Official Journal of the European Union

L 135

Volume 62

English edition

Legislation

22 May 2019

Contents

EN

Acts whose titles are printed in light type are those relating to day-to-day management of agricultural matters, and are generally valid for a limited period.

The titles of all other acts are printed in bold type and preceded by an asterisk.

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2019/816 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 17 April 2019

establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty of the Functioning of the European Union, and in particular Article 82(1), second subparagraph, point (d) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Acting in accordance with the ordinary legislative procedure ([1]),

Whereas:

(1) The Union has set itself the objective of offering its citizens an area of freedom, security and justice without internal frontiers, in which the free movement of persons is ensured. That objective should be achieved by means of, among others, appropriate measures to prevent and combat crime, including organised crime and terrorism.

(2) That objective requires that information on convictions handed down in the Member States be taken into account outside the convicting Member State in the course of new criminal proceedings, as laid down in Council Framework Decision 2008/675/JHA ([2]), as well as in order to prevent new offences.

(3) That objective presupposes the exchange of information extracted from criminal records between the competent authorities of the Member States. Such an exchange of information is organised and facilitated by the rules set out in Council Framework Decision 2009/315/JHA ([3]) and by the European Criminal Records Information System (ECRIS), established by Council Decision 2009/316/JHA ([4]).

(4) The existing ECRIS legal framework, however, does not sufficiently address the particularities of requests concerning third-country nationals. Although it is already possible to exchange information on third-country nationals through ECRIS, there is no common Union procedure or mechanism in place to do so efficiently, rapidly and accurately.

(5) Within the Union, information on third-country nationals is not gathered as it is for nationals of Member States — in the Member States of nationality — but only stored in the Member States where the convictions have been handed down. A complete overview of the criminal history of a third-country national can therefore be ascertained only if such information is requested from all Member States.

([1]) Position of the European Parliament of 12 March 2019 (not yet published in the Official Journal) and decision of the Council of 9 April 2019.

([2]) Council Framework Decision 2008/675/JHA of 24 July 2008 on taking account of convictions in the Member States of the European Union in the course of new criminal proceedings (OJ L 220, 15.8.2008, p. 32).

([3]) Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States (OJ L 93, 7.4.2009, p. 23).

([4]) Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA (OJ L 93, 7.4.2009, p. 33).

(6) Such 'blanket requests' impose a disproportionate administrative burden on all Member States, including those not holding information on the particular third-country national. In practice, that burden deters Member States from requesting information on third-country nationals from other Member States, which seriously hinders the exchange of information between them, limiting their access to criminal records information to information stored in their national register. As a consequence, the risk of information exchange between Member States being inefficient and incomplete is increased, which in turn affects the level of security and safety provided to citizens and persons residing within the Union.

(7) To improve the situation, a system should be established by which the central authority of a Member State can find out promptly and efficiently which other Member States hold criminal records information on a third-country national ('ECRIS-TCN'). The existing ECRIS framework could then be used to request the criminal records information from those Member States in accordance with Framework Decision 2009/315/JHA.

(8) This Regulation should therefore lay down rules establishing a centralised system at the Union level containing personal data, and rules on the division of responsibilities between the Member State and the organisation responsible for the development and maintenance of the centralised system, as well as any specific data protection provisions needed to supplement the existing data protection arrangements and to provide for an adequate overall level of data protection, data security and protection of the fundamental rights of the persons concerned.

(9) The objective of offering to citizens of the Union an area of freedom, security and justice without internal frontiers, in which the free movement of persons is ensured, also requires complete information to be held on convictions of citizens of the Union who also hold the nationality of a third country. Given the possibility that those persons could present themselves as holding one or several nationalities, and that different convictions could be stored in the convicting Member State or in the Member State of nationality, it is necessary to include citizens of the Union who also hold the nationality of a third country within the scope of this Regulation. The exclusion of such persons would result in the information stored in ECRIS-TCN being incomplete. That would jeopardise the reliability of the system. However, since such persons hold Union citizenship, the conditions under which fingerprint data can be included in ECRIS-TCN in respect of those persons should be comparable to the conditions under which the fingerprint data of Union citizens are exchanged between Member States through ECRIS, which was established by Framework Decision 2009/315/JHA and Decision 2009/316/JHA. Therefore, in respect of citizens of the Union who also hold the nationality of a third country, fingerprint data should only be included in ECRIS-TCN where they have been collected in accordance with national law during criminal proceedings, it being understood that for such inclusion Member States should be able to use fingerprint data collected for purposes other than criminal proceedings, where such use is permitted under national law.

(10) ECRIS-TCN should allow for processing of fingerprint data for the purpose of identifying the Member States in possession of criminal records information on a third-country national. It should also allow for processing of facial images in order to confirm his or her identity. It is essential that the entry and use of fingerprint data and facial images not exceed what is strictly necessary to achieve the aim, respect fundamental rights, as well as the best interests of children, and be in conformity with applicable Union data protection rules.

(11) The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) established by Regulation (EU) 2018/1726 of the European Parliament and of the Council ([5]) should be entrusted with the task of developing and operating ECRIS-TCN, given its experience with managing other large scale systems in the area of justice and home affairs. Its mandate should be amended to reflect those new tasks.

(12) eu-LISA should be equipped with the appropriate funding and staffing to meet its responsibilities under this Regulation.

(13) Given the need to create close technical links between ECRIS-TCN and ECRIS, eu-LISA should also be entrusted with the task of further developing and maintaining the ECRIS reference implementation, and its mandate should be amended to reflect this.

(14) Four Member States have developed their own national ECRIS implementation software in accordance with Decision 2009/316/JHA, and have been using it instead of the ECRIS reference implementation to exchange criminal records information. Given the particular features that those Member States have introduced in their systems for national use and the investments that they have made, they should be allowed to use their national ECRIS implementation software for the purposes of ECRIS-TCN as well, provided that the conditions set out in this Regulation are met.

([5]) Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011 (OJ L 295, 21.11.2018, p. 99).

(15) ECRIS-TCN should contain only the identity information of third-country nationals convicted by a criminal court within the Union. Such identity information should include alphanumeric and fingerprint data. It should also be possible for facial images to be included in as far as the law of the Member State where a conviction is handed down allows for the collection and storage of facial images of a convicted person.

(16) The alphanumeric data to be entered by the Member States into the central system should include the surname (family name) and the first names (given names) of the convicted person, as well as, where such information is available to the central authority, any pseudonyms or aliases of that person. If differing personal data, such as a different spelling of a name in another alphabet, are known to the Member State concerned, it should be possible to enter such data into the central system as additional information.

(17) The alphanumeric data should also include, as additional information, the identity number, or the type and number of the person's identification documents, as well as the name of the authority issuing those documents, where such information is available to the central authority. The Member State should seek to verify the authenticity of identification documents before entering the relevant information in the central system. In any case, given that such information could be unreliable, it should be used cautiously.

(18) The central authorities should use ECRIS-TCN to identify the Member States holding criminal records information on a third-country national when criminal records information on that person is requested in the Member State concerned for the purposes of criminal proceedings against that person, or for the purposes referred to in this Regulation. While ECRIS-TCN should in principle be used in all such cases, the authority responsible for conducting the criminal proceedings should be able to decide that ECRIS-TCN should not be used when it would not be appropriate in the circumstances of the case, e.g. in certain types of urgent criminal proceedings, in cases of transit, when criminal records information has recently been obtained via ECRIS, or in respect of minor offences, in particular minor traffic offences, minor offences in relation to general municipal regulations and minor public order offences.

(19) Member States should also be able to use ECRIS-TCN for purposes other than those set out in this Regulation, if provided for under and in accordance with national law. However, in order to enhance the transparency of the use of ECRIS-TCN, Member States should notify such other purposes to the Commission, which should ensure publication of all the notifications in the *Official Journal of the European Union*.

(20) It should also be possible for other authorities requesting criminal records information to decide that ECRIS-TCN should not be used when this would not be appropriate in the circumstances of the case, e.g. when certain standard administrative checks need to be carried out regarding the professional qualifications of a person, especially if it is known that criminal records information will not be requested from other Member States, irrespective of the result of the search in ECRIS-TCN. However, ECRIS-TCN should always be used when the request for criminal records information has been initiated by a person who asks for information on his or her own criminal record in accordance with Framework Decision 2009/315/JHA, or when it is made in order to obtain criminal records information in accordance with Directive 2011/93/EU of the European Parliament and of the Council ([6]).

(21) Third-country nationals should have the right to obtain information in writing concerning their own criminal record in accordance with the law of the Member State where they request such information to be provided and in accordance with Framework Decision 2009/315/JHA. Before providing such information to a third-country national, the Member State concerned should query ECRIS-TCN.

(22) Citizens of the Union who also hold the nationality of a third country will only be included in ECRIS-TCN if the competent authorities are aware that such persons hold the nationality of a third country. Where the competent authorities are not aware that citizens of the Union also hold the nationality of a third country, it is nevertheless possible that such persons have prior convictions as third-country nationals. In order to ensure that the competent authorities have a complete overview of criminal records, it should be possible to query ECRIS-TCN to verify whether, in respect of a citizen of the Union, any Member State holds criminal record information concerning this person as a third-country national.

(23) In the event that there is a match between data recorded in the central system and those used for search by a Member State (hit), the identity information against which a hit was recorded should be provided together with the hit. The result of a search should be used by the central authorities only for the purpose of making a request through ECRIS or by the European Union Agency for Criminal Justice Cooperation (Eurojust) established by

([6]) Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).

Regulation (EU) 2018/1727 of the European Parliament and of the Council ([7]), the European Union Agency for Law Enforcement Cooperation (Europol) established by Regulation (EU) 2016/794 of the European Parliament and of the Council ([8]), and the European Public Prosecutor's Office (the 'EPPO') established by Council Regulation (EU) 2017/1939 ([9]), only for the purpose of making a request for conviction information as referred to in this Regulation.

(24) In the first instance, facial images included in ECRIS-TCN should only be used for the purpose of confirming the identity of a third-country national in order to identify the Member States holding information on previous convictions of that third-country national. In the future, it should be possible for facial images to be used for automated biometric matching, provided that the technical and policy requirements to do so have been met. The Commission, taking into account necessity and proportionality, as well as the technical developments in the field of facial recognition software, should assess the availability and readiness of the required technology before adopting a delegated act concerning the use of facial images for the purpose of identifying third-country nationals in order to identify the Member States holding information on previous convictions concerning those persons.

(25) The use of biometrics is necessary as it is the most reliable method of identifying third-country nationals within the territory of the Member States, who are often not in possession of documents or any other means of identification, as well as for more reliable matching of third-country nationals' data.

(26) Member States should enter in the central system fingerprint data of convicted third-country nationals that have been collected in accordance with national law during criminal proceedings. In order to have as complete identity information as possible available in the central system, Member States should also be able to enter into the central system fingerprint data that have been collected for other purposes than criminal proceedings, where those fingerprint data are available for use in criminal proceedings in compliance with national law.

(27) This Regulation should establish minimum criteria as regards the fingerprint data that Member States should include in the central system. Member States should be given the choice either to enter the fingerprint data of third-country nationals who have received a custodial sentence of at least 6 months, or to enter the fingerprint data of third-country nationals who have been convicted of a criminal offence which is punishable under the law of the Member State concerned by a custodial sentence of a maximum period of at least 12 months.

(28) Member States should create records in ECRIS-TCN regarding convicted third-country nationals. This should, where possible, be done automatically and without undue delay after their conviction was entered into the national criminal records. Member States should, in accordance with this Regulation, enter into the central system alphanumeric and fingerprint data relating to convictions handed down after the date of the start of entry of data into the ECRIS-TCN. As from the same date, and any time thereafter, Member States should be able to enter facial images in the central system.

(29) Member States should also, in accordance with this Regulation, create records in ECRIS-TCN regarding third-country nationals convicted prior to the date of start of entry of data, in order to ensure the maximum effectiveness of the system. However, for that purpose Member States should not be obliged to collect information which is not already in their criminal records prior to the date of start of entry of data. The fingerprint data of third-country nationals collected in connection with such prior convictions should be included only where they have been collected during criminal proceedings, and where the Member State concerned considers that they can be clearly matched with other identity information in criminal records.

(30) Improving the exchange of information on convictions should assist Member States in their implementation of Framework Decision 2008/675/JHA, which obliges the Member States to take account of previous convictions in other Member States in the course of new criminal proceedings to the extent that previous national convictions are taken into account under national law.

([7]) Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA (OJ L 295, 21.11.2018, p. 138).

([8]) Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).

([9]) Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO') (OJ L 283, 31.10.2017, p. 1).

(31) A hit indicated by ECRIS-TCN should not of itself be taken to mean that the third-country national concerned has been convicted in the Member States that are indicated. The existence of previous convictions should only be confirmed based on information received from the criminal records of the Member States concerned.

(32) Notwithstanding the possibility of using the Union's financial programmes in accordance with the applicable rules, each Member State should bear its own costs arising from the implementation, administration, use and maintenance of its criminal records database and national fingerprints databases, and from the implementation, administration, use and maintenance of the technical alterations necessary to be able to use ECRIS-TCN, including their connections to the national central access point.

(33) Eurojust, Europol and the EPPO should have access to ECRIS-TCN for the purpose of identifying the Member States holding criminal records information on a third-country national in order to support their statutory tasks. Eurojust should also have direct access to ECRIS-TCN for the purpose of carrying out its task under this Regulation of acting as a contact point for third countries and international organisations, without prejudice to the application of principles of judicial cooperation in criminal matters, including rules on mutual legal assistance. While the position of Member States who are not part of the enhanced cooperation on the establishment of the EPPO should be taken into account, the EPPO should not be refused access to conviction information on the sole ground that the Member State concerned is not part of that enhanced cooperation.

(34) This Regulation establishes strict rules on access to ECRIS-TCN and the necessary safeguards, including the responsibility of the Member States in collecting and using the data. It also sets out how individuals may exercise their rights to compensation, access, rectification, erasure and redress, in particular the right to an effective remedy and the supervision of processing operations by public independent authorities. It therefore respects fundamental rights and freedoms enshrined, in particular, in the Charter of Fundamental Rights of the European Union, including the right to protection of personal data, the principle of equality before the law and the general prohibition of discrimination. In this regard, it also takes into account the European Convention for the Protection of Human Rights and Fundamental Freedoms, the International Covenant on Civil and Political Rights, and other human rights obligations under international law.

(35) Directive (EU) 2016/680 of the European Parliament and of the Council ([10]) should apply to the processing of personal data by competent national authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Regulation (EU) 2016/679 of the European Parliament and of the Council ([11]) should apply to the processing of personal data by national authorities when such processing does not fall within the scope of Directive (EU) 2016/680. Coordinated supervision should be ensured in accordance with Regulation (EU) 2018/1725 of the European Parliament and of the Council ([12]), which should also apply to the processing of personal data by eu-LISA.

(36) In respect of prior convictions, the central authorities should enter alphanumeric data by the end of the period for entry of data under this Regulation, and fingerprint data within two years after the date of the start of operations of ECRIS-TCN. Member States should be able to enter all data at the same time, provided those time limits are met.

(37) Rules should be laid down on the liability of the Member States, Eurojust, Europol, the EPPO and eu-LISA in respect of damage arising from any breach of this Regulation.

(38) In order to improve identification of the Member States holding information on previous convictions of third-country nationals, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union (TFEU) should be delegated to the Commission in respect of supplementing this Regulation by providing for the use of facial images for the purpose of identifying third-country nationals in order to identify the Member States holding information on previous convictions. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement

([10]) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

([11]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

([12]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons 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 (OJ L 295, 21.11.2018, p. 39).

of 13 April 2016 on Better Law-Making ([13]). In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(39) In order to ensure uniform conditions for the establishment and operational management of ECRIS-TCN, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and the Council ([14]).

(40) Member States should take the necessary measures to comply with this Regulation as soon as possible so as to ensure the proper functioning of ECRIS-TCN, taking into account the time that eu-LISA needs to develop and implement ECRIS-TCN. However, Member States should have at least 36 months after the entry into force of this Regulation to take measures to comply with this Regulation.

(41) Since the objective of this Regulation, namely to enable the rapid and efficient exchange of accurate criminal records information on third-country nationals, cannot be sufficiently achieved by the Member States, but can rather, by putting in place common rules, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary to achieve that objective.

(42) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the TEU and to the TFEU, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(43) In accordance with Articles 1 and 2 and Article 4a(1) of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the TEU and to the TFEU, and without prejudice to Article 4 of that Protocol, Ireland is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(44) In accordance with Article 3 and Article 4a(1) of Protocol No 21, the United Kingdom has notified its wish to take part in the adoption and application of this Regulation.

(45) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council ([15]) and delivered an opinion on 12 December 2017 ([16]),

HAVE ADOPTED THIS REGULATION:

CHAPTER I

General provisions

Article 1

Subject matter

This Regulation establishes:

(a) a system to identify the Member States holding information on previous convictions of third-country nationals ('ECRIS-TCN');

(b) the conditions under which ECRIS-TCN shall be used by the central authorities in order to obtain information on such previous convictions through the European Criminal Records Information System (ECRIS) established by Decision 2009/316/JHA, as well as the conditions under which Eurojust, Europol and the EPPO shall use ECRIS-TCN.

([13]) OJ L 123, 12.5.2016, p. 1.
([14]) Regulation (EU) No 182/2011 of the European Parliament and the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).
([15]) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).
([16]) OJ C 55, 14.2.2018, p. 4.

Article 2

Scope

This Regulation applies to the processing of identity information of third-country nationals who have been subject to convictions in the Member States for the purpose of identifying the Member States where such convictions were handed down. With the exception of point (b)(ii) of Article 5(1), the provisions of this Regulation that apply to third-country nationals also apply to citizens of the Union who also hold the nationality of a third country and who have been subject to convictions in the Member States.

Article 3

Definitions

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

(1) 'conviction' means any final decision of a criminal court against a natural person in respect of a criminal offence, to the extent that the decision is entered in the criminal records of the convicting Member State;

(2) 'criminal proceedings' means the pre-trial stage, the trial stage and the execution of the conviction;

(3) 'criminal record' means the national register or registers recording convictions in accordance with national law;

(4) 'convicting Member State' means the Member State in which a conviction is handed down;

(5) 'central authority' means an authority designated in accordance with Article 3(1) of Framework Decision 2009/315/JHA;

(6) 'competent authorities' means the central authorities and Eurojust, Europol and the EPPO, which are competent to access or query ECRIS-TCN in accordance with this Regulation;

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

(8) 'central system' means the database or databases developed and maintained by eu-LISA which hold identity information on third-country nationals who have been subject to convictions in the Member States;

(9) 'interface software' means the software hosted by the competent authorities allowing them to access the central system through the communication infrastructure referred to in point (d) of Article 4(1);

(10) 'identity information' means alphanumeric data, fingerprint data and facial images that are used to establish a connection between these data and a natural person;

(11) 'alphanumeric data' means data represented by letters, digits, special characters, spaces and punctuation marks;

(12) 'fingerprint data' means the data relating to plain and rolled impressions of the fingerprints of each of a person's fingers;

(13) 'facial image' means a digital image of a person's face;

(14) 'hit' means a match or matches established by comparison between identity information recorded in the central system and the identity information used for a search;

(15) 'national central access point' means the national connection point to the communication infrastructure referred to in point (d) of Article 4(1);

(16) 'ECRIS reference implementation' means the software developed by the Commission and made available to the Member States for the exchange of criminal records information through ECRIS;

(17) 'national supervisory authority' means an independent public authority which is established by a Member State pursuant to applicable Union data protection rules;

(18) 'supervisory authorities' means the European Data Protection Supervisor and the national supervisory authorities.

Article 4

Technical architecture of ECRIS-TCN

1. ECRIS-TCN shall be composed of:

(a) a central system in which identity information on convicted third-country nationals is stored;

(b) a national central access point in each Member State;

(c) interface software enabling the connection of the competent authorities to the central system via the national central access points and the communication infrastructure referred to in point (d);

(d) a communication infrastructure between the central system and the national central access points.

2. The central system shall be hosted by eu-LISA at its technical sites.

3. The interface software shall be integrated with the ECRIS reference implementation. The Member States shall use the ECRIS reference implementation or, in the situation and under the conditions set out in paragraphs 4 to 8, the national ECRIS implementation software to query ECRIS-TCN and to send subsequent requests for criminal records information.

