a) the national file reference;

(b) the date and time of the query;

(c) the type of data used to launch the query;

(d) the results of the query;

(e) the name of the authority consulting the CIR;

(f) in accordance with national rules or with Regulation (EU) 2016/794 or, when applicable, ~~Regulation (EU) 45/2001~~ [***Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC***], the ~~identifying mark~~ ***unique user identity*** of the official who carried out the query and of the official who ordered the query.

The logs of such access shall be regularly verified by the competent supervisory authority established in accordance with Article 51 of Regulation (EU) 2016/679 or in accordance with Article 41 of Directive 2016/680 ***or in accordance with Article 43 (EDPS) of Regulation 2016/794***, at intervals not exceeding ~~six months~~ ***one year***, to verify whether the procedures and conditions set out in Article 22(1) to (3) are fulfilled.

5. Each Member State shall keep logs of queries of the staff duly authorised to use the CIR pursuant to Articles 20, 21 and 22.

5a. Europol shall keep logs of queries of the staff duly authorised to use the CIR pursuant to Article 22.

6. The logs referred to in paragraphs 1***, 5*** and 5***a*** may be used only for data protection monitoring, including checking the admissibility of a request and the lawfulness of data processing, and for ensuring data security pursuant to Article 42. They shall be protected by appropriate measures against unauthorised access ***and modifications*** and erased one year after their creation, unless they are required for monitoring procedures that have already begun.

7. eu-LISA shall keep the logs related to the history of the data stored in individual file, for purposes defined in paragraph 6. The logs related to the history of the data stored shall be erased once the data is erased.

CHAPTER V
Multiple-identity Detector

Article 25
Multiple-identity detector

1. A multiple-identity detector (MID) creating and storing links between data in the EU information systems included in the common identity repository (CIR) and the SIS and as a consequence detecting multiple identities, with the dual purpose of facilitating identity checks and combating identity fraud, is established for the purpose of supporting the functioning of the CIR and the objectives of the EES, the VIS, the ETIAS], Eurodac, the SIS and [the ECRIS-TCN system].

2. The MID shall be composed of:

   (a) a central infrastructure, storing links and references to information systems;

   (b) a secure communication infrastructure to connect the MID with the SIS and the central infrastructures of the European search portal and the CIR.

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

Article 26
Access to the multiple-identity detector

1. For the purposes of the manual identity verification referred to in Article 29, access to the data referred to in Article 34 stored in the MID shall be granted to:

   (a) border authorities when creating or updating an individual file as provided for in Article 14 of ~~the [EES~~ Regulation ***(EU) 2017/2226***~~]~~;

   (b) competent authorities referred to in Article 6(1) and (2) of Regulation 767/2008 when creating or updating an application file in the VIS in accordance with ~~Article 8 of~~ Regulation (EC) No 767/2008;

   (c) [the ETIAS Central Unit and the ETIAS National Units when carrying out the assessment referred to in Articles 20 and 22 of the ETIAS Regulation;]

   ~~(d) (not applicable);~~

   (e) the SIRENE Bureau~~x~~ of the Member State creating a [SIS alert in accordance with the Regulation on SIS in the field of border checks];

   ~~(f) (not applicable).~~

2. Member State authorities and EU bodies having access to at least one EU information system included in the ~~common identity repository~~ ***CIR*** or to the SIS shall have access to the data referred to in Article 34(a) and (b) regarding any red links as referred to in Article 32.

Article 27
Multiple-identity detection

1. A multiple-identity detection in the ~~common identity repository~~ ***CIR*** and the SIS shall be launched where:

   (a) an individual file is created or updated in ~~[~~the EES in accordance with Article 14 of ~~the EES~~ Regulation ***(EU) 2017/2226***~~]~~;

   (b) an application file is created or updated in the VIS in accordance with ~~Article 8 of~~ Regulation (EC) No 767/2008;

   (c) [an application file is created or updated in the ETIAS in accordance with Article 17 of the ETIAS Regulation;]

   ~~(d) – (not applicable)~~;

   (e) [an alert on a person is created or updated in the SIS in accordance with Chapter V of the Regulation on SIS in the field of border checks];

   ~~(f) – (not applicable).~~

2. Where the data contained within an information system as referred to in paragraph 1 contains biometric data, the common identity repository (CIR) and the Central-SIS shall use the shared biometric matching service (shared BMS) in order to perform the multiple-identity detection. The shared BMS shall compare the biometric templates obtained from any new biometric data to the biometric templates already contained in the shared BMS in order to verify whether or not data belonging to the same third-country national is already stored in the CIR or in the Central SIS.

