Council of the European Union

Brussels, 28 February 2018
(OR. en)

6551/18

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	15729/17 + COR 1
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) - Presidency revised text of provisions specific to this Regulation

Delegations will find below the text containing provisions specific to the aforementioned Regulation (highlighted in yellow), as revised by the Presidency on the basis of the outcome of discussions on those provisions by DAPIX: interoperability of EU information systems on 22-23 January 2018 as well as written drafting suggestions provided by Member States.

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

Delegations are invited to note that only provisions highlighted in yellow have been amended in this document. The provisions which are common to both interoperability Regulations and which have already been amended in the Regulation relating to borders and visa would be reproduced in this Regulation at a later stage.

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

2017/==0352== (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on establishing a framework for interoperability between EU information systems (==police and judicial cooperation, asylum and migration==)

(…)

CHAPTER I
General provisions

Article 1
Subject matter

1.   This Regulation, together with [Regulation 2018/xx on interoperability ==borders and visa==], 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)] in order for those systems and data to supplement each other.

(…)

Article 3
Scope

1.   This Regulation applies to ==Eurodac,== the Schengen Information System (SIS) ==and [the European Criminal Records Information System for third-country nationals (ECRIS-TCN)].==

2.   ==This Regulation also applies to the Europol data to the extent of enabling querying it simultaneously to the EU information systems referred to in paragraph 1 in accordance with Union law.==

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

CHAPTER II
European Search Portal

(…)

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 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 Eurodac and [the ECRIS-TCN system] 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]. 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 Europol data in accordance with their access rights under Union and national law.

(…)

Article 10
Keeping of logs

1.   Without prejudice to [Article 39 of the Eurodac Regulation], [Articles 12 and 18 of the Regulation on SIS in the field of law enforcement], *[Article 13 of the Regulation on SIS in the field of illegal return]*, [Article 29 of the ECRIS-TCN Regulation] and Article 40 of Regulation (EU) 2016/794, 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 Europol data queried;

   (d)   ~~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.~~

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 erased one year after their creation, unless they are required for monitoring procedures that have already begun.

(…)

CHAPTER III
Shared Biometric Matching Service

(…)

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) 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) 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 13(a) 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.   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.

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

(…)

Article 16
Keeping of logs

1.   Without prejudice to [Article 39 of the Eurodac Regulation], [Article 12 and 18 of the Regulation on SIS in the field of law enforcement] and [Article 29 of the ECRIS-TCN Regulation], 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;

(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 with Regulation (EU) 2016/794 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 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 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)   (not applicable);

(b)   (not applicable);

(c)   (not applicable);

(d)   [the data referred to in Article *12(2)(a) to (e), (g) and (h), Article* 13*(2)*(a) to (e), (g) and (h) *and Article 14(2)(a) to (e), (g) and (h)* of the [Eurodac Regulation;]

(e)   [the data referred to in Article 5(1)(b) and 5(2) and the following data of Article 5(1)(a) of the ECRIS-TCN Regulation: surname or family name; first name(s) (given name(s)); sex; date of birth; place and country of birth; nationality or nationalities; gender and where applicable previous names, pseudonyms(s) and/or alias name(s).]

2.   For each set of data referred to in paragraph 1, the CIR shall include a reference to the 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 Eurodac or [the ECRIS-TCN system], 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 in accordance with Articles 32 and 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 22
Querying the common identity repository for law enforcement purposes

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 Eurodac, 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 Eurodac 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.

Article 23
Data retention in the common identity repository

1.   The data referred to in Article 18(1) and (2) shall be deleted from the CIR in accordance with the data retention provisions of [the ==Eurodac== Regulation] and [the ==ECRIS-TCN== 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.

Article 24
Keeping of logs

1.   Without prejudice to [==Article 39 of the Eurodac Regulation==] and [==Article 29 of the ECRIS-TCN Regulation==], eu-LISA shall keep logs of all data processing operations within the CIR in accordance with paragraphs 2, 3 and 4.