4. The Member States which use their national ECRIS implementation software shall be responsible for ensuring that their national ECRIS implementation software allows their national criminal records authorities to use ECRIS-TCN, with the exception of the Interface Software, in accordance with this Regulation. For that purpose, they shall, before the date of start of operations of ECRIS-TCN in accordance with Article 35(4), ensure that their national ECRIS implementation software functions in accordance with the protocols and technical specifications established in the implementing acts referred to in Article 10, and with any further technical requirements established by eu-LISA pursuant to this Regulation based on those implementing acts.

5. For as long as they do not use the ECRIS reference implementation, Member States which use their national ECRIS implementation software shall also ensure the implementation of any subsequent technical adaptations to their national ECRIS implementation software required by any changes to the technical specifications established in the implementing acts referred to in Article 10, or changes to any further technical requirements established by eu-LISA pursuant to this Regulation based on those implementing acts, without undue delay.

6. The Member States which use their national ECRIS implementation software shall bear all the costs associated with the implementation, maintenance and further development of their national ECRIS implementation software and its interconnection with ECRIS-TCN, with the exception of the interface software.

7. If a Member State which uses its national ECRIS implementation software is unable to comply with its obligations under this Article, it shall be obliged to use the ECRIS reference implementation, including the integrated interface software, to make use of ECRIS-TCN.

8. In view of the assessment to be carried out by the Commission pursuant to point (b) of Article 36(10), the Member States concerned shall provide the Commission with all necessary information.

CHAPTER II

Entry and use of data by central authorities

Article 5

Data entry in ECRIS-TCN

1. For each convicted third-country national, the central authority of the convicting Member State shall create a data record in the central system. The data record shall include:

(a) as concerns alphanumeric data:

(i) information to be included unless, in individual cases, such information is not known to the central authority (obligatory information):

— surname (family name),

— first names (given names),

— date of birth,

— place of birth (town and country),

— nationality or nationalities,

— gender,

— previous names, if applicable,

— the code of the convicting Member State,

(ii) information to be included if it has been entered in the criminal record (optional information):

— parents' names,

(iii) information to be included if it is available to the central authority (additional information):

— identity number, or the type and number of the person's identification documents, as well as the name of the issuing authority,

— pseudonyms or aliases;

(b) as concerns fingerprint data:

(i) fingerprint data that have been collected in accordance with national law during criminal proceedings;

(ii) as a minimum, fingerprint data collected on the basis of either of the following criteria:

— where the third-country national has received a custodial sentence of at least 6 months;

or

— where the third-country national has been convicted of a criminal offence which is punishable under the law of the Member State by a custodial sentence of a maximum period of at least 12 months.

2. The fingerprint data referred to in point (b) of paragraph 1 of this Article shall have the technical specifications for the quality, resolution and processing of fingerprint data provided for in the implementing act referred to in point (b) of Article 10(1). The reference number of the fingerprint data of the convicted person shall include the code of the convicting Member State.

3. The data record may also contain facial images of the convicted third-country national, if the law of the convicting Member State allows for the collection and storage of facial images of convicted persons.

4. The convicting Member State shall create the data record automatically, where possible, and without undue delay after the conviction has been entered into the criminal records.

5. The convicting Member States shall also create data records for convictions handed down prior to the date of start of entry of data in accordance with Article 35(1) to the extent that data related to convicted persons are stored in their national databases. In those cases, fingerprint data shall be included only where they have been collected during criminal proceedings in accordance with national law, and where they can be clearly matched with other identity information in criminal records.

6. In order to comply with the obligations set out in points (b)(i) and (ii) of paragraph 1, and in paragraph 5, Member States may use fingerprint data collected for purposes other than criminal proceedings, where such use is permitted under national law.

Article 6

Facial images

1. Until the entry into force of the delegated act provided for in paragraph 2, facial images may be used only to confirm the identity of a third-country national who has been identified as a result of an alphanumeric search or a search using fingerprint data.

2. The Commission is empowered to adopt delegated acts in accordance with Article 37 supplementing this Regulation concerning the use of facial images for the purpose of identifying third-country nationals in order to identify the Member States holding information on previous convictions concerning such persons, when it becomes technically possible. Before exercising this empowerment, the Commission, taking into account necessity and proportionality, as well as technical developments in the field of facial recognition software, shall assess the availability and readiness of the required technology.

Article 7

Use of ECRIS-TCN for identifying the Member States holding criminal records information

1. The central authorities shall use ECRIS-TCN to identify the Member States holding criminal records information on a third-country national in order to obtain information on previous convictions through ECRIS, when criminal records information on that person is requested in the Member State concerned for the purposes of criminal proceedings against that person, or for any of the following purposes, if provided for under and in accordance with national law:

— checking a person's own criminal record at his or her request,

— security clearance,

— obtaining a licence or permit,

— employment vetting,

— vetting for voluntary activities involving direct and regular contacts with children or vulnerable persons,

— visa, acquisition of citizenship and migration procedures, including asylum procedures, and

— checks in relation with public contracts and public examinations.

However, in specific cases other than those in which a third-country national asks the central authority for information on his or her own criminal record, or where the request is made in order to obtain criminal records information pursuant to Article 10(2) of Directive 2011/93/EU, the authority requesting criminal records information may decide that such use of ECRIS-TCN is not appropriate.

2. Any Member State which decides, if provided for under and in accordance with national law, to use ECRIS-TCN for purposes other than those set out in paragraph 1 in order to obtain information on previous convictions through ECRIS, shall, by the date of start of operations as referred to in Article 35(4), or any time thereafter, notify the Commission of such other purposes and any changes to such purposes. The Commission shall publish such notifications in the *Official Journal of the European Union* within 30 days of receipt of the notifications.

3. Eurojust, Europol and the EPPO are entitled to query ECRIS-TCN to identify the Member States holding criminal records information on a third-country national in accordance with Articles 14 to 18. However, they shall not enter, rectify or erase any data in ECRIS-TCN.

4. For the purposes referred to in paragraphs 1, 2 and 3, the competent authorities may also query ECRIS-TCN to verify whether, in respect of a citizen of the Union, any Member State holds criminal records information concerning this person as a third-country national.

5. When querying ECRIS-TCN, the competent authorities may use all or only some of the data referred to in Article 5(1). The minimum set of data that is required to query the system shall be specified in an implementing act adopted in accordance with point (g) of Article 10(1).

6. The competent authorities may also query ECRIS-TCN using facial images, provided that such functionality has been implemented in accordance with Article 6(2).

7. In the event of a hit, the central system shall automatically provide the competent authority with information on the Member States holding criminal records information on the third-country national, along with the associated reference numbers and any corresponding identity information. Such identity information shall only be used for the purpose of verifying the identity of the third-country national concerned. The result of a search in the central system may only be used for the purpose of making a request according to Article 6 of Framework Decision 2009/315/JHA or a request referred to in Article 17(3) of this Regulation.

8. In the event that there is no hit, the central system shall automatically inform the competent authority.

CHAPTER III

Retention and modification of the data

Article 8

Retention period for data storage

1. Each data record shall be stored in the central system for as long as the data related to the convictions of the person concerned are stored in the criminal records.

2. Upon expiry of the retention period referred to in paragraph 1, the central authority of the convicting Member State shall erase the data record, including any fingerprint data or facial images, from the central system. The erasure shall be done automatically, where possible, and in any event no later than one month after the expiry of the retention period.

Article 9

Modification and erasure of data

1. The Member States may modify or erase the data which they have entered into ECRIS-TCN.

2. Any modification of the information in the criminal records which led to the creation of a data record in accordance with Article 5 shall include identical modification of the information stored in that data record in the central system by the convicting Member State without undue delay.

3. If a convicting Member State has reason to believe that the data it has recorded in the central system are inaccurate or that data were processed in the central system in contravention of this Regulation, it shall:

(a) immediately launch a procedure for checking the accuracy of the data concerned or the lawfulness of its processing, as appropriate;

(b) if necessary, rectify the data or erase them from the central system without undue delay.

4. If a Member State other than the convicting Member State which entered the data has reason to believe that data recorded in the central system are inaccurate or that data were processed in the central system in contravention of this Regulation, it shall contact the central authority of the convicting Member State without undue delay.

The convicting Member State shall:

(a) immediately launch a procedure for checking the accuracy of the data concerned or the lawfulness of its processing, as appropriate;

(b) if necessary, rectify the data or erase them from the central system without undue delay;

(c) inform the other Member State that the data have been rectified or erased, or of the reasons why the data have not been rectified or erased, without undue delay.

CHAPTER IV

Development, operation and responsibilities

Article 10

Adoption of implementing acts by the Commission

1. The Commission shall adopt the implementing acts necessary for the technical development and implementation of ECRIS-TCN as soon as possible, and in particular acts concerning:

(a) the technical specifications for the processing of the alphanumeric data;

(b) the technical specifications for the quality, resolution and processing of fingerprint data;

(c) the technical specifications of the interface software;

(d) the technical specifications for the quality, resolution and processing of facial images for the purposes of and under the conditions set out in Article 6;

(e) data quality, including a mechanism for and procedures to carry out data quality checks;

(f) entering the data in accordance with Article 5;

(g) accessing and querying ECRIS-TCN in accordance with Article 7;

(h) modifying and erasing the data in accordance with Articles 8 and 9;

(i) keeping and accessing logs in accordance with Article 31;

(j) operation of the central repository and the data security and data protection rules applicable to the repository, in accordance with Article 32;

(k) providing statistics in accordance with Article 32;

(l) performance and availability requirements of ECRIS-TCN, including minimal specifications and requirements on the biometric performance of ECRIS-TCN in particular in terms of the required false positive identification rate and false negative identification rate.

2. The implementing acts referred to in paragraph 1 shall be adopted in accordance with the examination procedure referred to in Article 38(2).

Article 11

Development and operational management of ECRIS — TCN

1. eu-LISA shall be responsible for the development of ECRIS-TCN in accordance with the principle of data protection by design and by default. In addition, eu-LISA shall be responsible for the operational management of ECRIS-TCN. The development shall consist of the elaboration and implementation of the technical specifications, testing and overall project coordination.

2. eu-LISA shall also be responsible for the further development and maintenance of the ECRIS reference implementation.

3. eu-LISA shall define the design of the physical architecture of ECRIS-TCN including its technical specifications and evolution as regards the central system, the national central access point and the interface software. That design shall be adopted by its Management Board, subject to a favourable opinion of the Commission.

4. eu-LISA shall develop and implement ECRIS-TCN as soon as possible after the entry into force of this Regulation and following the adoption by the Commission of the implementing acts provided for in Article 10.

5. Prior to the design and development phase of ECRIS-TCN, the Management Board of eu-LISA shall establish a Programme Management Board composed of ten members.

The Programme Management Board shall be composed of eight members appointed by the Management Board, the Chair of the Advisory Group referred to in Article 39 and one member appointed by the Commission. The members appointed by the Management Board shall be elected only from those Member States which are fully bound under Union law by the legislative instruments governing ECRIS and which will participate in ECRIS-TCN. The Management Board shall ensure that the members it appoints to the Programme Management Board have the necessary experience and expertise in the development and management of IT systems supporting judicial and criminal records authorities.

eu-LISA shall participate in the work of the Programme Management Board. To that end, representatives of eu-LISA shall attend the meetings of the Programme Management Board in order to report on work regarding the design and development of ECRIS-TCN and on any other related work and activities.

The Programme Management Board shall meet at least once every three months, and more often when necessary. It shall ensure the adequate management of the design and development phase of ECRIS-TCN and shall ensure consistency between central and national ECRIS-TCN projects, and national ECRIS implementation software. The Programme Management Board shall submit written reports regularly and if possible every month to the Management Board of eu-LISA on the progress of the project. The Programme Management Board shall have no decision-making power nor any mandate to represent the members of the Management Board.

6. The Programme Management Board shall establish its rules of procedure which shall include in particular rules on:

(a) chairmanship;

(b) meeting venues;

(c) preparation of meetings;

(d) admission of experts to the meetings;

(e) communication plans ensuring that non-participating Members of the Management Board are kept fully informed.

7. The chairmanship of the Programme Management Board shall be held by a Member State which is fully bound under Union law by the legislative instruments governing ECRIS and the legislative instruments governing the development, establishment, operation and use of all the large-scale IT systems managed by eu-LISA.

8. All travel and subsistence expenses incurred by the members of the Programme Management Board shall be paid by eu-LISA. Article 10 of the eu-LISA Rules of Procedure shall apply *mutatis mutandis*. The Programme Management Board's secretariat shall be ensured by eu-LISA.

9. During the design and development phase, the Advisory Group referred to in Article 39 shall be composed of the national ECRIS-TCN project managers and chaired by eu-LISA. During the design and development phase it shall meet regularly, if possible at least once a month, until the start of operations of ECRIS-TCN. It shall report after each meeting to the Programme Management Board. It shall provide the technical expertise to support the tasks of the Programme Management Board and shall follow up on the state of preparation of the Member States.

10. In order to ensure the confidentiality and integrity of data stored in ECRIS-TCN at all times, eu-LISA shall, in cooperation with the Member States, provide for appropriate technical and organisational measures, taking into account the state of the art, the cost of implementation and the risks posed by the processing.

11. eu-LISA shall be responsible for the following tasks related to the communication infrastructure referred to in point (d) of Article 4(1):

(a) supervision;

(b) security;

(c) the coordination of relations between the Member States and the provider of the communication infrastructure.

12. The Commission shall be responsible for all other tasks relating to the communication infrastructure referred to in point (d) of Article 4(1), in particular:

(a) tasks relating to the implementation of the budget;

(b) acquisition and renewal;

(c) contractual matters.

13. eu-LISA shall develop and maintain a mechanism and procedures for carrying out quality checks on the data stored in ECRIS-TCN and shall provide regular reports to the Member States. eu-LISA shall provide regular reports to the Commission covering the issues encountered and the Member States concerned.

14. The operational management of ECRIS-TCN shall consist of all the tasks necessary to keep ECRIS-TCN operational in accordance with this Regulation, and in particular the maintenance work and technical developments necessary to ensure that ECRIS-TCN functions at a satisfactory level in accordance with the technical specifications.

15. eu-LISA shall perform tasks related to providing training on the technical use of ECRIS-TCN and the ECRIS reference implementation.

16. Without prejudice to Article 17 of the Staff Regulations of Officials of the European Union, laid down in Council Regulation (EEC, Euratom, ECSC) No 259/68 ([17]), eu-LISA shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality to its entire staff required to work with data registered in the central system. That obligation shall also apply after such staff leave office or employment or after the termination of their activities.

Article 12

Responsibilities of the Member States

1. Each Member State shall be responsible for:

(a) ensuring a secure connection between its national criminal records and fingerprints databases and the national central access point;

(b) the development, operation and maintenance of the connection referred to in point (a);

(c) ensuring a connection between its national systems and the ECRIS reference implementation;

([17]) OJ L 56, 4.3.1968, p. 1.

(d) the management of and arrangements for access of duly authorised staff of the central authorities to ECRIS-TCN in accordance with this Regulation and for establishing and regularly updating a list of such staff and the profiles referred to in point (g) of Article 19(3).

2. Each Member State shall give the staff of its central authority who have a right to access ECRIS-TCN appropriate training covering, in particular, data security and data protection rules and applicable fundamental rights, before authorising them to process data stored in the central system.

Article 13

Responsibility for the use of data

1. In accordance with applicable Union data protection rules, each Member State shall ensure that the data recorded in ECRIS-TCN are processed lawfully, and in particular that:

(a) only duly authorised staff have access to the data for the performance of their tasks;

(b) the data are collected lawfully in a manner that fully respects the human dignity and fundamental rights of the third-country national;

(c) the data are entered into ECRIS-TCN lawfully;

(d) the data are accurate and up-to-date when they are entered into ECRIS-TCN.

2. eu-LISA shall ensure that ECRIS-TCN is operated in accordance with this Regulation, with the delegated act referred to in Article 6(2) and with the implementing acts referred to in Article 10, as well as in accordance with Regulation (EU) 2018/1725. In particular, eu-LISA shall take the necessary measures to ensure the security of the central system and the communication infrastructure referred to in point (d) of Article 4(1), without prejudice to the responsibilities of each Member State.

3. eu-LISA shall inform the European Parliament, the Council and the Commission as well as the European Data Protection Supervisor as soon as possible of the measures it takes pursuant to paragraph 2 in view of the start of operations of ECRIS-TCN.

4. The Commission shall make the information referred to in paragraph 3 available to the Member States and to the public through a regularly updated public website.

Article 14

Access for Eurojust, Europol, and the EPPO

1. Eurojust shall have direct access to ECRIS-TCN for the purpose of the implementation of Article 17, as well as for fulfilling its tasks under Article 2 of Regulation (EU) 2018/1727, in order to identify the Member States holding information on previous convictions of third-country nationals.

2. Europol shall have direct access to ECRIS-TCN for the purpose of fulfilling its tasks under points (a) to (e) and (h) of Article 4(1) of Regulation (EU) 2016/794, in order to identify the Member States holding information on previous convictions of third-country nationals.

3. The EPPO shall have direct access to ECRIS-TCN for the purpose of fulfilling its tasks under Article 4 of Regulation (EU) 2017/1939, in order to identify the Member States holding information on previous convictions of third-country nationals.

4. Following a hit indicating the Member States holding criminal records information on a third-country national, Eurojust, Europol, and the EPPO may use their respective contacts with the national authorities of those Member States to request the criminal records information in the manner provided for in their respective founding acts.

Article 15

Access by authorised staff of Eurojust, Europol and the EPPO

Eurojust, Europol and the EPPO shall be responsible for the management of and arrangements for access of duly authorised staff to ECRIS-TCN in accordance with this Regulation and for establishing and regularly updating a list of such staff and their profiles.

Article 16

Responsibilities of Eurojust, Europol and the EPPO

Eurojust, Europol and the EPPO shall:

(a) establish the technical means to connect to ECRIS-TCN and be responsible for maintaining that connection;

(b) provide appropriate training covering, in particular, data security and data protection rules and applicable fundamental rights to those members of their staff who have a right to access ECRIS-TCN before authorising them to process data stored in the central system;

(c) ensure that the personal data processed by them under this Regulation is protected in accordance with the applicable data protection rules.

Article 17

Contact point for third countries and international organisations

1. Third countries and international organisations may, for the purposes of criminal proceedings, address requests for information on which Member States, if any, hold criminal records information on a third-country national to Eurojust. To that end, they shall use the standard form set out in the Annex to this Regulation.

2. When Eurojust receives a request under paragraph 1, it shall use ECRIS-TCN to identify which Member States, if any, hold criminal records information on the third-country national concerned.

3. If there is a hit, Eurojust shall ask the Member State that holds criminal records information on the third-country national concerned whether it consents to Eurojust informing the third country or the international organisation of the name of the Member State concerned. Where that Member State gives its consent, Eurojust shall inform the third country or the international organisation of the name of that Member State, and of how it can introduce a request for extracts from the criminal records with that Member State in accordance with the applicable procedures.

4. In cases where there is no hit or where Eurojust cannot provide an answer in accordance with paragraph 3 to requests made under this Article, it shall inform the third country or international organisation concerned that it has completed the procedure, without providing any indication of whether criminal records information on the person concerned is held by one of the Member States.

Article 18

Providing information to a third country, international organisation or private party

Neither Eurojust, Europol, the EPPO nor any central authority shall transfer or make available to a third country, an international organisation or a private party information obtained from ECRIS-TCN concerning a third-country national. This Article shall be without prejudice to Article 17(3).

Article 19

Data Security

1. eu-LISA shall take the necessary measures to ensure the security of ECRIS-TCN, without prejudice to the responsibilities of each Member State, taking the security measures specified in paragraph 3 into consideration.

2. As regards the operation of ECRIS-TCN, eu-LISA shall take the necessary measures in order to achieve the objectives set out in paragraph 3, including the adoption of a security plan and a business continuity and disaster recovery plan, and to ensure that installed systems may, in case of interruption, be restored.