3. In addition to the process referred to in paragraph 2, the CIR and the Central-SIS shall use the European search portal to search the data stored in ~~the CIR and~~ the Central-SIS ***and the CIR respectively*** using the following data:

   (a) surname (family name); first name(s) (given name(s)); date of birth, sex and nationality(ies) as referred to in Article 16(1)(a) of ~~the [EES~~ Regulation ***(EU) 2017/2226***~~]~~;

   (b) surname (family name); first name(s) (given name(s)); date of birth, sex and nationality(ies) as referred to in Article 9(4)(a) of Regulation (EC) No 767/2008;

   (c) [surname (family name); first name(s) (given name(s)); surname at birth; date of birth, place of birth, sex and nationality(ies) as referred to in Article 15(2) of the ETIAS Regulation;]

   ~~(d) – (not applicable);~~

   (e) [surname(s); forename(s); name(s) at birth, previously used names and aliases; date of birth, place of birth, nationality(ies) and sex as referred to in Article 20(2) of the Regulation on SIS in the field of border checks;]

~~(f) – (not applicable);~~

~~(g) – (not applicable);~~

~~(h) – (not applicable).~~

4. The multiple-identity detection shall only be launched in order to compare data available in one information system with data available in other information systems.

Article 28
Results of the multiple-identity detection

1. Where the queries referred to in Article 27(2) and (3) do not report any hit[8], the procedures referred to in Article 27(1) shall continue in accordance with the respective Regulations governing them.

2. Where the query laid down in Article 27(2) and (3) reports one or several hit(s), the common identity repository and, where relevant, the SIS shall create a link between the data used to launch the query and the data triggering the hit.

   Where several hits are reported, a link shall be created between all data triggering the hit. Where data was already linked, the existing link shall be extended to the data used to launch the query.

3. Where the query referred to in Article 27(2) or (3) reports one or several hit(s) and the identity data of the linked files is identical or similar, a white link shall be created in accordance with Article 33.

4. Where the query referred to in Article 27(2) or (3) reports one or several hit(s) and the identity data of the linked files cannot be considered as similar, a yellow link shall be created in accordance with Article 30 and the procedure referred to in Article 29 shall apply.

5. The Commission shall lay down the procedures to determine the cases where identity data can be considered as identical or similar in implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

6. The links shall be stored in the identity confirmation file referred to in Article 34.

7. The Commission shall lay down the technical rules for ~~linking data~~ ***creating links between data*** from different information systems by implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

[8] *NB: The use of "hit" and "match" in this and subsequent Articles is to be aligned with the definition of these terms in Article 4.*

Article 29
Manual verification of different identities

1. Without prejudice to paragraph 2, the authority responsible for verification of different identities shall be:

   (a) the border authority for hits that occurred when creating or updating an individual ***file*** in ~~[~~the EES in accordance with Article 14 of ~~the EES~~ Regulation ***(EU) 2017/2226***~~]~~;

   (b) the competent authorities referred to in Article 6(1) ~~and (2)~~ of Regulation 767/2008 for hits that occurred when creating or updating an application file in the VIS in accordance with Article 8 of Regulation (EC) No 767/2008;

   (c) [the ETIAS Central Unit and the ETIAS National Units for hits that occurred in accordance with Articles 18, 20 and 22 of the ETIAS Regulation;]

   ~~(d) (not applicable);~~

   (e) the SIRENE Bureau~~x~~ of the Member State for hits that occurred when creating a SIS alert in accordance with the [Regulations on SIS in the field of border checks];

   ~~(f) (not applicable).~~

   The multiple-identity detector shall indicate the authority responsible for the verification of different identities in the identity ~~verification~~ ***confirmation*** file.