(…)

CHAPTER V
Multiple-identity Detector

(…)

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)   – (not applicable);~~

~~(b)   – (not applicable);~~

~~(c)   – (not applicable);~~

(d)   the authorities competent to assess a request for international protection provided for in the Eurodac Regulation when assessing a new request for international protection;

(da)   the authorities competent to collect the data of a third country national or stateless person apprehended in connection with the irregular crossing of an external border provided for in the Eurodac Regulation when creating or updating data in the Eurodac;

(db)   the authorities competent to collect the data of a third country national or stateless person found illegally staying in a Member State provided for in the Eurodac Regulation when creating or updating data in the Eurodac;

(e)   the SIRENE Bureaux of the Member State creating a *or updating an alert in accordance with* [Regulation on SIS in the field of law enforcement or Regulation on SIS in the field of illegal return];

(f)   [the central authorities of the convicting Member State when recording or updating data in the ECRIS-TCN system in accordance with Article 5 of the ECRIS-TCN Regulation.]

2.   Member State authorities and EU bodies having access to at least one EU information system included in *the common identity repository 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 and the SIS shall be launched where:

(a)   (not applicable);

(b)   (not applicable);

(c)   (not applicable);

(d)   [an application for international protection *data* is created *added* or updated *modified* in Eurodac in accordance with Article*s* 10 *12, 13 or 14* of the Eurodac Regulation];

(e)   [an alert on a person is created or updated in the SIS in accordance with Chapters VI, VII, VIII and IX of the Regulation on SIS in the field of law enforcement and Article 3 of the Regulation on SIS in the field of illegal return];

(f)   [a data record is created or updated in the ECRIS-TCN system in accordance with Article 5 of the ECRIS-TCN Regulation.]

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 using the following data:

(a)   – (not applicable);

(b)   (not applicable);

(c)   (not applicable);

(d)   [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 12 of the Eurodac Regulation];

(e)   – (not applicable);

(f)   [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(3) of the Regulation on SIS in the field of law enforcement;]

(g)   [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 4 of the Regulation on SIS in the field of illegal return;]

(h)   [surname (family name); first name(s) (given names); date of birth, place of birth, nationality(ies) and gender as referred to in Article 5(1)(a) of the ECRIS-TCN Regulation.]

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 29
Manual verification of different identities

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

(a)   – (not applicable);

(b)   (not applicable);

(c)   (not applicable);

(d) the authority assessing a request for international protection as provided for in the Eurodac Regulation for hits that occurred when assessing such request;

(da) *the authority competent to collect the data of a third country national or stateless person apprehended in connection with the irregular crossing of an external border provided for in the Eurodac Regulation for hits that occurred when creating or updating data in the Eurodac;*

(db) *the authority competent to collect the data of a third country national or stateless person found illegally staying in a Member State provided for in the Eurodac Regulation for hits that occurred when creating or updating data in the Eurodac;*

(e) the SIRENE Bureaux of the Member State for hits that occurred when creating a SIS alert in accordance with the [Regulations on SIS in the field of law enforcement and on SIS in the field of illegal return];

(f) the central authorities of the convicting Member State for hits that occurred when recording or updating data in the ECRIS-TCN system in accordance with Article 5 of the [ECRIS-TCN Regulation].

The multiple-identity detector shall indicate the authority responsible for the verification of different identities in the identity verification 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.   ~~(not applicable).~~

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.

(…)

CHAPTER VI
Measures supporting interoperability

Article 37
Data quality

1.   eu-LISA shall establish automated data quality control mechanisms and procedures on the data stored in the SIS, Eurodac, [the ECRIS-TCN system], the shared biometric matching service (shared BMS), the common identity repository (CIR) and the multiple-identity detector (MID).

2.   eu-LISA shall establish common data quality indicators and the minimum quality standards to store data in the SIS, Eurodac, [the ECRIS-TCN system], the shared BMS, the CIR and the MID.

3.   eu-LISA shall provide regular reports on the automated data quality control mechanisms and procedures and the common data quality indicators to the Member States. eu-LISA shall also provide a regular report to the Commission covering the issues encountered and the Member States concerned.