3. The Member States shall ensure the security of the data before and during the transmission to and receipt from the national central access point. In particular, each Member State shall:

(a) physically protect data, including by making contingency plans for the protection of infrastructure;

(b) deny unauthorised persons access to national installations in which the Member State carries out operations related to ECRIS-TCN;

(c) prevent the unauthorised reading, copying, modification or removal of data media;

(d) prevent the unauthorised input of data and the unauthorised inspection, modification or erasure of stored personal data;

(e) prevent the unauthorised processing of data in ECRIS-TCN and any unauthorised modification or erasure of data processed in ECRIS-TCN;

(f) ensure that persons authorised to access ECRIS-TCN have access only to the data covered by their access authorisation, by means of individual user identities and confidential access modes only;

(g) ensure that all authorities with a right of access to ECRIS-TCN create profiles describing the functions and responsibilities of persons who are authorised to enter, rectify, erase, consult and search the data and make their profiles available to the national supervisory authorities without undue delay at their request;

(h) ensure that it is possible to verify and establish to which Union bodies, offices and agencies personal data may be transmitted using data communication equipment;

(i) ensure that it is possible to verify and establish what data have been processed in ECRIS-TCN, when, by whom and for what purpose;

(j) prevent the unauthorised reading, copying, modification or erasure of personal data during the transmission of personal data to or from ECRIS-TCN or during the transport of data media, in particular by means of appropriate encryption techniques;

(k) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to self-monitoring and supervision to ensure compliance with this Regulation.

4. eu-LISA and the Member States shall cooperate in order to ensure a coherent data security approach based on a security risk management process encompassing the entire ECRIS-TCN.

Article 20

Liability

1. Any person who, or any Member State which, has suffered material or non-material damage as a result of an unlawful processing operation or any other act incompatible with this Regulation shall be entitled to receive compensation from:

(a) the Member State which is responsible for the damage suffered; or

(b) eu-LISA, where eu-LISA has not complied with its obligations set out in this Regulation or in Regulation (EU) 2018/1725.

The Member State which is responsible for the damage suffered or eu-LISA, respectively, shall be exempted from liability, in whole or in part, if it proves that it is not responsible for the event which gave rise to the damage.

2. If any failure of a Member State, Eurojust, Europol, or the EPPO to comply with its obligations under this Regulation causes damage to ECRIS-TCN, that Member State, Eurojust, Europol, or the EPPO, respectively, shall be held liable for such damage, unless and insofar as eu-LISA or another Member State participating in ECRIS-TCN failed to take reasonable measures to prevent the damage from occurring or to minimise its impact.

3. Claims for compensation against a Member State for the damage referred to in paragraphs 1 and 2 shall be governed by the law of the defendant Member State. Claims for compensation against eu-LISA, Eurojust, Europol and the EPPO for the damage referred to in paragraphs 1 and 2 shall be governed by their respective founding acts.

Article 21

Self-monitoring

Member States shall ensure that each central authority takes the measures necessary to comply with this Regulation and cooperates, where necessary, with the supervisory authorities.

Article 22

Penalties

Any misuse of data entered in ECRIS-TCN shall be subject to penalties or disciplinary measures, in accordance with national or Union law, that are effective, proportionate and dissuasive.

CHAPTER V

Data protection rights and supervision

Article 23

Data controller and data processor

1. Each central authority is to be considered as data controller in accordance with applicable Union data protection rules for the processing of the personal data by that central authority's Member State under this Regulation.

2. eu-LISA shall be considered as data processor in accordance with Regulation (EU) 2018/1725 as regards the personal data entered into the central system by the Member States.

Article 24

Purpose of the processing of personal data

1. The data entered into the central system shall only be processed for the purpose of the identification of the Member States holding the criminal records information on third-country nationals.

2. With the exception of duly authorised staff of Eurojust, Europol and the EPPO who have access to ECRIS-TCN for the purposes of this Regulation, access to ECRIS-TCN shall be reserved exclusively to duly authorised staff of the central authorities. Access shall be limited to the extent needed for the performance of the tasks in accordance with the purpose referred to in paragraph 1, and to what is necessary and proportionate to the objectives pursued.

Article 25

Right of access, rectification, erasure and restriction of processing

1. The requests of third-country nationals concerning the rights of access to personal data, to rectification and erasure and to restriction of processing of personal data which are set out in the applicable Union data protection rules may be addressed to the central authority of any Member State.

2. Where a request is made to a Member State other than the convicting Member State, the Member State to which the request has been made shall forward it to the convicting Member State without undue delay and in any event within 10 working days of receiving the request. Upon receipt of the request, the convicting Member State shall:

(a) immediately launch a procedure for checking the accuracy of the data concerned and the lawfulness of its processing in ECRIS-TCN; and

(b) respond to the Member State that forwarded the request without undue delay.

3. In the event that data recorded in ECRIS-TCN are inaccurate or have been processed unlawfully, the convicting Member State shall rectify or erase the data in accordance with Article 9. The convicting Member State or, where applicable, the Member State to which the request has been made shall confirm in writing to the person concerned without undue delay that action has been taken to rectify or erase data relating to that person. The convicting Member State shall also without undue delay inform any other Member State which has been a recipient of conviction information obtained as a result of a query of ECRIS-TCN of what action has been taken.

4. If the convicting Member State does not agree that data recorded in ECRIS-TCN are inaccurate or have been processed unlawfully, that Member State shall adopt an administrative or judicial decision explaining in writing to the person concerned why it is not prepared to rectify or erase data relating to him or her. Such cases may, where appropriate, be communicated to the national supervisory authority.

5. The Member State which has adopted the decision pursuant to paragraph 4 shall also provide the person concerned with information explaining the steps which that person can take if the explanation given pursuant to paragraph 4 is not acceptable to him or her. This shall include information on how to bring an action or a complaint before the competent authorities or courts of that Member State and any assistance, including from the national supervisory authorities, that is available in accordance with the national law of that Member State.

6. Any request made pursuant to paragraph 1 shall contain the information necessary to identify the person concerned. That information shall be used exclusively to enable the exercise of the rights referred to in paragraph 1 and shall be erased immediately afterwards.

7. Where paragraph 2 applies, the central authority to whom the request was addressed shall keep a written record that such a request was made and of how it was addressed and to which authority it was forwarded. Upon request from the national supervisory authority, the central authority shall make that record available to that national supervisory authority without delay. The central authority and the national supervisory authority shall erase such records three years after their creation.

Article 26

Cooperation to ensure respect for data protection rights

1. The central authorities shall cooperate with each other in order to ensure respect for the rights laid down in Article 25.

2. In each Member State, the national supervisory authority shall, upon request, provide information to the person concerned on how to exercise his or her right to rectify or erase data relating to him or to her, in accordance with the applicable Union data protection rules.

3. For the purposes of this Article, the national supervisory authority of the Member State which transmitted the data and the national supervisory authority of the Member State to which the request has been made shall cooperate with each other.

Article 27

Remedies

Any person shall have the right to lodge a complaint and the right to a legal remedy in the convicting Member State which refused the right of access to or the right of rectification or erasure of data relating to him or to her, referred to in Article 25 in accordance with national or Union law.

Article 28

Supervision by the national supervisory authorities

1. Each Member State shall ensure that the national supervisory authorities designated pursuant to applicable Union data protection rules shall monitor the lawfulness of the processing of personal data referred to in Articles 5 and 6 by the Member State concerned, including their transmission to and from ECRIS-TCN.

2. The national supervisory authority shall ensure that an audit of the data processing operations in the national criminal records and fingerprints databases related to the data exchange between those systems and ECRIS-TCN is carried out in accordance with relevant international auditing standards at least every three years from the date of the start of operations of ECRIS-TCN.

3. Member States shall ensure that their national supervisory authorities have sufficient resources to fulfil the tasks entrusted to them under this Regulation.

4. Each Member State shall supply any information requested by its national supervisory authorities and shall, in particular, provide them with information on the activities carried out in accordance with Articles 12, 13 and 19. Each Member State shall grant its national supervisory authorities access to its records pursuant to Article 25(7) and to its logs pursuant to Article 31(6) and allow them access at all times to all its ECRIS-TCN related premises.

Article 29

Supervision by the European Data Protection Supervisor

1. The European Data Protection Supervisor shall monitor that the personal data processing activities of eu-LISA concerning ECRIS-TCN are carried out in accordance with this Regulation.

2. The European Data Protection Supervisor shall ensure that an audit of eu-LISA's personal data processing activities is carried out in accordance with relevant international auditing standards at least every three years. A report of that audit shall be sent to the European Parliament, the Council, the Commission, eu-LISA and the supervisory authorities. eu-LISA shall be given an opportunity to make comments before the report is adopted.

3. eu-LISA shall supply information requested by the European Data Protection Supervisor, give him or her access to all documents and to its logs referred to in Article 31 and allow him or her access to all of its premises at any time.

Article 30

Cooperation among national supervisory authorities and the European Data Protection Supervisor

Coordinated supervision of ECRIS-TCN shall be ensured in accordance with Article 62 of Regulation (EU) 2018/1725.

Article 31

Keeping of logs

1. eu-LISA and the competent authorities shall ensure, in accordance with their respective responsibilities, that all data processing operations in ECRIS-TCN are logged in accordance with paragraph 2 for the purposes of checking the admissibility of requests, monitoring data integrity and security and the lawfulness of the data processing as well as for the purposes of self-monitoring.

2. The log shall show:

(a) the purpose of the request for access to ECRIS-TCN data;

(b) the data transmitted as referred to in Article 5;

(c) the national file reference;

(d) the date and exact time of the operation;

(e) the data used for a query;

(f) the identifying mark of the official who carried out the search.

3. The log of consultations and disclosures shall make it possible to establish the justification of such operations.

4. Logs shall be used only for monitoring the lawfulness of data processing and for ensuring data integrity and security. Only logs containing non-personal data may be used for the monitoring and evaluation referred to in Article 36. Those logs shall be protected by appropriate measures against unauthorised access and erased after three years, if they are no longer required for monitoring procedures which have already begun.

5. On request, eu-LISA shall make the logs of its processing operations available to the central authorities without undue delay.

6. The competent national supervisory authorities responsible for checking the admissibility of the requests and monitoring the lawfulness of the data processing and data integrity and security shall have access to logs at their request for the purpose of fulfilling their duties. On request, the central authorities shall make the logs of their processing operations available to the competent national supervisory authorities without undue delay.

CHAPTER VI

Final provisions

Article 32

Use of data for reporting and statistics

1. The duly authorised staff of eu-LISA, of the competent authorities and of the Commission shall have access to the data processed within ECRIS-TCN solely for the purposes of reporting and providing statistics, without allowing for individual identification.

2. For the purpose of paragraph 1, eu-LISA shall establish, implement and host a central repository at its technical sites containing the data referred to in paragraph 1 which, without allowing for individual identification, enables customisable reports and statistics to be obtained. Access to the central repository shall be granted by means of secured access with control of access and specific user profiles, solely for the purpose of reporting and statistics.

3. The procedures put in place by eu-LISA to monitor the functioning of ECRIS-TCN referred to in Article 36 as well as the ECRIS reference implementation shall include the possibility to produce regular statistics for monitoring purposes.

Every month eu-LISA shall submit to the Commission statistics relating to the recording, storage and exchange of information extracted from criminal records through ECRIS-TCN and the ECRIS reference implementation. eu-LISA shall ensure that it is not possible to identify individuals on the basis of those statistics. At the request of the Commission, eu-LISA shall provide it with statistics on specific aspects related to the implementation of this Regulation.

4. The Member States shall provide eu-LISA with the statistics necessary to fulfil its obligations referred to in this Article. They shall provide the Commission with statistics on the number of convicted third-country nationals, as well as the number of convictions of third-country nationals on their territory.

Article 33

Costs

1. The costs incurred in connection with the establishment and operation of the central system, the communication infrastructure referred to in point (d) of Article 4(1), the interface software and the ECRIS reference implementation shall be borne by the general budget of the Union.

2. The costs of connection of Eurojust, Europol and the EPPO to ECRIS-TCN shall be borne by their respective budgets.

3. Other costs shall be borne by the Member States, specifically the costs incurred by the connection of the existing national criminal records registers, fingerprints databases and the central authorities to ECRIS-TCN, as well as the costs of hosting the ECRIS reference implementation.

Article 34

Notifications

1. Each Member State shall notify eu-LISA of its central authority, or authorities, that has access to enter, rectify, erase, consult or search data, as well as of any change in this respect.

2. eu-LISA shall ensure publication of the list of central authorities notified by the Member States, both in the *Official Journal of the European Union* and on its website. When eu-LISA receives notification of a change to a Member State's central authority, it shall update the list without undue delay.

Article 35

Entry of data and start of operations

1. Once the Commission is satisfied that the following conditions are met, it shall determine the date from which the Member States shall start entering the data referred to in Article 5 into ECRIS-TCN:

(a) the relevant implementing acts referred to in Article 10 have been adopted;

(b) the Member States have validated the technical and legal arrangements to collect and transmit the data referred to in Article 5 to ECRIS-TCN and have notified them to the Commission;

(c) eu-LISA has carried out a comprehensive test of ECRIS-TCN, in cooperation with the Member States, using anonymous test data.

2. When the Commission has determined the date of start of entry of data in accordance with paragraph 1, it shall communicate that date to the Member States. Within a period of two months following that date, the Member States shall enter the data referred to in Article 5 into ECRIS-TCN, taking account of Article 41(2).

3. After the end of the period referred to in paragraph 2, eu-LISA shall carry out a final test of ECRIS-TCN, in cooperation with the Member States.

4. When the test referred to in paragraph 3 has been successfully completed and eu-LISA considers that ECRIS-TCN is ready to start operations, it shall notify the Commission. The Commission shall inform the European Parliament and the Council of the results of the test and shall decide on the date on which ECRIS-TCN is to start operations.

5. The decision of the Commission on the date of the start of operations of ECRIS-TCN, as referred to in paragraph 4, shall be published in the *Official Journal of the European Union*.

6. The Member States shall start using ECRIS-TCN from the date determined by the Commission in accordance with paragraph 4.

7. When taking the decisions referred to in this Article, the Commission may specify different dates for the entry into ECRIS-TCN of alphanumeric data and fingerprint data as referred to in Article 5, as well as for the start of operations with respect to those different categories of data.

Article 36

Monitoring and evaluation

1. eu-LISA shall ensure that procedures are in place to monitor the development of ECRIS-TCN in light of objectives relating to planning and costs and to monitor the functioning of ECRIS-TCN and the ECRIS reference implementation in light of objectives relating to the technical output, cost-effectiveness, security and quality of service.

2. For the purposes of monitoring the functioning of ECRIS-TCN and its technical maintenance, eu-LISA shall have access to the necessary information relating to the data processing operations performed in ECRIS-TCN and in the ECRIS reference implementation.

3. By 12 December 2019 and every six months thereafter during the design and development phase, eu-LISA shall submit a report to the European Parliament and the Council on the state of play of the development of ECRIS-TCN and of the ECRIS reference implementation.

4. The report referred to in paragraph 3 shall include an overview of the current costs and the progress of the project, a financial impact assessment, and information on any technical problems and risks that may impact the overall costs of ECRIS-TCN to be borne by the general budget of the Union in accordance with Article 33.

5. In the event of substantial delays in the development process, eu-LISA shall inform the European Parliament and the Council as soon as possible of the reasons for these delays and of their impact in terms of time and finances.

6. Once the development of ECRIS-TCN and of the ECRIS reference implementation is finalised, eu-LISA shall submit a report to the European Parliament and to the Council explaining how the objectives, in particular relating to planning and costs, were achieved and justifying any divergences.

7. In the event of a technical upgrade of ECRIS-TCN which could result in substantial costs, eu-LISA shall inform the European Parliament and the Council.

8. Two years after the start of operations of ECRIS-TCN and every year thereafter, eu-LISA shall submit to the Commission a report on the technical functioning of ECRIS-TCN and of the ECRIS reference implementation, including their security, based in particular on the statistics on the functioning and use of ECRIS-TCN and on the exchange, through the ECRIS reference implementation, of information extracted from the criminal records.

9. Four years after the start of operations of ECRIS-TCN and every four years thereafter, the Commission shall conduct an overall evaluation of ECRIS-TCN and of the ECRIS reference implementation. The overall evaluation report established on this basis shall include an assessment of the application of this Regulation and an examination of results that have been achieved relative to the objectives that were set and of the impact on fundamental rights. The report shall also include an assessment of whether the underlying rationale for operating ECRIS-TCN continues to hold, of the appropriateness of the use of biometric data for the purposes of ECRIS-TCN, of the security of ECRIS-TCN and of any security implications for future operations. The evaluation shall include any necessary recommendations. The Commission shall transmit the report to the European Parliament, the Council, the European Data Protection Supervisor and the European Union Agency for Fundamental Rights.

10. In addition, the first overall evaluation as referred to in paragraph 9 shall include an assessment of:

(a) the extent to which, on the basis of relevant statistical data and further information from the Member States, the inclusion in ECRIS-TCN of identity information of citizens of the Union who also hold the nationality of a third country has contributed to the achievement of the objectives of this Regulation;

(b) the possibility, for some Member States, to continue the use of national ECRIS implementation software, as referred to in Article 4;

(c) the entry of fingerprint data into ECRIS-TCN, in particular the application of the minimum criteria as referred to in point (b)(ii) of Article 5(1);

(d) the impact of ECRIS and of ECRIS-TCN on the protection of personal data.

The assessment may be accompanied, if necessary, by legislative proposals. Subsequent overall evaluations may include an assessment of any or all of those aspects.

11. The Member States, Eurojust, Europol and the EPPO shall provide eu-LISA and the Commission with the information necessary to draft the reports referred to in paragraphs 3, 8 and 9 according to the quantitative indicators predefined by the Commission or eu-LISA or both. That information shall not jeopardise working methods or include information that reveals sources, staff members or investigations.

12. Where relevant, the supervisory authorities shall provide eu-LISA and the Commission with the information necessary to draft the reports referred to in paragraph 9 according to the quantitative indicators predefined by the Commission or eu-LISA or both. That information shall not jeopardise working methods or include information that reveals sources, staff members or investigations.

13. eu-LISA shall provide the Commission with the information necessary to produce the overall evaluations referred to in paragraph 9.

Article 37

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 6(2) shall be conferred on the Commission for an indeterminate period of time from 11 June 2019.

3. The delegation of power referred to in Article 6(2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Article 6(2) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 38

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Where the committee delivers no opinion, the Commission shall not adopt the draft implementing act and the third subparagraph of Article 5(4) of Regulation (EU) No 182/2011 shall apply.

Article 39

Advisory Group

eu-LISA shall establish an Advisory Group in order to obtain expertise related to ECRIS-TCN and the ECRIS reference implementation, in particular in the context of preparation of its annual work programme and its annual activity report. During the design and development phase, Article 11(9) shall apply.

Article 40

Amendments to Regulation (EU) 2018/1726

Regulation (EU) 2018/1726 is amended as follows:

(1) In Article 1, paragraph 4 is replaced by the following:

'4. The Agency shall be responsible for the preparation, development or operational management of the Entry/Exit System (EES), DubliNet, the European Travel Information and Authorisation System (ETIAS), ECRIS-TCN and the ECRIS reference implementation.';

(2) The following Article is inserted:

'*Article 8a*

Tasks related to ECRIS-TCN and the ECRIS reference implementation

In relation to ECRIS-TCN and the ECRIS reference implementation, the Agency shall perform:

(a) the tasks conferred on it by Regulation (EU) 2019/816 of the European Parliament and of the Council (*);

(b) tasks relating to training on the technical use of ECRIS-TCN and the ECRIS reference implementation.