2. The authority responsible for the verification of different identities in the identity confirmation file shall be the SIRENE Bureau of the Member State that created the alert where a link is created to data contained:

   (a) in an alert in respect of persons wanted for arrest or for surrender or extradition purposes as referred to in Article 26 of [the Regulation on SIS in the field of law enforcement];

   (b) in an alert on missing or vulnerable persons as referred to in Article 32 of [the Regulation on SIS in the field of law enforcement];

   (c) in an alert on persons sought to assist with a judicial procedure as referred to in Article 34 of [the Regulation on SIS in the field of law enforcement];

   (d) [in an alert on return in accordance with the Regulation on SIS in the field of illegal return];

   (e) in an alert on persons for discreet checks, inquiry checks or specific checks as referred to in Article 36 of [the Regulation on SIS in the field of law enforcement];

   (f) in an alert on unknown wanted persons for identification according to national law and search with biometric data as referred to in Article 40 of [the Regulation on SIS in the field of law enforcement].

3. Without prejudice to paragraph 4, the authority responsible for verification of different identities shall have access to the related data contained in the relevant identity confirmation file and to the identity data linked in the common identity repository and, where relevant, in the SIS, and shall assess the different identities and shall update the link in accordance with Articles 31, 32 and 33 and add it to the identity confirmation file without delay.

4. Where the authority responsible for the verification of different identities in the identity confirmation file is the border authority creating or updating an individual file in the EES in accordance with Article 14 of ~~the EES~~ Regulation ***(EU) 2017/2226***, and where a yellow link is obtained, the border authority shall carry out additional verifications as part of a second-line check. During this second-line check, the border authorities shall have access to the related data contained in the relevant identity confirmation file and shall assess the different identities and shall update the link in accordance with Articles 31 to 33 and add it to the identity confirmation file without delay.

5. Where more than one link is obtained, the authority responsible for the verification of different identities shall assess each link separately.

6. Where data reporting a hit was already linked, the authority responsible for the verification of different identities shall take into account the existing links when assessing the creation of new links.

Article 30
Yellow link

1. A link between data from two or more information systems shall be classified as yellow in any of the following cases:

   (a) the linked data shares the same biometric but different identity data and no manual verification of different identity has taken place;

   (b) the linked data has different identity data and no manual verification of different identity has taken place.

2. Where a link is classified as yellow in accordance with paragraph 1, the procedure laid down in Article 29 applies.

Article 31
Green link

1. A link between data from two or more information systems shall be classified as green where the linked data do not share the same biometric but have similar identity data and the authority responsible for the verification of different identities concluded it refers to two different persons.

2. Where the common identity repository (CIR) or the SIS are queried and where a green link exists between two or more of the information systems constituting the CIR or with the SIS, the multiple-identity detector shall indicate that the identity data of the linked data does not correspond to the same person. The queried information system shall reply indicating only the data of the person whose data was used for the query, without triggering a hit against the data that is subject to the green link.

Article 32
Red link

1. A link between data from two or more information systems shall be classified as red in any of the following cases:

   (a) the linked data shares the same biometric but different identity data and the authority responsible for the verification of different identities concluded it refers unlawfully to the same person;

   (b) the linked data has similar identity data and the authority responsible for the verification of different identities concluded it refers unlawfully to the same person.

2. Where the CIR or the SIS are queried and where a red link exists between two or more of the information systems constituting the CIR or with the SIS, the multiple-identity detector shall reply indicating the data referred to in Article 34. Follow-up to a red link shall take place in accordance with Union and national law.

3. Where a red link is created between data from the EES, the VIS, [the ETIAS], Eurodac or [the ECRIS-TCN System], the individual file stored in the CIR shall be updated in accordance with Article 19~~(1)~~ ***(2)***.

4. Without prejudice to the provisions related to the handling of alerts in the SIS referred to in the [Regulations on SIS in the field of border checks, on SIS in the field of law enforcement and on SIS in the field of illegal return], and without prejudice to limitations necessary to protect security and public order, prevent crime and guarantee that any national investigation will not be jeopardised, where a red link is created, the authority responsible for verification of different identities shall inform the person of the presence of multiple unlawful identities.

5. Where a red link is created, the authority responsible for verification of different identities shall provide a reference to the authorities responsible for the data linked.

6. If a Member State authority has evidence to suggest that a red link recorded in the MID is factually incorrect or that data were processed in the MID, the CIR or the SIS in breach of this Regulation, it shall check the relevant data stored in the CIR and SIS and shall, if necessary, rectify or erase the link from the MID without delay. That Member State authority shall inform the Member State responsible for the manual verification without delay.