4.   The details of the automated data quality control mechanisms and procedures and the common data quality indicators and the minimum quality standards to store data in the SIS, Eurodac, [the ECRIS-TCN system], the shared BMS, the CIR and the MID, in particular regarding biometric data, shall be laid down in implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

5.   One year after the establishment of the automated data quality control mechanisms and procedures and common data quality indicators and every year thereafter, the Commission shall evaluate Member State implementation of data quality and shall make any necessary recommendations. The Member States shall provide the Commission with an action plan to remedy any deficiencies identified in the evaluation report and shall report on any progress against this action plan until it is fully implemented. The Commission shall transmit the evaluation report to the European Parliament, to the Council, to the European Data Protection Supervisor and to the European Union Agency for Fundamental Rights established by Council Regulation (EC) No 168/2007.[1]

Article 38
Universal Message Format

1.   The Universal Message Format (UMF) standard is hereby established. The UMF defines standards for certain content elements of cross-border information exchange between information systems, authorities and/or organisations in the field of Justice and Home affairs

2.   The UMF standard shall be used in the development of the [Eurodac], the [ECRIS-TCN system], the European search portal, the CIR, the MID and, if appropriate, in the development by eu-LISA or any other EU body of new information exchange models and information systems in the area of Justice and Home Affairs.

3.   The implementation of the UMF standard may be considered in the SIS and in any existing or new cross-border information exchange models and information systems in the area of Justice and Home Affairs, developed by Member States or associated countries.

4.   The Commission shall adopt an implementing act to lay down and develop the UMF standard referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

---

[1]   Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights (OJ L 53, 22.2.2007, p. 1).

Article 39
Central repository for reporting and statistics

1.   A central repository for reporting and statistics (CRRS) is established for the purposes of supporting the objectives of Eurodac, the SIS and [the ECRIS-TCN system] and to generate cross-system statistical data and analytical reporting for policy, operational and data quality purposes.

2.   eu-LISA shall establish, implement and host the CRRS in its technical sites containing the data referred to in [Article 42(8) of the Eurodac Regulation], [Article 71 of the Regulation on SIS in the field of law enforcement] and [Article 30 of the ECRIS-TCN Regulation] logically separated. The data contained in the CRRS shall not enable the identification of individuals. Access to the repository shall be granted by means of secured access through the Trans- European Services for Telematics between Administrations (TESTA) network service with control of access and specific user profiles, solely for the purpose of reporting and statistics, to the authorities referred to in [Article 42(8) of the Eurodac Regulation], [Article 71 of the Regulation on SIS in the field of law enforcement] and [Article 30 of the ECRIS-TCN Regulation].

3.   eu-LISA shall render the data anonymous and shall record such anonymous data in the CRRS. The process for rendering the data anonymous shall be automated.

4.   The CRRS shall be composed of:

    (a)   a central infrastructure, consisting of a data repository enabling the rendering of anonymous data;

    (b)   a secure communication infrastructure to connect the CRRS to the SIS, Eurodac and [the ECRIS-TCN], as well as the central infrastructures of the shared BMS, the CIR and the MID.

5.   The Commission shall lay down detailed rules on the operation of the CRRS, including specific safeguards for processing of personal data referred to under paragraph 2 and 3 and security rules applicable to the repository by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

CHAPTER VII
Data protection

Article 40
Data controller

1. In relation to the processing of data in the shared biometric matching service (shared BMS), the Member State authorities that are controllers for the Eurodac, SIS and [the ECRIS-TCN system] respectively, shall also be considered as controllers in accordance with Article 4(7) of Regulation (EU) 2016/679 in relation to the biometric templates obtained from the data referred to in Article 13 that they enter into respective systems and shall have responsibility for the processing of the biometric templates in the shared BMS.

2. In relation to the processing of data in the common identity repository (CIR), the Member State authorities that are controllers for the Eurodac and [the ECRIS-TCN system] respectively, shall also be considered as controllers in accordance with Article 4(7) of Regulation (EU) 2016/679 in relation to data referred to in Article 18 that they enter into respective systems and shall have responsibility for the processing of that personal data in the CIR.