(*) Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System) and amending Regulation (EU) 2018/1726 (OJ L 135, 22.5.2019, p. 1).';

(3) In Article 14, paragraph 1 is replaced by the following:

'1. The Agency shall monitor developments in research relevant for the operational management of SIS II, VIS, Eurodac, the EES, ETIAS, DubliNet, ECRIS-TCN and other large-scale IT systems as referred to in Article 1(5).';

(4) In Article 19, paragraph 1 is amended as follows:

(a) point (ee) is replaced by the following:

'(ee) adopt the reports on the development of the EES pursuant to Article 72(2) of Regulation (EU) 2017/2226, the reports on the development of ETIAS pursuant to Article 92(2) of Regulation (EU) 2018/1240 and the reports on the development of ECRIS-TCN and of the ECRIS reference implementation pursuant to Article 36(3) of Regulation (EU) 2019/816;';

(b) point (ff) is replaced by the following:

'(ff) adopt the reports on the technical functioning of SIS II pursuant to Article 50(4) of Regulation (EC) No 1987/2006 and Article 66(4) of Decision 2007/533/JHA respectively, of VIS pursuant to Article 50(3) of Regulation (EC) No 767/2008 and Article 17(3) of Decision 2008/633/JHA, of the EES pursuant to Article 72(4) of Regulation (EU) 2017/2226, of ETIAS pursuant to Article 92(4) of Regulation (EU) 2018/1240, and of ECRIS-TCN and of the ECRIS reference implementation pursuant to Article 36(8) of Regulation (EU) 2019/816;';

(c) point (hh) is replaced by the following:

'(hh) adopt formal comments on the European Data Protection Supervisor's reports on the audits carried out pursuant to Article 45(2) of Regulation (EC) No 1987/2006, Article 42(2) of Regulation (EC) No 767/2008 and Article 31(2) of Regulation (EU) No 603/2013, Article 56(2) of Regulation (EU) 2017/2226, Article 67 of Regulation (EU) 2018/1240 and to Article 29(2) of Regulation (EU) 2019/816 and ensure appropriate follow-up of those audits;';

(d) the following point is inserted:

'(lla) submit to the Commission statistics related to ECRIS-TCN and to the ECRIS reference implementation pursuant to the second subparagraph of Article 32(3) of Regulation (EU) 2019/816;';

(e) point (mm) is replaced by the following:

'(mm) ensure annual publication of the list of competent authorities authorised to search directly the data contained in SIS II pursuant to Article 31(8) of Regulation (EC) No 1987/2006 and Article 46(8) of Decision 2007/533/JHA, together with the list of Offices of the national systems of SIS II (N.SIS II Offices) and SIRENE Bureaux pursuant to Article 7(3) of Regulation (EC) No 1987/2006 and Article 7(3) of Decision 2007/533/JHA respectively as well as the list of competent authorities pursuant to Article 65(2) of Regulation (EU) 2017/2226, the list of competent authorities pursuant to Article 87(2) of Regulation (EU) 2018/1240 and the list of central authorities pursuant to Article 34(2) of Regulation (EU) 2019/816;';

(5) In Article 22(4), the following subparagraph is inserted after the third subparagraph:

'Eurojust, Europol and the EPPO may attend the meetings of the Management Board as observers when a question concerning ECRIS-TCN in relation to the application of Regulation (EU) 2019/816 is on the agenda.';

(6) In Article 24(3), point (p) is replaced by the following:

'(p) establishing, without prejudice to Article 17 of the Staff Regulations of Officials, confidentiality requirements in order to comply with Article 17 of Regulation (EC) No 1987/2006, Article 17 of Decision 2007/533/JHA, Article 26(9) of Regulation (EC) No 767/2008, Article 4(4) of Regulation (EU) No 603/2013, Article 37(4) of Regulation (EU) 2017/2226, Article 74(2) of Regulation (EU) No 2018/1240 and Article 11(16) of Regulation (EU) 2019/816;';

(7) In Article 27(1), the following point is inserted:

'(da) ECRIS-TCN Advisory Group;'.

Article 41

Implementation and transitional provisions

1. Member States shall take the necessary measures to comply with this Regulation as soon as possible so as to ensure the proper functioning of ECRIS-TCN.

2. For convictions handed down prior to the date of start of entry of data in accordance with Article 35(1), the central authorities shall create the individual data records in the central system as follows:

(a) alphanumeric data to be entered into the central system by the end of the period referred to in Article 35(2);

(b) fingerprint data to be entered into the central system within two years after the start of operations in accordance with Article 35(4).

Article 42

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

Done at Strasbourg, 17 April 2019.

For the European Parliament	*For the Council*
The President	*The President*
A. TAJANI	G. CIAMBA

ANNEX

STANDARD INFORMATION REQUEST FORM AS REFERRED TO IN ARTICLE 17(1) OF REGULATION (EU) 2019/816 IN ORDER TO OBTAIN INFORMATION ON WHICH MEMBER STATE, IF ANY, HOLDS CRIMINAL RECORDS INFORMATION OF A THIRD-COUNTRY NATIONAL

This form, which is available at www.eurojust.europa.eu in all 24 official languages of the institutions of the Union, should be addressed in one of those languages to ECRIS-TCN@eurojust.europa.eu

Requesting state or international organisation:

Name of state or international organisation:
Authority submitting the request:
Represented by *(name of person):*
Title:
Address:
Telephone number:
Email address:

Criminal proceedings for which the information is sought:

Domestic reference number:
Competent authority:
Type of crimes under investigation *(please mention relevant article(s) of criminal code):*
Other relevant information *(e.g. urgency of the request):*

Identity information of the person having the nationality of a third country in respect of whom information regarding the convicting Member State is sought:

NB: please provide as much available information as possible.

Surname *(family name):*
First name(s) *(given names):*
Date of birth:
Place of birth *(town and country):*
Nationality or nationalities:
Gender:
Previous name(s), if applicable:
Parents' names:
Identity number:
Type and number of the person's identification document(s):
Issuing authority of document(s):
Pseudonyms or aliases:
If fingerprint data are available, please provide these.

In case of multiple persons, please indicate them separately

A drop down panel would allow the insertion of additional subjects

Place	
Date	

(Electronic) signature and stamp:

REGULATION (EU) 2019/817 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 20 May 2019

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2), Article 74 and Article 77(2)(a), (b), (d) and (e) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee ([1]),

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure ([2]),

Whereas:

(1) In its Communication of 6 April 2016 entitled Stronger and Smarter Information Systems for Borders and Security, the Commission underlined the need to improve the Union's data management architecture for border management and security. The Communication initiated a process towards achieving interoperability between EU information systems for security, border and migration management, with the aim to address the structural shortcomings related to those systems that impede the work of national authorities and to ensure that border guards, customs authorities, police officers and judicial authorities have the necessary information at their disposal.

(2) In its Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area of 6 June 2016, the Council identified various legal, technical and operational challenges in the interoperability of EU information systems and called for the pursuit of solutions.

(3) In its Resolution of 6 July 2016 on the strategic priorities for the Commission Work Programme 2017 ([3]), the European Parliament called for proposals to improve and develop existing EU information systems, address information gaps and move towards their interoperability, as well as proposals for compulsory information sharing at EU level, accompanied by the necessary data protection safeguards.

(4) In its conclusions of 15 December 2016 the European Council called for work to continue on delivering interoperability of EU information systems and databases.

(5) In its final report of 11 May 2017, the high-level expert group on information systems and interoperability concluded that it was necessary and technically feasible to work towards practical solutions for interoperability and that interoperability could, in principle, both deliver operational gains and be established in compliance with data protection requirements.

([1]) OJ C 283, 10.8.2018, p. 48.
([2]) Position of the European Parliament of 16 April 2019 (not yet published in the Official Journal) and decision of the Council of 14 May 2019.
([3]) OJ C 101, 16.3.2018, p. 116.

(6) In its Communication of 16 May 2017 entitled Seventh progress report towards an effective and genuine Security Union, the Commission set out, in line with its Communication of 6 April 2016 and the findings and recommendations of the high-level expert group on information systems and interoperability, a new approach to the management of data for borders, security and migration whereby all EU information systems for security, border and migration management were to be interoperable, in a manner fully respecting fundamental rights.

(7) In its Conclusions of 9 June 2017 on the way forward to improve information exchange and ensure the interoperability of EU information systems, the Council invited the Commission to pursue the solutions for interoperability proposed by the high-level expert group.

(8) In its conclusions of 23 June 2017 the European Council underlined the need to improve interoperability between databases and invited the Commission to prepare draft legislation on the basis of the proposals made by the high-level expert group on information systems and interoperability as soon as possible.

(9) With a view to improving the effectiveness and efficiency of checks at the external borders, to contributing to prevention and combating illegal immigration and to contributing 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 security in the territories of the Member States, to improving the implementation of the common visa policy, to assisting in the examination of applications for international protection, to contributing to the prevention, detection and investigation of terrorist offences and other serious criminal offences, to facilitating the identificaton of unknown persons who are unable to identify themselves or unidentified human remains in the case of a natural disaster, accident or terrorist attack, in order to maintain public trust in the Union migration and asylum system, Union security measures and Union capabilities to manage the external border, interoperability between EU information systems, namely 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) should be established in order for these EU information systems and their data to supplement each other while respecting the fundamental rights of individuals, in particular the right to protection of personal data. To achieve this, a European search portal (ESP), a shared biometric matching service (shared BMS), a common identity repository (CIR) and a multiple-identity detector (MID) should be established as interoperability components.

(10) Interoperability between the EU information systems should allow those systems to supplement each other in order to facilitate the correct identification of persons, including unknown persons who are unable to identify themselves or unidentified human remains, contribute to combating identity fraud, improve and harmonise the data quality requirements of the respective EU information systems, facilitate the technical and operational implementation by Member States of EU information systems, strengthen the data security and data protection safeguards that govern the respective EU information systems, streamline access for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences to the EES, VIS, ETIAS and Eurodac, and support the purposes of the EES, VIS, ETIAS, Eurodac, SIS and ECRIS-TCN.

(11) The interoperability components should cover the EES, VIS, ETIAS, Eurodac, SIS, and ECRIS-TCN. They should also cover Europol data, but only to the extent of enabling Europol data to be queried simultaneously with those EU information systems.

(12) The interoperability components should process the personal data of persons whose personal data are processed in the underlying EU information systems and by Europol.

(13) The ESP should be established to facilitate technically the fast, seamless, efficient, systematic and controlled access by Member State authorities and Union agencies to the EU information systems, to Europol data and to the International Criminal Police Organization (Interpol) databases, insofar as this is needed to perform their tasks in accordance with their access rights. The ESP should also be established to support the objectives of the EES, VIS, ETIAS, Eurodac, SIS, ECRIS-TCN and Europol data. By enabling all relevant EU information systems, Europol data

and the Interpol databases to be queried in parallel, the ESP should act as a single window or 'message broker' to search the various central systems and retrieve the necessary information seamlessly and in full respect of the access control and data protection requirements of the underlying systems.

(14) The design of the ESP should ensure that, when querying the Interpol databases, the data used by an ESP user to launch a query is not shared with the owners of Interpol data. The design of the ESP should also ensure that the Interpol databases are only queried in accordance with applicable Union and national law.

(15) The Interpol database of Stolen and Lost Travel Documents (SLTD database) enables authorised entities responsible for preventing, detecting or investigating terrorist offences or other serious criminal offences in Member States, including immigration and border control authorities, to establish the validity of a travel document. ETIAS queries the SLTD database and the Interpol Travel Documents Associated with Notices database (TDAWN database) in the context of assessing whether a person applying for a travel authorisation is likely for instance to migrate irregularly or could pose a threat to security. The ESP should enable queries against the SLTD and TDAWN databases using an individual's identity data or travel document data. Where personal data are transferred from the Union to Interpol through the ESP, the provisions on international transfers in Chapter V of Regulation (EU) 2016/679 of the European Parliament and of the Council ([4]), or the national provisions transposing Chapter V of Directive (EU) 2016/680 of the European Parliament and of the Council ([5]) should apply. This should be without prejudice to the specific rules laid down in Council Common Position 2005/69/JHA ([6]) and Council Decision 2007/533/JHA ([7]).

(16) The ESP should be developed and configured in such a way that it only allows such queries to be performed using data related to persons or travel documents held in an EU information system, in Europol data or in the Interpol databases.

(17) To ensure the systematic use of the relevant EU information systems, the ESP should be used to query the CIR, the EES, VIS, ETIAS, Eurodac and ECRIS-TCN. However, a national connection to the different EU information systems should remain in order to provide a technical fall back. The ESP should also be used by Union agencies to query Central SIS in accordance with their access rights and in order to perform their tasks. The ESP should be an additional means to query Central SIS, Europol data and the Interpol databases, complementing the existing dedicated interfaces.

(18) Biometric data, such as fingerprints and facial images, are unique and therefore much more reliable than alphanumeric data for the purposes of identifying a person. The shared BMS should be a technical tool to reinforce and facilitate the work of the relevant EU information systems and the other interoperability components. The main purpose of the shared BMS should be to facilitate the identification of an individual who is registered in several databases, by using a single technological component to match that individual's biometric data across different systems, instead of several components. The shared BMS should contribute to security, as well as financial, maintenance and operational benefits. All automated fingerprint identification systems, including those currently used for Eurodac, VIS and SIS, use biometric templates comprised of data derived from a feature extraction of actual biometric samples. The shared BMS should regroup and store all these biometric templates – logically separated according to the information system from which the data originated – in one single location, thereby facilitating cross-system comparisons using biometric templates and enabling economies of scale in developing and maintaining the EU central systems.

([4]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

([5]) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

([6]) Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol (OJ L 27, 29.1.2005, p. 61).

([7]) Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007, p. 63).

(19) The biometric templates stored in the shared BMS should be comprised of data derived from a feature extraction of actual biometric samples and obtained in such a way that reversing the extraction process is not possible. Biometric templates should be obtained from biometric data but it should not be possible to obtain that same biometric data from the biometric templates. As palm print data and DNA profiles are only stored in SIS and cannot be used to perform cross-checks with data present in other information systems, following the principles of necessity and proportionality, the shared BMS should not store DNA profiles or biometric templates obtained from palm print data.

(20) Biometric data constitute sensitive personal data. This Regulation should lay down the basis and the safeguards for processing such data for the purpose of uniquely identifying the persons concerned.

(21) The EES, VIS, ETIAS, Eurodac and ECRIS-TCN require accurate identification of the persons whose personal data are stored in them. The CIR should therefore facilitate the correct identification of persons registered in those systems.

(22) Personal data stored in those EU information systems may relate to the same persons but under different or incomplete identities. Member States dispose of efficient ways to identify their citizens or registered permanent residents in their territory. The interoperability between EU information systems should contribute to the correct identification of persons present in those systems. The CIR should store the personal data that are necessary to enable the more accurate identification of the individuals whose data are stored in those systems, including their identity data, travel document data and biometric data, regardless of the system in which the data were originally collected. Only the personal data strictly necessary to perform an accurate identity check should be stored in the CIR. The personal data recorded in the CIR should be kept for no longer than is strictly necessary for the purposes of the underlying systems and should be automatically deleted when the data are deleted from the underlying systems in accordance with their logical separation.

(23) A new processing operation consisting of the storage of such data in the CIR instead of the storage in each of the separate systems is necessary to increase the accuracy of identification through the automated comparison and matching of the data. The fact that identity data, travel document data and biometric data are stored in the CIR should not hinder in any way the processing of data for the purposes of the EES, VIS, ETIAS, Eurodac or ECRIS-TCN, as the CIR should be a new shared component of those underlying systems.

(24) It is therefore necessary to create an individual file in the CIR for each person registered in the EES, VIS, ETIAS, Eurodac or ECRIS-TCN, to achieve the purpose of correct identification of persons within the Schengen area and to support the MID for the dual purpose of facilitating identity checks for *bona fide* travellers and combating identity fraud. The individual file should store all the identity information linked to a person in a single place and make it accessible to duly authorised end-users.

(25) The CIR should thus facilitate and streamline access by authorities responsible for preventing, detecting or investigating terrorist offences or other serious criminal offences to the EU information systems that are not established exclusively for purposes of prevention, detection or investigation of serious crime.

(26) The CIR should provide for a shared container for identity data, travel document data and biometric data of persons registered in the EES, VIS, ETIAS, Eurodac and the ECRIS-TCN. It should be part of the technical architecture of these systems and serve as the shared component between them for storing and querying the identity data, travel document data and biometric data they process.

(27) All records in the CIR should be logically separated by automatically tagging each record with the name of the underlying system owning that record. The access controls of the CIR should use these tags to determine whether to allow access to the record.

(28) Where a Member State police authority is unable to identify a person due to the lack of a travel document or another credible document proving that person's identity, or where there are doubts about the identity data provided by that person or as to the authenticity of the travel document or the identity of its holder, or where

the person is unable or refuses to cooperate, that police authority should be able to query the CIR in order to identify the person. For those purposes, police authorities should capture fingerprints using live-scan fingerprinting techniques, provided that the procedure was initiated in the presence of that person. Such queries of the CIR should not be permitted for the purposes of identifying minors under the age of 12 years old, unless in the best interests of the child.

(29) Where the biometric data of a person cannot be used or if a query with that data fails, the query should be carried out with identity data of the person in combination with travel document data. Where the query indicates that data on that person are stored in the CIR, Member State authorities should have access to the CIR to consult the identity data and travel document data of that person, without the CIR providing any indication as to which EU information system the data belong.

(30) Member States should adopt national legislative measures designating the authorities competent to perform identity checks using the CIR and laying down the procedures, conditions and criteria for such checks, which should follow the principle of proportionality. In particular, the power to collect biometric data during an identity check of a person present before a staff member of those authorities should be provided for by national law.

(31) This Regulation should also introduce a new possibility for streamlined access to data beyond the identity data or travel document data present in the EES, VIS, ETIAS or Eurodac by Member State designated authorities responsible for preventing, detecting or investigating terrorist offences or other serious criminal offences and Europol. Such data may be necessary for the prevention, detection or investigation of terrorist offences or other serious criminal offences in a specific case where there are reasonable grounds to believe that consulting them will contribute to the prevention, detection or investigation of the terrorist offences or other serious criminal offences, in particular where there is a suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence is a person whose data are stored in the EES, VIS, ETIAS or Eurodac.

(32) Full access to data contained in the EES, VIS, ETIAS or Eurodac that is necessary for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences, beyond access to identity data or travel document data held in the CIR, should continue to be governed by the applicable legal instruments. The designated authorities responsible for preventing, detecting or investigating terrorist offences or other serious criminal offences and Europol do not know in advance which of the EU information systems contains data of the persons they need to inquire upon. This results in delays and inefficiencies. The end-user authorised by the designated authority should therefore be allowed to see in which of those EU information systems the data corresponding to the result of a query are recorded. The system concerned would thus be flagged following the automated verification of the presence of a match in the system (a so-called match-flag functionality).

(33) In this context, a reply from the CIR should not be interpreted or used as a ground or reason to draw conclusions on or undertake measures in respect of a person, but should be used only for the purpose of submitting an access request to the underlying EU information systems, subject to the conditions and procedures laid down in the respective legal instruments governing such access. Any such access request should be subject to Chapter VII of this Regulation and as applicable, Regulation (EU) 2016/679, Directive (EU) 2016/680 or Regulation (EU) 2018/1725 of the European Parliament and of the Council ([8]).

(34) As a general rule, where a match-flag indicates that the data are recorded in the EES, VIS, ETIAS or Eurodac, the designated authorities or Europol should request full access to at least one of the EU information systems concerned. Where exceptionally such full access is not requested, for example because designated authorities or Europol have already obtained the data by other means, or obtaining the data is no longer permitted under national law, the justification for not requesting access should be recorded.

([8]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons 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 (OJ L 295, 21.11.2018, p. 39).

(35) The logs of the queries of the CIR should indicate the purpose of the queries. Where such a query was performed using the two-step data consultation approach, the logs should include a reference to the national file of the investigation or case, thereby indicating that the query was launched for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences.

(36) The query of the CIR by the designated authorities and Europol in order to obtain a match-flag type of response indicating that the data are recorded in the EES, VIS, ETIAS or Eurodac requires automated processing of personal data. A match-flag should not reveal personal data of the concerned individual other than an indication that some of his or her data are stored in one of the systems. No adverse decision for the individual concerned should be made by the authorised end-user solely on the basis of the simple occurrence of a match-flag. Access by the end-user to a match-flag will therefore constitute a very limited interference with the right to protection of personal data of the individual concerned, while allowing the designated authorities and Europol to request access to personal data more effectively.

(37) The MID should be established to support the functioning of the CIR and to support the objectives of the EES, VIS, ETIAS, Eurodac, SIS and ECRIS-TCN. In order to be effective in fulfilling their respective objectives, all of these EU information systems require the accurate identification of the persons whose personal data are stored in them.

(38) To better attain the objectives of EU information systems, the authorities using those systems should be able to conduct sufficiently reliable verifications of the identities of the persons whose data are stored in different systems. The set of identity data or travel document data stored in a given individual system may be incorrect, incomplete or fraudulent, and there is currently no way of detecting incorrect, incomplete or fraudulent identity data or travel document data by way of comparison with data stored in another system. To remedy this situation, it is necessary to have a technical instrument at Union level allowing accurate identification of persons for these purposes.

(39) The MID should create and store links between data in the different EU information systems in order to detect multiple identities, with the dual purpose of facilitating identity checks for *bona fide* travellers and combating identity fraud. The MID should only contain links between data on individuals present in more than one EU information system. The linked data should be strictly limited to the data necessary to verify that a person is recorded in a justified or unjustified manner under different identities in different systems, or to clarify that two persons having similar identity data may not be the same person. Data processing through the ESP and the shared BMS in order to link individual files across different systems should be kept to an absolute minimum and therefore limited to multiple-identity detection, to be conducted at the time new data are added in one of the systems which has data stored in the CIR or added in SIS. The MID should include safeguards against potential discrimination and unfavourable decisions for persons with multiple lawful identities.

(40) This Regulation provides for new data processing operations aimed at identifying the persons concerned correctly. This constitutes an interference with their fundamental rights as protected by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Since the effective implementation of the EU information systems is dependent upon correct identification of the individuals concerned, such interference is justified by the same objectives for which each of those systems have been established, the effective management of the Union's borders, the internal security of the Union and the effective implementation of the Union's asylum and visa policies.

(41) The ESP and the shared BMS should compare data on persons in the CIR and SIS when new records are created or uploaded by a national authority or a Union agency. Such comparison should be automated. The CIR and SIS should use the shared BMS to detect possible links on the basis of biometric data. The CIR and SIS should use the ESP to detect possible links on the basis of alphanumeric data. The CIR and SIS should be able to identify the same or similar data on a person stored across several systems. Where such is the case, a link indicating that it is the same person should be established. The CIR and SIS should be configured in such a way that small transliteration or spelling mistakes are detected in such a way as not to create any unjustified hindrance to the person concerned.

(42) The national authority or Union agency that recorded the data in the respective EU information system should confirm or change the links. This national authority or Union agency should have access to the data stored in the CIR or SIS and in the MID for the purpose of a manual verification of different identities.

(43) A manual verification of different identities should be ensured by the authority creating or updating the data that triggered a match resulting in a link with data stored in another EU information system. The authority responsible for the manual verification of different identities should assess whether there are multiple identities referring to the same person in a justified or unjustified manner. Such an assessment should be performed where possible in the presence of the person concerned and where necessary by requesting additional clarifications or information. The assessment should be performed without delay, in line with legal requirements for the accuracy of information under Union and national law. At the borders especially, the movement of the persons involved will be restricted for the duration of the verification, which should therefore not last indefinitely. The existence of a yellow link in the MID should not constitute in itself a ground for refusal of entry and any decision on authorising or refusing entry should be taken exclusively on the basis of the applicable provisions of Regulation (EU) 2016/399 of the European Parliament and of the Council ([9]).

(44) For links obtained through SIS related to alerts in respect of persons wanted for arrest for surrender or extradition purposes, on missing or vulnerable persons, on persons sought to assist with a judicial procedure or on persons for discreet checks, inquiry checks or specific checks, the authority responsible for the manual verification of different identities should be the SIRENE Bureau of the Member State that created the alert. These categories of SIS alerts are sensitive and should not necessarily be shared with the authorities creating or updating data that are linked to them in one of the other EU information systems. The creation of a link with SIS data should be without prejudice to the actions to be taken in accordance with Regulations (EU) 2018/1860 ([10]), (EU) 2018/1861 ([11]) and (EU) 2018/1862 ([12]) of the European Parliament and of the Council.

(45) The creation of such links requires transparency towards the individuals affected. In order to facilitate the implementation of the necessary safeguards in accordance with applicable Union data protection rules, individuals who are subject to a red link or a white link following manual verification of different identities should be informed in writing without prejudice to limitations to protect security and public order, prevent crime and guarantee that national investigations are not jeopardised. Those individuals should receive a single identification number allowing them to identify the authority to which they should address themselves to exercise their rights.

(46) Where a yellow link is created, the authority responsible for the manual verification of different identities should have access to the MID. Where a red link exists, Member State authorities and Union agencies having access to at least one EU information system included in the CIR or to SIS should have access to the MID. A red link should indicate that a person is using different identities in an unjustified manner or that a person is using somebody else's identity.

(47) Where a white or green link exists between data from two EU information systems, Member State authorities and Union agencies should have access to the MID where the authority or agency concerned has access to both information systems. Such access should be granted for the sole purpose of allowing that authority or agency to detect potential cases where data have been linked incorrectly or processed in the MID, CIR and SIS in breach of this Regulation and of taking action to correct the situation and update or delete the link.

([9]) Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ L 77, 23.3.2016, p. 1).

([10]) Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals (OJ L 312, 7.12.2018, p. 1).

([11]) Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 (OJ L 312, 7.12.2018, p. 14).

([12]) Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56).

(48) The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) should establish automated data quality control mechanisms and common data quality indicators. eu-LISA should be responsible for developing a central monitoring capacity for data quality and for producing regular data analysis reports to improve the control of the implementation by Member States of EU information systems. The common data quality indicators should include minimum quality standards for storing data in the EU information systems or interoperability components. The goal of such data quality standards should be for the EU information systems and interoperability components to identify automatically apparently incorrect or inconsistent data submissions, so that the originating Member State is able to verify the data and carry out any necessary remedial action.

(49) The Commission should evaluate eu-LISA's quality reports and should issue recommendations to Member States where appropriate. Member States should be responsible for preparing an action plan describing actions to remedy any deficiencies in data quality and should report on its progress regularly.

(50) The universal message format (UMF) should serve as a standard for structured, cross-border information exchange between information systems, authorities or organisations in the field of Justice and Home Affairs. The UMF should define a common vocabulary and logical structures for commonly exchanged information with the objective to facilitate interoperability by enabling the creation and reading of the contents of exchanges in a consistent and semantically equivalent manner.

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

(52) A central repository for reporting and statistics (CRRS) should be established to generate cross-system statistical data and analytical reporting for policy, operational and data quality purposes in accordance with the applicable legal instruments. eu-LISA should establish, implement and host the CRRS in its technical sites. It should contain anonymised statistical data from the EU information systems, the CIR, the MID and the shared BMS. The data contained in the CRRS should not enable the identification of individuals. eu-LISA should render the data anonymous in an automated manner and should record such anonymised data in the CRRS. The process for rendering the data anonymous should be automated and no direct access by eu-LISA staff should be granted to any personal data stored in the EU information systems or in the interoperability components.

(53) Regulation (EU) 2016/679 applies to the processing of personal data for the purpose of interoperability under this Regulation by national authorities unless such processing is carried out by the designated authorities or central access points of the Member States for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences.

(54) Where the processing of personal data by the Member States for the purpose of interoperability under this Regulation is carried out by the competent authorities for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences, Directive (EU) 2016/680 applies.

(55) Regulation (EU) 2016/679, Regulation (EU) 2018/1725 or, where relevant, Directive (EU) 2016/680 apply to any transfer of personal data to third countries or international organisations carried out under this Regulation. Without prejudice to the grounds for transfer pursuant to Chapter V of Regulation (EU) 2016/679 or, where relevant, Directive (EU) 2016/680, any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data should only be recognised or enforceable in any manner if based on an international agreement in force between the requesting third country and the Union or a Member State.

(56) The specific provisions on data protection of Regulations (EU) 2017/2226 ([13]), (EC) No 767/2008 ([14]), (EU) 2018/1240 ([15]) of the European Parliament and of the Council and Regulation (EU) 2018/1861 apply to the processing of personal data in the systems governed by those Regulations.

(57) Regulation (EU) 2018/1725 applies to the processing of personal data by eu-LISA and other institutions and bodies of the Union when carrying out their responsibilities under this Regulation, without prejudice to Regulation (EU) 2016/794 of the European Parliament and of the Council ([16]), which applies to the processing of personal data by Europol.

(58) The supervisory authorities referred to in Regulation (EU) 2016/679 or Directive (EU) 2016/680 should monitor the lawfulness of the processing of personal data by the Member States. The European Data Protection Supervisor should monitor the activities of the Union institutions and bodies in relation to the processing of personal data. The European Data Protection Supervisor and the supervisory authorities should cooperate with each other in the monitoring of the processing of personal data by interoperability components. For the European Data Protection Supervisor to fulfil the tasks entrusted to it under this Regulation, sufficient resources, including both human and financial resources, are required.

(59) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council ([17]) and delivered an opinion on 16 April 2018 ([18]).

(60) The Article 29 Data Protection Working Party provided an opinion on 11 April 2018.

(61) Both the Member States and eu-LISA should maintain security plans in order to facilitate the implementation of security obligations and should cooperate with each other in order to address security issues. eu-LISA should also make sure there is a continuous use of the latest technological developments to ensure data integrity in the context of the development, design and management of the interoperability components. eu-LISA's obligations in this respect should include adopting the measures necessary to prevent access by unauthorised persons, such as staff of external service providers, to personal data processed through the interoperability components. When awarding contracts for the provision of services, the Member States and eu-LISA should consider all measures necessary to secure compliance with laws or regulations relating to the protection of personal data and to the privacy of individuals or to safeguard essential security interests, pursuant to Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council ([19]) and applicable international conventions. eu-LISA should apply the principles of privacy by design and by default during the development of the interoperability components.

(62) The implementation of the interoperability components provided for in this Regulation will have an impact on the way checks are carried out at border crossing points. The impact will result from the combined application of the existing rules of Regulation (EU) 2016/399 and the rules on interoperability provided for in this Regulation.

(63) As a consequence of this combined application of the rules, the ESP should constitute the main access point for the compulsory systematic consultation of databases in respect of persons at border crossing points provided for by Regulation (EU) 2016/399. In addition, the identity data or travel document data that have led to the classification of a link in the MID as a red link should be taken into account by border guards for the purposes of

([13]) Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (EES Regulation) (OJ L 327, 9.12.2017, p. 20).

([14]) Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) (OJ L 218, 13.8.2008, p. 60).

([15]) Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018, p. 1).

([16]) Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).

([17]) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

([18]) OJ C 233, 4.7.2018, p. 12.

([19]) Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 (OJ L 193, 30.7.2018, p. 1).

assessing whether or not the person fulfils the conditions of entry defined in Regulation (EU) 2016/399. However, the presence of a red link should not in itself constitute a ground for refusal of entry and the existing grounds for refusal of entry listed in Regulation (EU) 2016/399 should therefore not be amended.

(64) It would be appropriate to update the Practical Handbook for Border Guards to make these clarifications explicit.

(65) Should a query of the MID through the ESP result in a yellow link or detect a red link, the border guard should consult the CIR or SIS or both in order to assess the information on the person being checked, to manually verify his or her identity data and to adapt the colour of the link if required.

(66) To support the purposes of statistics and reporting, it is necessary to grant access to authorised staff of the competent authorities, Union institutions and agencies referred to in this Regulation to consult certain data related to certain interoperability components without enabling the identification of individuals.

(67) In order to allow Member State authorities and Union agencies to adapt to the new requirements on the use of the ESP, it is necessary to provide for a transitional period. Similarly, in order to allow for a coherent and optimal functioning of the MID, transitional measures should be established for the start of its operations.

(68) Since the objective of this Regulation, namely, the establishment of a framework for interoperability between EU information systems, cannot be sufficiently achieved by the Member States but can rather, by reason of the scale and effects of the action, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(69) The remaining amount in the budget earmarked for smart borders in Regulation (EU) No 515/2014 of the European Parliament and of the Council ([20]) should be reallocated to this Regulation pursuant to Article 5(5)(b) of Regulation (EU) No 515/2014, to cover the costs of the development of the interoperability components.

(70) In order to supplement certain detailed technical aspects of this Regulation, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union (TFEU) should be delegated to the Commission in respect of:

— extending the transitional period for the use of the ESP;

— extending the transitional period for multiple-identity detection carried out by the ETIAS Central Unit;

— the procedures for determining the cases where identity data can be considered as the same or similar;

— the rules on the operation of the CRRS, including specific safeguards for processing of personal data and the security rules applicable to the repository; and

— detailed rules on the operation of the web portal.

It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making ([21]). In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member State' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(71) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to determine the dates from which the ESP, the shared BMS, the CIR, the MID and the CRRS are to start operations.

([20]) Regulation (EU) No 515/2014 of the European Parliament and of the Council of 16 April 2014 establishing as part of the Internal Security Fund, the Instrument for financial support for externalborders and visa and repealing Decision No 574/2007/EC (OJ L 150, 20.5.2014, p. 143).

([21]) OJ L 123, 12.5.2016, p. 1.

(72) Implementing powers should also be conferred on the Commission relating to the adoption of detailed rules on: the technical details of the ESP user profiles; the specifications of the technical solution allowing the EU information systems, Europol data and Interpol databases to be queried through the ESP and the format of the ESP's replies; the technical rules for creating links in the MID between data from different EU information systems; the content and presentation of the form to be used to inform the data subject when a red link is created; the performance requirements and performance monitoring of the shared BMS; automated data quality control mechanisms, procedures and indicators; the development of the UMF standard; the cooperation procedure to be used in the case of a security incident; and the specifications of the technical solution for Member States to manage users access requests. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council ([22]).

(73) As the interoperability components will involve the processing of significant amounts of sensitive personal data, it is important that persons whose data are processed through those components can effectively exercise their rights as data subjects as required under Regulation (EU) 2016/679, Directive (EU) 2016/680 and Regulation (EU) 2018/1725. The data subjects should be provided with a web portal that facilitates their exercise of their rights of access to, rectification, erasure and restriction of processing of their personal data. eu-LISA should establish and manage such a web portal.

(74) One of the core principles of data protection is data minimisation: under Article 5(1)(c) of Regulation (EU) 2016/679, the processing of personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. For this reason, the interoperability components should not provide for the storage of any new personal data, with the exception of the links which will be stored in the MID and which are the minimum necessary for the purposes of this Regulation.

(75) This Regulation should contain clear provisions on liability and the right to compensation for unlawful processing of personal data and for any other act incompatible with it. Such provisions should be without prejudice to the right to compensation from, and liability of the controller or processor under Regulation (EU) 2016/679, Directive (EU) 2016/680 and Regulation (EU) 2018/1725. eu-LISA should be responsible for any damage it causes in its capacity as a data processor where it has not complied with the obligations specifically imposed on it by this Regulation, or where it has acted outside or contrary to lawful instructions of the Member State which is the data controller.

(76) This Regulation is without prejudice to the application of Directive 2004/38/EC of the European Parliament and of the Council ([23]).

(77) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the TEU and to the TFEU, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Given that this Regulation builds upon the Schengen *acquis*, Denmark shall, in accordance with Article 4 of that Protocol, decide within a period of six months after the Council has decided on this Regulation whether it will implement it in its national law.

(78) This Regulation constitutes a development of the provisions of the Schengen *acquis* in which the United Kingdom does not take part, in accordance with Council Decision 2000/365/EC ([24]); the United Kingdom is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(79) This Regulation constitutes a development of the provisions of the Schengen *acquis* in which Ireland does not take part, in accordance with Council Decision 2002/192/EC ([25]); Ireland is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

([22]) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

([23]) Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (OJ L 158, 30.4.2004, p. 77).

([24]) Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis* (OJ L 131, 1.6.2000, p. 43).

([25]) Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen *acquis* (OJ L 64, 7.3.2002, p. 20).

(80) As regards Iceland and Norway, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latters' association with the implementation, application and development of the Schengen *acquis* ([26]) which fall within the area referred to in Article 1, points A, B, C and G of Council Decision 1999/437/EC ([27]).

(81) As regards Switzerland, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* ([28]) which fall within the area referred to in Article 1, points A, B, C and G of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/146/EC ([29]).

(82) As regards Liechtenstein, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* ([30]) which fall within the area referred to in Article 1, points A, B, C and G of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU ([31]).

(83) This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union and should be applied in accordance with those rights and principles.

(84) In order to have this Regulation fit into the existing legal framework, Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861, and Council Decisions 2004/512/EC ([32]) and 2008/633/JHA ([33]) should be amended accordingly,

HAVE ADOPTED THIS REGULATION:

CHAPTER I

General provisions

Article 1

Subject matter

1. This Regulation, together with Regulation (EU) 2019/818 of the European Parliament and of the Council ([34]), establishes a framework to ensure 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).

([26]) OJ L 176, 10.7.1999, p. 36.
([27]) Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis* (OJ L 176, 10.7.1999, p. 31).
([28]) OJ L 53, 27.2.2008, p. 52.
([29]) Council Decision 2008/146/EC of 28 January 2008 on the conclusion, on behalf of the European Community, of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L 53, 27.2.2008, p. 1).
([30]) OJ L 160, 18.6.2011, p. 21.
([31]) Council Decision 2011/350/EU of 7 March 2011 on the conclusion, on behalf of the European Union, of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*, relating to the abolition of checks at internal borders and movement of persons (OJ L 160, 18.6.2011, p. 19).
([32]) Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS) (OJ L 213, 15.6.2004, p. 5).
([33]) Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (OJ L 218, 13.8.2008, p. 129).
([34]) Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (See page 85 of this Official Journal).

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).

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 on 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, development and operation of the interoperability components.

4. This Regulation also adapts the procedures and conditions for the designated authorities and for the European Union Agency for Law Enforcement Cooperation (Europol) to access the EES, VIS, ETIAS and Eurodac for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences.

5. This Regulation also lays down a framework for verifying the identity of persons and for identifying persons.

Article 2

Objectives

1. By ensuring interoperability, this Regulation has the following objectives:

(a) to improve the effectiveness and efficiency of border checks at external borders;

(b) to contribute to the prevention and the combating of illegal immigration;

(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 security in the territories of the Member States;

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

(e) to assist in the examination of applications for international protection;

(f) to contribute to the prevention, detection and investigation of terrorist offences and of other serious criminal offences;

(g) to facilitate the identification of unknown persons who are unable to identify themselves or unidentified human remains in case of a natural disaster, accident or terrorist attack.

2. The objectives referred to in paragraph 1 shall be achieved by:

(a) ensuring the correct identification of persons;

(b) contributing to combating identity fraud;

(c) improving data quality and harmonising the quality requirements for the data stored in the EU information systems while respecting the data processing requirements of the legal instruments governing the individual systems, data protection standards and principles;

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

(e) strengthening, simplifying and making more uniform the data security and data protection conditions that govern the respective EU information systems, without affecting the special protection and safeguards afforded to certain categories of data;

(f) streamlining the conditions for designated authorities' access to the EES, VIS, ETIAS and Eurodac, while ensuring necessary and proportionate conditions for that access;

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

Article 3

Scope

1. This Regulation applies to the EES, VIS, ETIAS and 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 of this Article and whose data are collected for the purposes defined in Articles 1 and 2 of Regulation (EC) No 767/2008, Article 1 of Regulation (EU) 2017/2226, Articles 1 and 4 of Regulation (EU) 2018/1240, Article 1 of Regulation (EU) 2018/1860 and Article 1 of Regulation (EU) 2018/1861.

Article 4

Definitions

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

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

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

(3) 'border authority' means the border guard assigned in accordance with national law to carry out border checks;

(4) 'supervisory authorities' means the supervisory authority referred to in Article 51(1) of Regulation (EU) 2016/679 and the supervisory authority referred to in 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) 'alphanumeric data' means data represented by letters, digits, special characters, spaces and punctuation marks;

(8) 'identity data' means the data referred to in Article 27(3)(a) to (e);

(9) 'fingerprint data' means fingerprint images and images of fingerprint latents, which due to their unique character and the reference points contained therein enable accurate and conclusive comparisons on a person's identity;

(10) 'facial image' means digital images of the face;

(11) 'biometric data' means fingerprint data or facial images or both;

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

(13) 'travel document' means a passport or other equivalent document entitling the holder to cross the external borders and to which a visa can be affixed;

(14) '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;

(15) 'EU information systems' means the EES, VIS, ETIAS, Eurodac, SIS and ECRIS-TCN;

(16) 'Europol data' means personal data processed by Europol for the purpose referred to in Article 18(2)(a), (b) and (c) of Regulation (EU) 2016/794;

(17) 'Interpol databases' means the Interpol Stolen and Lost Travel Document database (SLTD database) and the Interpol Travel Documents Associated with Notices database (TDAWN database);

(18) 'match' means the existence of a correspondence as a result of an automated comparison between personal data recorded or being recorded in an information system or database;

(19) 'police authority' means the competent authority as defined in point (7) of Article 3 of Directive (EU) 2016/680;

(20) 'designated authorities' means the Member State designated authorities as defined in point (26) of Article 3(1) of Regulation (EU) 2017/2226, point (e) of Article 2(1) of Decision 2008/633/JHA and point (21) Article 3(1) of Regulation (EU) 2018/1240;

(21) '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 of the European Parliament and of the Council ([35]);

(22) 'serious criminal offence' means an offence which corresponds or is equivalent to one of the offences referred to in Article 2(2) of Council Framework Decision 2002/584/JHA ([36]), if it is punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years;

(23) 'Entry/Exit System' or 'EES' means the Entry/Exit System established by Regulation (EU) 2017/2226;

(24) 'Visa Information System' or 'VIS' means the Visa Information System established by Regulation (EC) No 767/2008;

(25) 'European Travel Information and Authorisation System' or 'ETIAS' means the European Travel Information and Authorisation System established by Regulation (EU) 2018/1240;

(26) 'Eurodac' means Eurodac established by Regulation (EU) No 603/2013 of the European Parliament and of the Council ([37]);

(27) 'Schengen Information System' or 'SIS' means the Schengen Information System established by Regulations (EU) 2018/1860, (EU) 2018/1861 and (EU) 2018/1862;

(28) 'ECRIS-TCN' means the centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons established by Regulation (EU) 2019/816 of the European Parliament and of the Council ([38]).