3. In relation to the processing of data in the multiple-identity detector:

    (a) the European Border and Coast Guard Agency shall be considered a data controller in accordance with Article 2(b) of Regulation No 45/2001 in relation to processing of personal data by the ETIAS Central Unit;

    (b) the Member State authorities adding or modifying the data in the identity confirmation file are also to be considered as controllers in accordance with Article 4(7) of Regulation (EU) 2016/679 and shall have responsibility for the processing of the personal data in the multiple-identity detector;

(…)

Article 46
Right of information

1.   Without prejudice to the right of information referred to in Articles 11 and 12 of Regulation (EC) 45/2001 and Articles 13 and 14 of Regulation (EU) 2016/679, persons whose data are stored in the shared biometric matching service, the common identity repository or the multiple-identity detector shall be informed by the authority collecting their data, at the time their data are collected, about the processing of personal data for the purposes of this Regulation, including about identity and contact details of the respective data controllers, and about the procedures for exercising their rights of access, rectification and erasure, as well as about the contact details of the European Data Protection Supervisor and of the national supervisory authority of the Member State responsible for the collection of the data.

2.   Persons whose data is recorded in Eurodac or [the ECRIS-TCN system] shall be informed about the processing of data for the purposes of this Regulation in accordance with paragraph 1 when:

(a)   (not applicable);

(b)   (not applicable);

(c)   (not applicable);

(d)   [an application for international protection *data* is *added* created or updated *modified* in Eurodac in accordance with Article*s* 10 *12, 13 or 14* of the Eurodac Regulation];

(e)   [a data record is created or updated in the ECRIS-TCN system in accordance with Article 5 of the ECRIS-TCN Regulation.]

(…)

Article 48
Communication of personal data to third countries, international organisations and private parties

Personal data stored in or accessed by the interoperability components shall not be transferred or made available to any third country, to any international organisation or to any private party.

(…)

CHAPTER VIII
Responsibilities

Article 52
Responsibilities of eu-LISA during the design and development phase

1. eu-LISA shall ensure that the central infrastructures of the interoperability components are operated in accordance with this Regulation.

2. The interoperability components 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 referred to in Article 53(1).

3. eu-LISA shall be responsible for the development of the interoperability components, for any adaptations required for establishing interoperability between the central systems of the EES, VIS, [ETIAS], SIS, and Eurodac, and [the ECRIS-TCN system], and the European search portal, the shared biometric matching service, the common identity repository and the multiple-identity detector.

   eu-LISA shall define the design of the physical architecture of the interoperability components including their communication infrastructures and the technical specifications and their evolution as regards the central infrastructure and the secure communication infrastructure, 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 SIS, Eurodac or [ECRIS-TCN system] deriving from the establishment of interoperability and provided for by this Regulation.

   eu-LISA shall develop and implement the interoperability components as soon as possible after the entry into force of this Regulation and the adoption by the Commission of the measures provided for in Articles 8(2), 9(7), 28(5) and (6), 37(4), 38(4), 39(5) and 44(5).

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

(…)

Article 54a
Responsibilities of Europol

1. Europol shall ensure processing of the queries by the ESP to the Europol data and shall accordingly adapt its Querying Europol Systems (QUEST) interface for basic protection level (BPL) data.

2. Europol shall be responsible for the management of, and arrangements for, its duly authorised staff to use and access respectively the ESP and the CIR in accordance with this Regulation and the creation and regular update of a list of those staff and their profiles.

(…)

CHAPTER IX
Final provisions

Article 56
Reporting and statistics

1. The duly authorised staff of the competent authorities of Member States, the Commission and eu-LISA shall have access to consult the following data related to the European search portal (ESP), solely for the purposes of reporting and statistics without enabling individual identification:

    (a) number of queries per user of the ESP profile;

    (b) — (not applicable).

2. The duly authorised staff of the competent authorities of Member States, the Commission and eu-LISA shall have access to consult the following data related to the common identity repository, solely for the purposes of reporting and statistics without enabling individual identification:

    (a) number of queries for the purposes of Articles 20, 21 and 22;

    (b) nationality, sex and year of birth of the person;

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

    (d) the number of searches conducted with and without biometric data.

3. The duly authorised staff of the competent authorities of Member States, the Commission and eu-LISA shall have access to consult the following data related to the multiple-identity detector, solely for the purposes of reporting and statistics without enabling individual identification:

    (a) nationality, sex and year of birth of the person;

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

    (b) the number of searches conducted with and without biometric data;

    (c) the number of each type of link.