Article 5

Non-discrimination and fundamental rights

Processing of personal data for the purposes of this Regulation shall not result in discrimination against persons on any grounds such as gender, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation. It shall fully respect human dignity and integrity and fundamental rights, including the right to respect for one's private life and to the protection of personal data. Particular attention shall be paid to children, the elderly, persons with a disability and persons in need of international protection. The best interests of the child shall be a primary consideration.

CHAPTER II

European search portal

Article 6

European search portal

1. A European search portal (ESP) is established for the purposes of facilitating the fast, seamless, efficient, systematic and controlled access of Member State authorities and Union agencies to the EU information systems, to Europol data and to the Interpol databases for the performance of their tasks and in accordance with their access rights and the objectives and purposes of the EES, VIS, ETIAS, Eurodac, SIS and ECRIS-TCN.

([35]) Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, p. 6).

([36]) Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1).

([37]) Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 180, 29.6.2013, p. 1).

([38]) Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 (See page 1 of this Official Journal).

2. The ESP shall be composed of:

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

(b) a secure communication channel between the ESP, Member States and Union agencies that are entitled to use the ESP;

(c) a secure communication infrastructure between the ESP and the EES, VIS, ETIAS, Eurodac, Central SIS, ECRIS-TCN, Europol data and the Interpol databases as well as between the ESP and the central infrastructures of the CIR and the 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 Union agencies having access to at least one of the EU information systems in accordance with the legal instruments governing those EU information systems, to the CIR and the MID in accordance with this Regulation, to Europol data in accordance with Regulation (EU) 2016/794 or to the Interpol databases in accordance with Union or national law governing such access.

Those Member State authorities and Union agencies may make use of the ESP and the data provided by it only for the objectives and purposes laid down in the legal instruments governing those EU information systems, in Regulation (EU) 2016/794 and in this Regulation.

2. The Member State authorities and Union agencies 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, VIS and ETIAS in accordance with their access rights as referred to in the legal instruments governing those EU information systems and in 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 Regulations (EU) 2018/1860 and (EU) 2018/1861.

4. Where provided for under Union law, the Union agencies referred to in paragraph 1 shall use the ESP to search data related to persons or their travel documents in the Central SIS.

5. The Member State authorities and Union agencies referred to in paragraph 1 may use the ESP to search data related to travel documents in the Interpol databases, where provided for and 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 shall, in cooperation with Member States, create a profile based on each category of ESP user and on the purposes of the queries, in accordance with the technical details and access rights referred to in paragraph 2. Each profile shall, in accordance with Union and national law, comprise the following information:

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

(b) the EU information systems, Europol data and the Interpol databases that are to be queried, those that can be queried and those that are to provide a reply to the user;

(c) the specific data in the EU information systems, Europol data and the Interpol databases that may be queried;

(d) the categories of data that may be provided in each reply.

2. The Commission shall adopt implementing acts to specify the technical details of the profiles referred to in paragraph 1 in accordance with the ESP users' access rights under the legal instruments governing the EU information systems and under national law. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 74(2).

3. The profiles referred to in paragraph 1 shall be reviewed regularly by eu-LISA in cooperation with Member States, at least once per year, and if necessary updated.

Article 9

Queries

1. The ESP users shall launch a query by submitting alphanumeric or biometric data to the ESP. Where a query has been launched, the ESP shall query the EES, ETIAS, VIS, SIS, Eurodac, ECRIS-TCN, the CIR, Europol data and the Interpol databases simultaneously with the data submitted by the user and in accordance with the user profile.

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

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

4. When a query is launched by an ESP user, the EES, ETIAS, VIS, SIS, Eurodac, ECRIS-TCN, the CIR, the MID, the Europol data and the Interpol databases shall in reply to the query provide the data that they hold.

Without prejudice to Article 20, the reply provided by the ESP shall indicate to which EU information system or database the data belong.

The ESP shall provide no information regarding data in EU information systems, Europol data and the Interpol databases to which the user has no access under the applicable Union and national law.

5. Any queries of the Interpol databases launched via the ESP shall be performed in such a way that no information shall be revealed to the owner of the Interpol alert.

6. The ESP shall provide replies to the user as soon as data are available from one of the EU information systems, Europol data or Interpol databases. Those replies shall contain only the data to which the user has access under Union and national law.

7. The Commission shall adopt an implementing act to specify the technical procedure for the ESP to query the EU information systems, Europol data and Interpol databases and the format of the ESP replies. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 74(2).

Article 10

Keeping of logs

1. Without prejudice to Article 46 of Regulation (EU) 2017/2226, Article 34 of Regulation (EC) No 767/2008, Article 69 of Regulation (EU) 2018/1240 and Articles 12 and 18 of Regulation (EU) 2018/1861, eu-LISA shall keep logs of all data processing operations in the ESP. Those logs shall include the following:

(a) the Member State or Union agency launching the query and the ESP profile used;

(b) the date and time of the query;

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

2. Each Member State shall keep logs of queries that its authorities and the staff of those authorities duly authorised to use the ESP make. Each Union agency shall keep logs of queries that its duly authorised staff make.

3. The logs referred to in paragraphs 1 and 2 may be used only for data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, and for ensuring data security and integrity. Those logs shall be protected by appropriate measures against unauthorised access and erased one year after their creation. If, however, they are required for monitoring procedures that have already begun, they shall be erased once the monitoring procedures no longer require the logs.

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 or the CIR, because of a failure of the ESP, the ESP users shall be notified in an automated manner by eu-LISA.

2. Where it is technically impossible to use the ESP to query one or several EU information systems or the CIR, because of a failure of the national infrastructure in a Member State, that Member State shall notify eu-LISA and the Commission in an automated manner.

3. In the cases referred to in paragraphs 1 or 2 of this Article, and until the technical failure is addressed, the obligation referred to in Article 7(2) and (4) shall not apply and Member States shall access the EU information systems or the CIR directly where they are required to do so under Union or national law.

4. Where it is technically impossible to use the ESP to query one or several EU information systems or the CIR, because of a failure of the infrastructure of a Union agency, that agency shall notify eu-LISA and the Commission in an automated manner.

CHAPTER III

Shared biometric matching service

Article 12

Shared biometric matching service

1. A shared biometric matching service (shared BMS) storing biometric templates obtained from the biometric data referred to in Article 13 that are stored in the CIR and SIS and enabling querying with biometric data across several EU information systems is established for the purposes of supporting the CIR and the MID and the objectives of the EES, VIS, Eurodac, SIS and ECRIS-TCN.

2. The shared BMS shall be composed of:

(a) a central infrastructure, which shall replace the central systems of the EES, VIS, SIS, Eurodac and ECRIS-TCN respectively, to the extent that it shall store biometric templates and allow searches with biometric data;

(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

Storing biometric templates in the shared biometric matching service

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

(a) the data referred to in Article 16(1)(d), 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 point (6) of Article 9 of Regulation (EC) No 767/2008;

(c) the data referred to in Article 20(2)(w) and (x), excluding data on palm prints, of Regulation (EU) 2018/1861;

(d) the data referred to in Article 4(1)(u) and (v), excluding data on palm prints, of Regulation (EU) 2018/1860.

The biometric templates shall be stored in the shared BMS in logically separated form according to the EU information system from which the data originate.

2. For each set of data referred to in paragraph 1, the shared BMS shall include in each biometric template a reference to the EU information systems in which the corresponding biometric data are stored and a reference to the actual records in those EU information systems.

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 EU 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).

5. The Commission shall lay down, by means of an implementing act, the performance requirements and practical arrangements for monitoring the performance of the shared BMS in order to ensure that the effectiveness of biometric searches respect time-critical procedures such as border checks and identifications. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 74(2).

Article 14

Searching biometric data with the shared biometric matching service

In order to search the biometric data stored within the CIR and SIS, the CIR and 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 Regulations (EC) No 767/2008, (EU) 2017/2226, (EU) 2018/1860, (EU) 2018/1861, (EU) 2018/1862 and (EU) 2019/816.

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 only for as long as the corresponding biometric data are stored in the CIR or SIS. The data shall be erased from the shared BMS in an automated manner.

Article 16

Keeping of logs

1. Without prejudice to Article 46 of Regulation (EU) 2017/2226, Article 34 of Regulation (EC) No 767/2008 and Articles 12 and 18 of Regulation (EU) 2018/1861, eu-LISA shall keep logs of all data processing operations in the shared BMS. Those logs shall include the following:

(a) the Member State or Union agency launching the query;

(b) the history of the creation and storage of biometric templates;

(c) the EU information systems queried with the biometric templates stored in the shared BMS;

(d) the date and time of the query;

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

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

2. Each Member State shall keep logs of queries that its authorities and the staff of those authorities duly authorised to use the shared BMS make. Each Union agency shall keep logs of queries that its duly authorised staff make.

3. The logs referred to in paragraphs 1 and 2 may be used only for data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, and for ensuring data security and integrity. Those logs shall be protected by appropriate measures against unauthorised access and erased one year after their creation. If, however, they are required for monitoring procedures that have already begun, they shall be erased once the monitoring procedures no longer require the logs.

CHAPTER IV

Common identity repository

Article 17

Common identity repository

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

2. The CIR shall be composed of:

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

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

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

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

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

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

Article 18

The common identity repository data

1. The CIR shall store the following data, logically separated according to the information system from which the data have originated:

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

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

(c) the data referred to in Article 17(2)(a) to (e) of Regulation (EU) 2018/1240;

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

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

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

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

Article 19

Adding, amending and deleting data in the common identity repository

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

Article 20

Access to the common identity repository for identification

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

(a) where a police authority is unable to identify a person due to the lack of a travel document or another credible document proving that person's identity;

(b) where there are doubts about the identity data provided by a person;

(c) where there are doubts as to the authenticity of the travel document or another credible document provided by a person;

(d) where there are doubts as to the identity of the holder of a travel document or of another credible document; or

(e) where a person is unable or refuses to cooperate.

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

2. Where one of the circumstances listed in paragraph 1 arises and a police authority has been so empowered by national legislative measures as referred to in paragraph 5, it may, solely for the purpose of identifying a person, query the CIR with the biometric data of that person taken live during an identity check, provided that the procedure was initiated in the presence of that person.

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

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

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

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

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

Article 21

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

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

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

Article 22

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

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

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

The reply indicating that data on that person are present in any of the EU information systems referred to in paragraph 1 shall be used only for the purposes of submitting a request for full access subject to the conditions and procedures laid down in the respective legal instruments governing such access.

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

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

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

Article 23

Data retention in the common identity repository

1. The data referred to in Article 18(1), (2) and (4) shall be deleted from the CIR in an automated manner in accordance with the data retention provisions of Regulations (EU) 2017/2226, (EC) No 767/2008 and (EU) 2018/1240 respectively.

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

Article 24

Keeping of logs

1. Without prejudice to Article 46 of Regulation (EU) 2017/2226, Article 34 of Regulation (EC) No 767/2008 and Article 69 of Regulation (EU) 2018/1240, eu-LISA shall keep logs of all data processing operations in the CIR in accordance with paragraphs 2, 3 and 4 of this Article.

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

(a) the Member State or Union agency launching the query;

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

(c) the date and time of the query;

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

(e) the results of the query.

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

(a) the Member State or Union agency launching the query;

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

(c) the date and time of the query;

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

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

(a) the date and time of the query;

(b) the data used to launch the query;

(c) the results of the query;

(d) the Member State or Union agency querying the CIR.

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

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

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

(a) the national file reference;

(b) the purpose of access;

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

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

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

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

CHAPTER V

Multiple-identity detector

Article 25

Multiple-identity detector

1. A multiple-identity detector (MID) creating and storing identity confirmation files as referred to in Article 34, containing links between data in the EU information systems included in the CIR and SIS and allowing detection of 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, VIS, ETIAS, Eurodac, SIS and ECRIS-TCN.

2. The MID shall be composed of:

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

(b) a secure communication infrastructure to connect the MID with SIS and the central infrastructures of the ESP 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 verification of different identities referred to in Article 29, access to the data referred to in Article 34 stored in the MID shall be granted to:

(a) competent authorities designated in accordance with Article 9(2) of Regulation (EU) 2017/2226 when creating or updating an individual file in the EES in accordance with Article 14 of that Regulation;

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

(c) the ETIAS Central Unit and the ETIAS National Units when carrying out the processing referred to in Articles 22 and 26 of Regulation (EU) 2018/1240;

(d) the SIRENE Bureau of the Member State creating or updating a SIS alert in accordance with Regulations (EU) 2018/1860 and (EU) 2018/1861.

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

3. Member State authorities and Union agencies shall have access to the white links referred to in Article 33 where they have access to the two EU information systems containing data between which the white link was created.

4. Member State authorities and Union agencies shall have access to the green links referred to in Article 31 where they have access to the two EU information systems containing data between which the green link was created and a query of those information systems has revealed a match with the two sets of linked data.

Article 27

Multiple-identity detection

1. Multiple-identity detection in the CIR and SIS shall be launched where:

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

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

(c) an application file is created or updated in ETIAS in accordance with Article 19 of Regulation (EU) 2018/1240;

(d) an alert on a person is created or updated in SIS in accordance with Article 3 of Regulation (EU) 2018/1860 and Chapter V of Regulation (EU) 2018/1861.

2. Where the data contained within an EU information system referred to in paragraph 1 contains biometric data, the CIR and Central SIS shall use the shared BMS in order to perform 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 data belonging to the same person are already stored in the CIR or in Central SIS.

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

(a) surname (family name); first name or names (given names); date of birth; nationality or nationalities; and sex; as referred to in Articles 16(1)(a), 17(1) and 18(1) of Regulation (EU) 2017/2226;

(b) surname (family name); first name or names (given names); date of birth; sex; place and country of birth; and nationalities; as referred to in point (4)(a) and (aa) of Article 9 of Regulation (EC) No 767/2008;

(c) surname (family name), first name(s) (given name(s)), surname at birth; alias(es); date of birth, place of birth, sex and current nationality; as referred to in Article 17(2) of Regulation (EU) 2018/1240;

(d) surnames, forenames, names at birth, previously used names and aliases, place of birth, date of birth, gender and any nationalities held, as referred to in Article 20(2) of Regulation (EU) 2018/1861;

(e) surnames, forenames, names at birth, previously used names and aliases, place of birth, date of birth, gender and any nationalities held, as referred to in Article 4 of Regulation (EU) 2018/1860.

4. In addition to the process referred to in paragraphs 2 and 3, the CIR and Central SIS shall use the ESP to search the data stored in Central SIS and the CIR respectively using travel document data.

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

Article 28

Results of the multiple-identity detection

1. Where the queries referred to in Article 27(2), (3) and (4) do not report any match, the procedures referred to in Article 27(1) shall continue in accordance with the legal instruments governing them.

2. Where the query laid down in Article 27(2), (3) and (4) reports one or several matches, the CIR and, where relevant, SIS shall create a link between the data used to launch the query and the data triggering the match.

Where several matches are reported, a link shall be created between all data triggering the match. Where the data were 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), (3) and (4) reports one or several matches and the identity data of the linked files are the same or similar, a white link shall be created in accordance with Article 33.

4. Where the query referred to in Article 27(2), (3) and (4) reports one or several matches and the identity data of the linked files cannot be considered to be 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 adopt delegated acts in accordance with Article 73 laying down the procedures to determine the cases in which identity data can be considered to be the same or similar.

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

7. The Commission shall, in cooperation with eu-LISA, lay down the technical rules for creating links between data from different EU information systems, by implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 74(2).

Article 29

Manual verification of different identities and the authorities responsible

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

(a) the competent authority designated in accordance with Article 9(2) of Regulation (EU) 2017/2226 for matches that occurred when creating or updating an individual file in the EES in accordance with that Regulation;

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

(c) the ETIAS Central Unit and the ETIAS National Units for matches that occurred when creating or updating an application file in accordance with Regulation (EU) 2018/1240;

(d) the SIRENE Bureau of the Member State for matches that occurred when creating or updating a SIS alert in accordance with Regulations (EU) 2018/1860 and (EU) 2018/1861.

The MID shall indicate the authority responsible for the manual verification of different identities in the identity confirmation file.

2. The authority responsible for the manual 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 in an alert:

(a) in respect of persons wanted for arrest for surrender or extradition purposes referred to in Article 26 of Regulation (EU) 2018/1862;

(b) on missing or vulnerable persons referred to in Article 32 of Regulation (EU) 2018/1862;

(c) on persons sought to assist with a judicial procedure referred to in Article 34 of Regulation (EU) 2018/1862;

(d) on persons for discreet checks, inquiry checks or specific checks referred to in Article 36 of Regulation (EU) 2018/1862.

3. Without prejudice to paragraph 4 of this Article, the authority responsible for the manual verification of different identities shall have access to the linked data contained in the relevant identity confirmation file and to the identity data linked in the CIR and, where relevant, in SIS. It shall assess the different identities without delay. Once such assessment is completed, it 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 manual verification of different identities in the identity confirmation file is the competent authority designated in accordance with Article 9(2) of Regulation (EU) 2017/2226 creating or updating an individual file in the EES in accordance with Article 14 of that Regulation, and where a yellow link is created, that authority shall carry out additional verifications. That authority shall, for that purpose only, have access to the related data contained in the relevant identity confirmation file. It shall assess the different identities, update the link in accordance with Articles 31, 32 and 33 of this Regulation and add it to the identity confirmation file without delay.

Such manual verification of different identities shall be initiated in the presence of the person concerned, who shall be offered the opportunity to explain the circumstances to the authority responsible, which shall take those explanations into account.

In cases in which the manual verification of different identities takes place at the border, it shall take place within 12 hours from the creation of a yellow link under Article 28(4), where possible.

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

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

Article 30

Yellow link

1. Where manual verification of different identities has not yet taken place, a link between data from two or more EU information systems shall be classified as yellow in any of the following cases:

(a) the linked data share the same biometric data but have similar or different identity data;

(b) the linked data have different identity data but share the same travel document data, and at least one of the EU information systems does not contain biometric data on the person concerned;

(c) the linked data share the same identity data but have different biometric data;

(d) the linked data have similar or different identity data, and share the same travel document data, but have different biometric data.

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 EU information systems shall be classified as green where:

(a) the linked data have different biometric data but share the same identity data and the authority responsible for the manual verification of different identities has concluded that the linked data refer to two different persons;

(b) the linked data have different biometric data, have similar or different identity data, share the same travel document data and the authority responsible for the manual verification of different identities has concluded that the linked data refer to two different persons;

(c) the linked data have different identity data but share the same travel document data, at least one of the EU information systems does not contain biometric data on the person concerned and the authority responsible for the manual verification of different identities has concluded that the linked data refer to two different persons.

2. Where the CIR or SIS are queried and where a green link exists between data in two or more of the EU information systems, the MID shall indicate that the identity data of the linked data do not correspond to the same person.

3. If a Member State authority has evidence to suggest that a green link has been incorrectly recorded in the MID, that a green link is out of date or that data were processed in the MID or the EU information systems 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 of different identities without delay.

Article 32

Red link

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

(a) the linked data share the same biometric data but have similar or different identity data and the authority responsible for the manual verification of different identities has concluded that the linked data refer to the same person in an unjustified manner;

(b) the linked data have the same, similar or different identity data and the same travel document data, but different biometric data and the authority responsible for the manual verification of different identities has concluded that the linked data refer to two different persons, at least one of whom is using the same travel document in an unjustified manner;

(c) the linked data share the same identity data, but have different biometric data and different or no travel document data and the authority responsible for the manual verification of different identities has concluded that the linked data refer to two different persons in an unjustified manner;

(d) the linked data have different identity data, but share the same travel document data, at least one of the EU information systems does not contain biometric data on the person concerned and the authority responsible for the manual verification of different identities has concluded that the linked data refer to the same person in an unjustified manner.

2. Where the CIR or SIS are queried and where a red link exists between data in two or more of the EU information systems, the MID shall indicate the data referred to in Article 34. Follow-up to a red link shall take place in accordance with Union and national law, with any legal consequence for the person concerned being based only on the relevant data on that person. No legal consequence for the person concerned shall derive solely from the existence of a red link.

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

4. Without prejudice to the provisions related to the handling of alerts in SIS contained in Regulations (EU) 2018/1860, (EU) 2018/1861 and (EU) 2018/1862, and without prejudice to limitations necessary to protect security and public order, prevent crime and guarantee that no national investigation will be jeopardised, where a red link is created, the authority responsible for the manual verification of different identities shall inform the person concerned of the presence of multiple unlawful identity data and shall provide the person with the single identification number referred to in Article 34(c) of this Regulation, a reference to the authority responsible for the manual verification of different identities referred to in Article 34(d) of this Regulation and the website address of the web portal established in accordance with Article 49 of this Regulation.

5. The information referred to in paragraph 4 shall be provided in writing by means of a standard form by the authority responsible for the manual verification of different identities. The Commission shall determine the content and presentation of that form by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 74(2).

6. Where a red link is created, the MID shall notify the authorities responsible for the linked data in an automated manner.

7. If a Member State authority or Union agency having access to the CIR or SIS has evidence to suggest that a red link has been incorrectly recorded in the MID or that data were processed in the MID, the CIR or SIS in breach of this Regulation, that authority or agency shall check the relevant data stored in the CIR and SIS and shall:

(a) where the link relates to one of the SIS alerts referred to in Article 29(2), immediately inform the relevant SIRENE Bureau of the Member State that created the SIS alert;

(b) in all other cases, either rectify or erase the link from the MID immediately.

If a SIRENE Bureau is contacted pursuant to point (a) of the first subparagraph, it shall verify the evidence provided by the Member State authority or the Union agency and where relevant rectify or erase the link from the MID immediately.

The Member State authority obtaining the evidence shall inform the Member State authority responsible for the manual verification of different identities without delay of any relevant rectification or erasure of a red link.

Article 33

White link

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

(a) the linked data share the same biometric data and the same or similar identity data;

(b) the linked data share the same or similar identity data, the same travel document data, and at least one of the EU information systems does not have biometric data on the person concerned;

(c) the linked data share the same biometric data, the same travel document data and similar identity data;

(d) the linked data share the same biometric data but have similar or different identity data and the authority responsible for the manual verification of different identities has concluded that linked data refer to the same person in a justified manner.

2. Where the CIR or SIS are queried and where a white link exists between data in two or more of the EU information systems, the MID shall indicate that the identity data of the linked data correspond to the same person. The queried EU information systems shall reply indicating, where relevant, all the linked data on the person, thereby triggering a match against the data that are linked by the white link, if the authority launching the query has access to the linked data under Union or national law.

3. Where a white link is created between data in the EES, VIS, ETIAS, Eurodac or ECRIS-TCN, the individual file stored in the CIR shall be updated in accordance with Article 19(2).

4. Without prejudice to the provisions related to the handling of alerts in SIS contained in Regulations (EU) 2018/1860, (EU) 2018/1861 and (EU) 2018/1862, and without prejudice to limitations necessary to protect security and public order, prevent crime and guarantee that no national investigation will be jeopardised, where a white link is created following a manual verification of different identities, the authority responsible for the manual verification of different identities shall inform the person concerned of the presence of similar or different identity data and shall provide the person with the single identification number referred to in Article 34(c) of this Regulation, a reference to the authority responsible for the manual verification of different identities referred to in Article 34(d) of this Regulation and the website address of the web portal established in accordance with Article 49 of this Regulation.

5. If a Member State authority has evidence to suggest that a white link has been incorrectly recorded in the MID, that a white link is out of date or that data were processed in the MID or the EU information systems 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 of different identities without delay.

6. The information referred to in paragraph 4 shall be in writing by means of a standard form by the authority responsible for the manual verification of different identities. The Commission shall determine the content and presentation of that form by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 74(2).

Article 34

Identity confirmation file

The identity confirmation file shall contain the following data:

(a) the links referred to in Articles 30 to 33;

(b) a reference to the EU information systems in which the linked data are held;

(c) a single identification number allowing retrieval of the linked data from the corresponding EU information systems;

(d) the authority responsible for the manual verification of different identities;

(e) the date of creation of the link or of any update to it.

Article 35

Data retention in the multiple-identity detector

The identity confirmation files and the data in them, including the links, shall be stored in the MID only for as long as the linked data are stored in two or more EU information systems. They shall be erased from the MID in an automated manner.

Article 36

Keeping of logs

1. eu-LISA shall keep logs of all data processing operations in the MID. Those logs shall include the following:

(a) the Member State launching the query;

(b) the purpose of user's access;

(c) the date and time of the query;

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

(e) the reference to the linked data;

(f) the history of the identity confirmation file.

2. Each Member State shall keep logs of queries that its authorities and the staff of those authorities duly authorised to use the MID make. Each Union agency shall keep logs of queries that its duly authorised staff make.

3. The logs referred to in paragraphs 1 and 2 may be used only for data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, and for ensuring data security and integrity. Those logs shall be protected by appropriate measures against unauthorised access and erased one year after their creation. If, however, they are required for monitoring procedures that have already begun, they shall be erased once the monitoring procedures no longer require the logs.

CHAPTER VI

Measures supporting interoperability

Article 37

Data quality

1. Without prejudice to Member States' responsibilities with regard to the quality of data entered into the systems, eu-LISA shall establish automated data quality control mechanisms and procedures on the data stored in the EES, VIS, ETIAS, SIS, the shared BMS and the CIR.

2. eu-LISA shall implement mechanisms for evaluating the accuracy of the shared BMS, common data quality indicators and the minimum quality standards for storage of data in the EES, VIS, ETIAS, SIS, the shared BMS and the CIR.

Only data fulfilling the minimum quality standards may be entered in the EES, VIS, ETIAS, SIS, 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. eu-LISA shall also provide that report to the European Parliament and to the Council upon request. No reports provided under this paragraph shall contain any personal data.

4. The details of the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum quality standards for storage of data in the EES, VIS, ETIAS, SIS, the shared BMS and the CIR, 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 74(2).

5. One year after the establishment of the automated data quality control mechanisms and procedures, common data quality indicators and the minimum data quality standards, and every year thereafter, the Commission shall evaluate Member States' implementation of data quality and 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, in particular, data quality issues deriving from erroneous data in EU information systems. The Member States shall regularly report to the Commission 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, to the European Data Protection Board and to the European Union Agency for Fundamental Rights established by Council Regulation (EC) No 168/2007 ([39]).

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 or organisations in the field of Justice and Home Affairs.

2. The UMF standard shall be used in the development of the EES, ETIAS, the ESP, the CIR, the MID and, if appropriate, in the development by eu-LISA or by any other Union agency of new information exchange models and information systems in the area of Justice and Home Affairs.

3. The Commission shall adopt an implementing act to lay down and develop the UMF standard referred to in paragraph 1 of this Article. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 74(2).

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 the EES, VIS, ETIAS and SIS, in accordance with the respective legal instruments governing those systems, and to provide cross-system statistical data and analytical reporting for policy, operational and data quality purposes.

2. eu-LISA shall establish, implement and host in its technical sites the CRRS containing the data and statistics referred to in Article 63 of Regulation (EU) 2017/2226, Article 17 of Regulation (EC) No 767/2008, Article 84 of Regulation (EU) 2018/1240, Article 60 of Regulation (EU) 2018/1861 and Article 16 of Regulation (EU) 2018/1860, logically separated by EU information system. Access to the CRRS shall be granted by means of controlled, secured access and specific user profiles, solely for the purpose of reporting and statistics, to the authorities referred to in Article 63 of Regulation (EU) 2017/2226, Article 17 of Regulation (EC) No 767/2008, Article 84 of Regulation (EU) 2018/1240 and Article 60 of Regulation (EU) 2018/1861.

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

The data contained in CRRS shall not allow for the identification of individuals.

4. The CRRS shall be composed of:

(a) the tools necessary for anonymising data;

(b) a central infrastructure, consisting of a data repository of anonymous data;

(c) a secure communication infrastructure to connect the CRRS to the EES, VIS, ETIAS and SIS, as well as the central infrastructures of the shared BMS, the CIR and the MID.

5. The Commission shall adopt a delegated act in accordance with Article 73 laying down detailed rules on the operation of the CRRS, including specific safeguards for the processing of personal data under paragraphs 2 and 3 of this Article and security rules applicable to the repository.

([39]) 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).

CHAPTER VII

Data protection

Article 40

Data controller

1. In relation to the processing of data in the shared BMS, the Member State authorities that are controllers for the EES, VIS and SIS respectively shall be controllers in accordance with point (7) of Article 4 of Regulation (EU) 2016/679 or point (8) of Article 3 of Directive (EU) 2016/680 in relation to the biometric templates obtained from the data referred to in Article 13 of this Regulation that they enter into the underlying 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 CIR, the Member State authorities that are controllers for the EES, VIS and ETIAS respectively, shall be controllers in accordance with point (7) of Article 4 of Regulation (EU) 2016/679 in relation to data referred to in Article 18 of this Regulation that they enter into the underlying systems and shall have responsibility for the processing of those personal data in the CIR.

3. In relation to the processing of data in the MID:

(a) the European Border and Coast Guard Agency shall be a data controller within the meaning of point (8) of Article 3 of Regulation (EU) 2018/1725 in relation to the processing of personal data by the ETIAS Central Unit;

(b) the Member State authorities adding or modifying the data in the identity confirmation file shall be controllers in accordance with point (7) of Article 4 of Regulation (EU) 2016/679 or point (8) of Article 3 of Directive (EU) 2016/680 and shall have responsibility for the processing of the personal data in the MID.

4. For the purposes of data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, the data controllers shall have access to the logs referred to in Articles 10, 16, 24 and 36 for self-monitoring as referred to in Article 44.

Article 41

Data processor

In relation to the processing of personal data in the shared BMS, the CIR and the MID, eu-LISA shall be the data processor within the meaning of point (12)(a) of Article 3 of Regulation (EU) 2018/1725.

Article 42

Security of processing

1. eu-LISA, the ETIAS Central Unit, Europol and the Member State authorities shall ensure the security of the processing of personal data that takes place pursuant to this Regulation. eu-LISA, the ETIAS Central Unit, Europol and the Member State authorities shall cooperate on security-related tasks.

2. Without prejudice to Article 33 of Regulation (EU) 2018/1725, eu-LISA shall take the necessary measures to ensure the security of the interoperability components and their related communication infrastructure.

3. In particular, eu-LISA shall adopt the necessary measures, including a security plan, a business continuity plan and a disaster recovery plan, in order to:

(a) physically protect data, including by making contingency plans for the protection of critical infrastructure;

(b) deny unauthorised persons access to data-processing equipment and installations;

(c) prevent the unauthorised reading, copying, modification or removal of data media;

(d) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of recorded personal data;

(e) prevent the unauthorised processing of data and any unauthorised copying, modification or deletion of data;

(f) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment;

(g) ensure that persons authorised to access the interoperability components have access only to the data covered by their access authorisation, by means of individual user identities and confidential access modes only;

(h) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment;

(i) ensure that it is possible to verify and establish what data have been processed in the interoperability components, when, by whom and for what purpose;

(j) prevent the unauthorised reading, copying, modification or deletion of personal data during the transmission of personal data to or from the interoperability components or during the transport of data media, in particular by means of appropriate encryption techniques;

(k) ensure that, in the event of interruption, installed systems can be restored to normal operation;

(l) ensure reliability by making sure that any faults in the functioning of the interoperability components are properly reported;

(m) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Regulation and to assess those security measures in the light of new technological developments.

4. Member States, Europol and the ETIAS Central Unit shall take measures equivalent to those referred to in paragraph 3 as regards security in respect of the processing of personal data by the authorities having a right to access any of the interoperability components.

Article 43

Security incidents

1. Any event that has or may have an impact on the security of the interoperability components and may cause damage to or loss of data stored in them shall be considered to be a security incident, in particular where unauthorised access to data may have occurred or where the availability, integrity and confidentiality of data has or may have been compromised.

2. Security incidents shall be managed so as to ensure a quick, effective and proper response.

3. Without prejudice to the notification and communication of a personal data breach pursuant to Article 33 of Regulation (EU) 2016/679, Article 30 of Directive (EU) 2016/680, or both, Member States shall notify the Commission, eu-LISA, the competent supervisory authorities and the European Data Protection Supervisor of any security incidents without delay.

Without prejudice to Articles 34 and 35 of Regulation (EU) 2018/1725 and Article 34 of Regulation (EU) 2016/794, the ETIAS Central Unit and Europol shall notify the Commission, eu-LISA and the European Data Protection Supervisor of any security incidents without delay.

In the event of a security incident in relation to the central infrastructure of the interoperability components, eu-LISA shall notify the Commission and the European Data Protection Supervisor without delay.

4. Information regarding a security incident that has or may have an impact on the operation of the interoperability components or on the availability, integrity and confidentiality of the data shall be provided to the Member States, the ETIAS Central Unit and Europol without delay and reported in compliance with the incident management plan to be provided by eu-LISA.

5. The Member States concerned, the ETIAS Central Unit, Europol and eu-LISA shall cooperate in the event of a security incident. The Commission shall lay down the specifications of this cooperation procedure by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 74(2).

Article 44

Self-monitoring

Member States and the relevant Union agencies shall ensure that each authority entitled to access the interoperability components takes the measures necessary to monitor its compliance with this Regulation and cooperates, where necessary, with the supervisory authority.

The data controllers referred to in Article 40 shall take the necessary measures to monitor the compliance of data processing pursuant to this Regulation, including through frequent verification of the logs referred to in Articles 10, 16, 24 and 36, and cooperate, where necessary, with the supervisory authorities and with the European Data Protection Supervisor.

Article 45

Penalties

Member States shall ensure that any misuse of data, processing of data or exchange of data contrary to this Regulation is punishable in accordance with national law. The penalties provided shall be effective, proportionate and dissuasive.

Article 46

Liability

1. Without prejudice to the right to compensation from, and liability of the controller or processor under Regulation (EU) 2016/679, Directive (EU) 2016/680 and Regulation (EU) 2018/1725:

(a) any person or Member State that has suffered material or non-material damage as a result of an unlawful personal da processing operation or any other act incompatible with this Regulation by a Member State shall be entitled to receive compensation from that Member State;

(b) any person or Member State that has suffered material or non-material damage as a result of any act by Europol, the European Border and Coast Guard Agency or eu-LISA incompatible with this Regulation shall be entitled to receive compensation from the agency in question.

The Member State concerned, Europol, the European Border and Coast Guard Agency or eu-LISA shall be exempted from their liability under the first subparagraph, in whole or in part, if they prove that they are not responsible for the event which gave rise to the damage.

2. If any failure of a Member State to comply with its obligations under this Regulation causes damage to the interoperability components, that Member ate shall be liable for such damage, unless and insofar as eu-LISA or another Member State bound by this Regulation failed to take reasonable measures to prevent the damage from occurring or to minimise its impact.

3. Claims for compensation against a Member State for the damage referred to in paragraphs 1 and 2 shall be governed by the national law of the defendant Member State. Claims for compensation against the controller or eu-LISA for the damage referred to in paragraphs 1 and 2 shall be subject to the conditions provided for in the Treaties.

Article 47

Right to information

1. The authority collecting the personal data to be stored in the shared BMS, the CIR or the MID shall provide the persons whose data are collected with the information required under Articles 13 and 14 of Regulation (EU) 2016/679, Articles 12 and 13 of Directive (EU) 2016/680 and Articles 15 and 16 of Regulation (EU) 2018/1725. The authority shall provide the information at the time that such data are collected.

2. All information shall be made available, using clear and plain language, in a linguistic version the person concerned understands or is reasonably expected to understand. This shall include providing information in a manner which is appropriate to the age of the data subjects who are minors.

3. Persons whose data are recorded in the EES, VIS or ETIAS shall be informed about the processing of personal data for the purposes of this Regulation in accordance with paragraph 1 when:

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

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

(c) an application file is created or updated in ETIAS in accordance with Article 19 of Regulation (EU) 2018/1240.

Article 48

Right of access to, rectification and erasure of personal data stored in the MID and restriction of processing thereof

1. In order to exercise their rights under Articles 15 to 18 of Regulation (EU) 2016/679, Articles 17 to 20 of Regulation (EU) 2018/1725 and Articles 14, 15 and 16 of Directive (EU) 2016/680, any person shall have the right to address himself or herself to the competent authority of any Member State, which shall examine and reply to the request.

2. The Member State which examines such a request shall reply without undue delay and in any event within 45 days of receipt of the request. That period may be extended by 15 further days where necessary, taking into account the complexity and number of the requests. The Member State which examines the request shall inform the data subject of any such extension within 45 days of receipt of the request, together with the reasons for the delay. Member States may decide that replies are to be given by central offices.

3. If a request for rectification or erasure of personal data is made to a Member State other than the Member State responsible for the manual verification of different identities, the Member State to which the request has been made shall contact the authorities of the Member State responsible for the manual verification of different identities within seven days. The Member State responsible for the manual verification of different identities shall check the accuracy of the data and the lawfulness of the data processing without undue delay and in any event within 30 days of such contact. That period may be extended by 15 further days where necessary, taking into account the complexity and number of the requests. The Member State responsible for the manual verification of different identities shall inform the Member State which contacted it of any such extension together with the reasons for the delay. The person concerned shall be informed by the Member State which contacted the authority of the Member State responsible for the manual verification of different identities about the further procedure.

4. If a request for rectification or erasure of personal data is made to a Member State where the ETIAS Central Unit was responsible for the manual verification of different identities, the Member State to which the request has been made shall contact the ETIAS Central Unit within seven days to ask for its opinion. The ETIAS Central Unit shall give its opinion without undue delay and in any event within 30 days of being contacted. That period may be extended by 15 further days where necessary, taking into account the complexity and number of the requests. The person concerned shall be informed by the Member State which contacted the ETIAS Central Unit about the further procedure.

5. Where, following an examination, it is found that the data stored in the MID are inaccurate or have been recorded unlawfully, the Member State responsible for the manual verification of different identities or, where there was no Member State responsible for the manual verification of different identities or where the ETIAS Central Unit was responsible for the manual verification of different identities, the Member State to which the request has been made shall rectify or erase those data without any undue delay. The person concerned shall be informed in writing that his or her data have been rectified or erased.

6. Where data stored in the MID are amended by a Member State during their retention period, that Member State shall carry out the processing laid down in Article 27 and, where relevant, Article 29 to determine whether the amended data are to be linked. Where the processing does not report any match, that Member State shall erase the data from the identity confirmation file. Where the automated processing reports one or several matches, that Member State shall create or update the relevant link in accordance with the relevant provisions of this Regulation.

7. Where the Member State responsible for the manual verification of different identities or, where applicable, the Member State to which the request has been made does not agree that data stored in the MID are inaccurate or have been recorded unlawfully, that Member State shall adopt an administrative decision explaining in writing to the person concerned without delay why it is not prepared to rectify or erase data relating to him or her.

8. The decision referred to in paragraph 7 shall also provide the person concerned with information explaining the possibility to challenge the decision taken in respect of the request for access to, rectification, erasure or restriction of processing of personal data and, where relevant, information on how to bring an action or a complaint before the competent authorities or courts, and any assistance, including from the supervisory authorities.

9. Any request for access to, rectification, erasure or restriction of processing of personal data shall contain the necessary information to identify the person concerned. That information shall be used exclusively to enable the exercise of the rights referred to in this Article and shall be erased immediately afterwards.