4.   The duly authorised staff of the European Border and Coast Guard Agency established by Regulation (EU) 2016/1624 of the European Parliament and of the Council[2] shall have access to consult the data referred to in paragraphs 1, 2 and 3 for the purpose of carrying out risk analyses and vulnerability assessments as referred to in Articles 11 and 13 of that Regulation.

5.   For the purpose of paragraph 1 of this Article, eu-LISA shall store the data referred to in paragraph 1 of this Article in the central repository for reporting and statistics referred to in Chapter VII of this Regulation. The data included in the repository shall not enable the identification of individuals, but it shall allow the authorities listed in paragraph 1 of this Article to obtain customisable reports and statistics to enhance the efficiency of border checks, to help authorities processing visa applications and to support evidence-based policymaking on migration and security in the Union.

(…)

Article 58
Transitional period applicable to the provisions on access to the common identity repository for law enforcement purposes

Article 22 shall apply from the date of the start of operations referred to in Article 62(1).

Article 59
Transitional period for the multiple-identity detection

1.   For a period of one year following the notification by eu-LISA of the completion of the test referred to in Article 62(1)(b) regarding the multiple-identity detector (MID) and before the start of operations of the MID, the ETIAS Central Unit as referred to in [Article 33(a) of Regulation (EU) 2016/1624] shall be responsible for carrying out a multiple-identity detection between the data stored in the VIS, Eurodac and the SIS. The multiple-identity detections shall be carried out using only biometric data in accordance with Article 27(2) of this Regulation.

---

[2]   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 (OJ L 251, 16.9.2016, p. 1).

2. Where the query 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.

Where the query 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.

Where several hits are reported, a link shall be created to each piece of data triggering the hit.

3. Where a yellow link is created ~~in accordance with paragraph 3~~, the MID shall grant access to the identity data present in the different information systems to the ETIAS Central Unit.

4. Where a link is created to an alert in the SIS, other than a refusal of entry alert or an alert on a travel document reported lost, stolen or invalidated in accordance with Article 24 of the Regulation on SIS in the field of border checks and Article 38 of the Regulation on SIS in the field of law enforcement respectively, the MID shall grant access to the identity data present in the different information systems to the SIRENE Bureau of the Member State that created the alert.

5. The ETIAS Central Unit or the SIRENE Bureau of the Member State that created the alert shall have access to the data contained in the identity confirmation file 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.

6. eu-LISA shall assist where necessary the ETIAS Central Unit in carrying out the multiple-identity detection referred to in this Article.

(…)

Article 68
Monitoring and evaluation

1. eu-LISA shall ensure that procedures are in place to monitor the development of the interoperability components in light of objectives relating to planning and costs and to monitor the functioning of the interoperability components 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 interoperability components, eu-LISA shall submit a report to the European Parliament and the Council on the state of play of the development of the interoperability components. 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 interoperability components.

4.   Four years after the start of operations of each interoperability component and every four years thereafter, eu-LISA shall submit to the European Parliament, the Council and the Commission a report on the technical functioning of the interoperability components, including the security thereof.

5.   In addition, one year after each report from eu-LISA, the Commission shall produce an overall evaluation of the components, including:

        (a)   an assessment of the application of this Regulation;

        (b)   an examination of the results achieved against objectives and the impact on fundamental rights;

        (c)   an assessment of the continuing validity of the underlying rationale of the interoperability components;

        (d)   an assessment of the security of the interoperability components;

        (e)   an assessment of any implications, including any disproportionate impact on the flow of traffic at border crossing points and those with a budgetary impact on the Union budget.

        The evaluations shall include any necessary recommendations. The Commission shall transmit the evaluation report to the European Parliament, to the Council, to the European Data Protection Supervisor and to the European Union Agency for Fundamental Rights established by Council Regulation (EC) No 168/2007.[3]

6.   The Member States and Europol shall provide eu-LISA 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 shall provide the Commission with the information necessary to produce the evaluations referred to in paragraph 5.

---

[3]   Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights (OJ L 53, 22.2.2007, p. 1).

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 common identity repository 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 the Eurodac Regulation;

   (c)   the number of requests for access to the common identity repository for law enforcement purposes;

   (d)   the number and type of cases that 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 State and Europol annual reports shall be transmitted to the Commission by 30 June of the subsequent year.

(…)

_____