10. The Member State responsible for the manual verification of different identities or, where applicable, the Member State to which the request has been made shall keep a written record that a request for access to, rectification, erasure or restriction of processing of personal data was made and how it was addressed, and shall make that record available to supervisory authorities without delay.

11. This Article is without prejudice to any limitations and restrictions to the rights set out in this Article pursuant to Regulation (EU) 2016/679 and Directive (EU) 2016/680.

Article 49

Web portal

1. A web portal is established for the purpose of facilitating the exercise of the rights of access to, rectification, erasure or restriction of processing of personal data.

2. The web portal shall contain information on the rights and procedures referred to in Articles 47 and 48 and a user interface enabling persons whose data are processed in the MID and who have been informed of the presence of a red link in accordance with Article 32(4) to receive the contact information of the competent authority of the Member State responsible for the manual verification of different identities.

3. In order to obtain the contact information of the competent authority of the Member State responsible for the manual verification of different identities, the person whose data are processed in the MID should enter the reference to the authority responsible for the manual verification of different identities referred to in Article 34(d). The web portal shall use this reference in order to retrieve the contact information of the competent authority of the Member State responsible for the manual verification of different identities. The web portal shall also include a template e-mail to facilitate communication between the portal user and the competent authority of the Member State responsible for the manual verification of different identities. Such e-mail shall include a field for the single identification number referred to in Article 34(c) in order to allow the competent authority of the Member State responsible for the manual verification of different identities to identify the data concerned.

4. Member States shall provide eu-LISA with the contact details of all authorities that are competent to examine and reply to any request referred to in Articles 47 and 48 and shall regularly review whether those contact details are up to date.

5. eu-LISA shall develop the web portal and ensure its technical management.

6. The Commission shall adopt a delegated act in accordance with Article 73 laying down detailed rules on the operation of the web portal, including the user interface, the languages in which the web portal shall be available and the template e-mail.

Article 50

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

Without prejudice to Article 65 of Regulation (EU) 2018/1240, Articles 25 and 26 of Regulation (EU) 2016/794, Article 41 of Regulation (EU) 2017/2226, Article 31 of Regulation (EC) No 767/2008, and the querying of Interpol databases through the ESP in accordance with Article 9(5) of this Regulation which comply with the provisions of Chapter V of Regulation (EU) 2018/1725 and Chapter V of Regulation (EU) 2016/679, personal data stored in, processed 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.

Article 51

Supervision by the supervisory authorities

1. Each Member State shall ensure that the supervisory authorities independently monitor the lawfulness of the processing of personal data under this Regulation by the Member State concerned, including their transmission to and from the interoperability components.

2. Each Member State shall ensure that the national laws, regulations and administrative provisions adopted pursuant to Directive (EU) 2016/680 are also applicable, where relevant, to access to the interoperability components by police authorities and designated authorities, including in relation to the rights of the persons whose data are so accessed.

3. The supervisory authorities shall ensure that an audit of the personal data processing operations by the responsible national authorities for the purposes of this Regulation is carried out in accordance with relevant international auditing standards at least every four years.

The supervisory authorities shall publish annually the number of requests for rectification, erasure or restriction of processing of personal data, the action subsequently taken and the number of rectifications, erasures and restrictions of processing made in response to requests by the persons concerned.

4. Member States shall ensure that their supervisory authorities have sufficient resources and expertise to fulfil the tasks entrusted to them under this Regulation.

5. Member States shall supply any information requested by a supervisory authority referred to in Article 51(1) of Regulation (EU) 2016/679 and shall, in particular, provide it with information on the activities carried out in accordance with their responsibilities under this Regulation. Member States shall grant the supervisory authorities referred to in Article 51(1) of Regulation (EU) 2016/679 access to their logs referred to in Articles 10, 16, 24 and 36 of this Regulation, to the justifications referred to in Article 22(2) of this Regulation and allow them to access all their premises used for interoperability purposes at all times.

Article 52

Audits by the European Data Protection Supervisor

The European Data Protection Supervisor shall ensure that an audit of personal data processing operations by eu-LISA, the ETIAS Central Unit and Europol for the purposes of this Regulation is carried out in accordance with relevant international auditing standards at least every four years. A report of that audit shall be sent to the European Parliament, to the Council, to eu-LISA, to the Commission, to the Member States and to the Union agency concerned. eu-LISA, the ETIAS Central Unit and Europol shall be given an opportunity to make comments before the reports are adopted.

eu-LISA, the ETIAS Central Unit and Europol shall supply information requested by the European Data Protection Supervisor to it, grant the European Data Protection Supervisor access to all the documents it requests and to their logs referred to in Articles 10, 16, 24 and 36 and allow the European Data Protection Supervisor access to all their premises at any time.

Article 53

Cooperation between supervisory authorities and the European Data Protection Supervisor

1. The supervisory authorities and the European Data Protection Supervisor shall, each acting within the scope of their respective competences, cooperate actively within the framework of their respective responsibilities and ensure coordinated supervision of the use of the interoperability components and the application of other provisions of this Regulation, in particular if the European Data Protection Supervisor or a supervisory authority finds major discrepancies between practices of Member States or finds potentially unlawful transfers using the communication channels of the interoperability components.

2. In the cases referred to in paragraph 1 of this Article, coordinated supervision shall be ensured in accordance with Article 62 of Regulation (EU) 2018/1725.

3. The European Data Protection Board shall send a joint report of its activities under this Article to the European Parliament, to the Council, to the Commission, to Europol, to the European Border and Coast Guard Agency and to eu-LISA by 12 June 2021 and every two years thereafter. That report shall include a chapter on each Member State prepared by the supervisory authority of the Member State concerned.

CHAPTER VIII

Responsibilities

Article 54

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 performance referred to in Article 55(1).

3. eu-LISA shall be responsible for the development of the interoperability components and for any adaptations required for establishing interoperability between the central systems of the EES, VIS, ETIAS, SIS, Eurodac, ECRIS-TCN, and the ESP, the shared BMS, the CIR, the MID and the CRRS.

Without prejudice to Article 66, eu-LISA shall not have access to any of the personal data processed through the ESP, the shared BMS, the CIR or the MID.

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 EES, VIS, ETIAS or SIS 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 (7), 37(4), 38(3), 39(5), 43(5) and 78(10).

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

4. During the design and development phase, a Programme Management Board composed of a maximum of 10 members shall be established. It shall be composed of seven members appointed by eu-LISA's Management Board from among its members or its alternates, the chair of the Interoperability Advisory Group referred to in Article 75, a member representing eu-LISA appointed by its Executive Director, and one member appointed by the Commission. The members appointed by eu-LISA's Management Board shall be elected only from those Member States that are fully bound under Union law by the legal instruments governing the development, establishment, operation and use of all the EU information systems and which will participate in the interoperability components.

5. The Programme Management Board shall meet regularly and at least three times per quarter. It shall ensure the adequate management of the design and development phase of the interoperability components.

Every month, the Programme Management Board shall submit written reports on progress of the project to eu-LISA's Management Board. The Programme Management Board shall have no decision-making power, nor any mandate to represent the members of eu-LISA's Management Board.

6. eu-LISA's Management Board shall establish the rules of procedure of the Programme Management Board, which shall include in particular rules on:

(a) chairmanship;

(b) meeting venues;

(c) preparation of meetings;

(d) admission of experts to the meetings;

(e) communication plans ensuring that non-participating Members of the Management Board are kept fully informed.

The chairmanship shall be held by a Member State that is fully bound under Union law by the legal instruments governing the development, establishment, operation and use of all the EU information systems and which will participate in the interoperability components.

All travel and subsistence expenses incurred by the members of the Programme Management Board shall be paid by eu-LISA, and Article 10 of the eu-LISA Rules of Procedure shall apply *mutatis mutandis*. eu-LISA shall provide the Programme Management Board with a secretariat.

The Interoperability Advisory Group referred to in Article 75 shall meet regularly until the start of operations of the interoperability components. It shall report after each meeting to the Programme Management Board. It shall provide the technical expertise to support the tasks of the Programme Management Board and shall follow up on the state of preparation of the Member States.

Article 55

Responsibilities of eu-LISA following the entry into operations

1. Following the entry into operations of each interoperability component, eu-LISA shall be responsible for the technical management of the central infrastructure of the interoperability components, including their maintenance and technological developments. In cooperation with the Member States, it shall ensure that the best available technology is used, subject to a cost-benefit analysis. eu-LISA shall also be responsible for the technical management of the communication infrastructure referred to in Articles 6, 12, 17, 25 and 39.

Technical management of the interoperability components shall consist of all the tasks and technical solutions necessary to keep the interoperability components functioning and providing uninterrupted services to the Member States and to the Union agencies 24 hours a day, 7 days a week in accordance with this Regulation. It shall include the maintenance work and technical developments necessary to ensure that the components function at a satisfactory level of technical quality, in particular as regards the response time for interrogation of the central infrastructures in accordance with the technical specifications.

All interoperability components shall be developed and managed in such a way as to ensure fast, seamless, efficient and controlled access, full, uninterrupted availability of the components and of the data stored in the MID, the shared BMS and the CIR, and a response time in line with the operational needs of the Member States' authorities and Union agencies.

2. Without prejudice to Article 17 of the Staff Regulations of Officials of the European Union, eu-LISA shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality to its staff required to work with data stored in the interoperability components. This obligation shall also apply after such staff leave office or employment or after the termination of their activities.

Without prejudice to Article 66, eu-LISA shall not have access to any of the personal data processed through the ESP, the shared BMS, the CIR and the MID.

3. eu-LISA shall develop and maintain a mechanism and procedures for carrying out quality checks on the data stored in the shared BMS and the CIR in accordance with Article 37.

4. eu-LISA shall also perform tasks related to providing training on the technical use of the interoperability components.

Article 56

Responsibilities of Member States

1. Each Member State shall be responsible for:

(a) the connection to the communication infrastructure of the ESP and the CIR;

(b) the integration of the existing national systems and infrastructures with the ESP, the CIR and the MID;

(c) the organisation, management, operation and maintenance of its existing national infrastructure and of its connection to the interoperability components;

(d) the management of, and arrangements for, access by the duly authorised staff of the competent national authorities to the ESP, the CIR and the MID in accordance with this Regulation and the creation and regular update of a list of those staff and their profiles;

(e) the adoption of the legislative measures referred to in Article 20(5) and (6) in order to access the CIR for identification purposes;

(f) the manual verification of different identities referred to in Article 29;

(g) compliance with the data quality requirements established under Union law;

(h) compliance with the rules of each EU information system regarding the security and integrity of personal data;

(i) remedying any deficiencies identified in the Commission's evaluation report concerning data quality referred to in Article 37(5).

2. Each Member State shall connect their designated authorities to the CIR.

Article 57

Responsibilities of the ETIAS Central Unit

The ETIAS Central Unit shall be responsible for:

(a) the manual verification of different identities in accordance with Article 29;

(b) carrying out multiple-identity detection between the data stored in the EES, VIS, Eurodac and SIS, as referred to in Article 69.

CHAPTER IX

Amendments to other Union instruments

Article 58

Amendments to Regulation (EC) No 767/2008

Regulation (EC) No 767/2008 is amended as follows:

(1) in Article 1, the following paragraph is added:

'By storing identity data, travel document data and biometric data in the common identity repository (CIR) established by Article 17(1) of Regulation (EU) 2019/817 of the European Parliament and of the Council (*), the VIS contributes to facilitating and assisting in the correct identification of persons registered in the VIS under the conditions and for the purposes of Article 20 of that Regulation.

(*) Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27).';

(2) in Article 4, the following points are added:

'(12) 'VIS data' means all data stored in the VIS Central System and in the CIR in accordance with Articles 9 to 14;

(13) 'identity data' means the data referred to in Article 9(4)(a) and (aa);

(14) 'fingerprint data' means the data relating to the five fingerprints of the index, middle finger, ring finger, little finger and the thumb from the right hand and, where present, from the left hand;';

(3) in Article 5, the following paragraph is inserted:

'1a. The CIR shall contain the data referred to in Article 9(4)(a) to (c), (5) and (6). The remaining VIS data shall be stored in the VIS Central System.';

(4) in Article 6 paragraph 2 is replaced by the following:

'2. Access to the VIS for the purposes of consulting the data shall be reserved exclusively for the duly authorised staff of the national authorities of each Member State which are competent for the purposes laid down in Articles 15 to 22, and for the duly authorised staff of the national authorities of each Member State and of the Union agencies which are competent for the purposes laid down in Articles 20 and 21 of Regulation (EU) 2019/817. Such access shall be limited according to the extent that the data are required for the performance of their tasks for those purposes, and proportionate to the objectives pursued.';

(5) in point (4) of Article 9, points (a) to (c) are replaced by the following:

'(a) surname (family name); first name or names (given names); date of birth; sex;

(aa) surname at birth (former surname(s)); place and country of birth; current nationality and nationality at birth;

(b) the type and number of the travel document or documents and the three-letter code of the issuing country of the travel document or documents;

(c) the date of expiry of the validity of the travel document or documents;

(ca) the authority which issued the travel document and its date of issue;'.

Article 59

Amendments to Regulation (EU) 2016/399

In Article 8 the following paragraph is inserted:

'4a. Where on entry or exit, consultation of the relevant databases including the multiple-identity detector through the European search portal established by Article 25(1) and Article 6(1) of Regulation (EU) 2019/817 of the European Parliament and of the Council (*) respectively results in a yellow link or detects a red link, the border guard shall consult the common identity repository established by Article 17(1) of that Regulation or SIS or both to assess the differences in the linked identity data or travel document data. The border guard shall carry out any additional verification necessary to take a decision on the status and colour of the link.

In accordance with Article 69(1) of Regulation (EU) 2019/817, this paragraph shall apply as from the start of operations of the multiple-identity detector under Article 72(4) of that Regulation.

(*) Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27).'.

Article 60

Amendments to Regulation (EU) 2017/2226

Regulation (EU) 2017/2226 is amended as follows:

(1) in Article 1, the following paragraph is added:

'3. By storing identity data, travel document data and biometric data in the common identity repository (CIR) established by Article 17(1) of Regulation (EU) 2019/817 of the European Parliament and of the Council (*), the EES contributes to facilitating and assisting in the correct identification of persons registered in the EES under the conditions and for the purposes of Article 20 of that Regulation.

(*) Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27).';

(2) in Article 3, paragraph 1 is amended as follows:

(a) point (22) is replaced by the following:

'(22) 'EES data' means all data stored in the EES Central System and in the CIR in accordance with Articles 15 to 20;';

(b) the following point is inserted:

'(22a) 'identity data' means the data referred to in point (a) of Article 16(1) as well as the relevant data referred to in Articles 17(1) and 18(1);';

(c) the following points are added:

'(32) 'ESP' means the European search portal established by Article 6(1) of Regulation (EU) 2019/817;

(33) 'CIR' means the common identity repository established by Article 17(1) of Regulation (EU) 2019/817.';

(3) in Article 6(1), the following point is added:

'(j) ensure the correct identification of persons.';

(4) Article 7 is amended as follows:

(a) paragraph 1 is amended as follows:

(i) the following point is inserted:

'(aa) the CIR central infrastructure as referred to in point (a) of Article 17(2) of Regulation (EU) 2019/817;';

(ii) point (f) is replaced by the following:

'(f) a secure communication infrastructure between the EES Central System and the central infrastructures of the ESP and the CIR.';

(b) the following paragraph is inserted:

'1a. The CIR shall contain the data referred to in points (a) to (d) of Article 16(1), points (a), (b) and (c) of Article 17(1) and Article 18(1) and (2). The remaining EES data shall be stored in the EES Central System.';

(5) in Article 9, the following paragraph is added:

'4. Access to the EES data stored in the CIR shall be reserved exclusively for the duly authorised staff of the national authorities of each Member State and for the duly authorised staff of the Union agencies that are competent for the purposes laid down in Article 20 and Article 21 of Regulation (EU) 2019/817. Such access shall be limited according to the extent that the data are required for the performance of their tasks for those purposes, and proportionate to the objectives pursued.';

(6) Article 21 is amended as follows:

(a) paragraph 1 is replaced by the following:

'1. Where it is technically impossible to enter data in the EES Central System or the CIR or in the event of a failure of the EES Central System or the CIR, the data referred to in Articles 16 to 20 shall be temporarily stored in the NUI. Where that is not possible, the data shall be temporarily stored locally in an electronic format. In both cases, the data shall be entered in the EES Central System or the CIR as soon as the technical impossibility or failure has been remedied. The Member States shall take the appropriate measures and deploy the required infrastructure, equipment and resources to ensure that such temporary local storage may be carried out at any time and for any of their border crossing points.';

(b) in paragraph 2, the first subparagraph is replaced by the following:

'2. Without prejudice to the obligation to carry out border checks under Regulation (EU) 2016/399, the border authority, in the exceptional situation where it is technically impossible to enter data in either the EES Central System and the CIR or in the NUI and it is technically impossible to temporarily store the data locally in an electronic format, shall manually store the data referred to in Articles 16 to 20 of this Regulation, with the exception of biometric data, and shall affix an entry or exit stamp in the travel document of the third-country national. That data shall be entered in the EES Central System and the CIR as soon as technically possible.';

(7) Article 23 is amended as follows:

(a) the following paragraph is inserted:

'2a. For the purpose of the verifications in accordance with paragraph 1 of this Article, the border authority shall launch a query by using the ESP to compare the data on the third-country national with the relevant data in the EES and the VIS.';

(b) in paragraph 4, the first subparagraph is replaced by the following:

'4. Where the search with the alphanumeric data set out in paragraph 2 of this Article indicates that data on the third-country national are not recorded in the EES, where a verification of the third-country national pursuant to paragraph 2 of this Article fails or where there are doubts as to the identity of the third-country national, the border authorities shall have access to data for identification in accordance with Article 27 in order to create or update an individual file in accordance with Article 14.';

(8) in Article 32 the following paragraph is inserted:

'1a. In cases where the designated authorities have launched a query of the CIR in accordance with Article 22 of Regulation (EU) 2019/817, they may access the EES for consultation where the conditions laid down in this Article are met and where the reply received as referred to in Article 22(2) of Regulation (EU) 2019/817 reveals that data are stored in the EES.';

(9) in Article 33 the following paragraph is inserted:

'1a. In cases where Europol has launched a query of the CIR in accordance with Article 22 of Regulation (EU) 2019/817, it may access the EES for consultation where the conditions laid down in this Article are met and where the reply received as referred to in Article 22(2) of Regulation (EU) 2019/817 reveals that data are stored in the EES.';

(10) Article 34 is amended as follows:

(a) in paragraphs 1 and 2, the words 'in the EES Central System' are replaced by the words 'in the CIR and in the EES Central System';

(b) in paragraph 5, the words 'from the EES Central System' are replaced by the words 'from the EES Central System and from the CIR';

(11) in Article 35, paragraph 7 is replaced by the following:

'7. The EES Central System and the CIR shall immediately inform all Member States of the erasure of EES or CIR data and where applicable remove them from the list of identified persons referred to in Article 12(3).';

(12) in Article 36, the words 'of the EES Central System' shall be replaced by the words 'of the EES Central System and the CIR';

(13) Article 37 is amended as follows:

(a) the first subparagraph of paragraph 1 is replaced by the following:

'1. eu-LISA shall be responsible for the development of the EES Central System and the CIR, the NUIs, the Communication Infrastructure and the Secure Communication Channel between the EES Central System and the VIS Central System. eu-LISA shall also be responsible for the development of the web service referred to in Article 13 in accordance with the detailed rules referred to in Article 13(7) and the specifications and conditions adopted pursuant to point (h) of the first paragraph of Article 36 and for the development of the data repository referred to in Article 63(2).';

(b) the first subparagraph of paragraph 3 is replaced by the following:

'3. eu-LISA shall be responsible for the operational management of the EES Central System and the CIR, the NUIs and the Secure Communication Channel between the EES Central System and the VIS Central System. It shall ensure, in cooperation with the Member States, that at all times the best available technology, subject to a cost-benefit analysis, is used for the EES Central System and the CIR, the NUIs, the Communication Infrastructure, the Secure Communication Channel between the EES Central System and the VIS Central System, the web service referred to in Article 13 and the data repository referred to in Article 63(2). eu-LISA shall also be responsible for the operational management of the Communication Infrastructure between the EES Central System and the NUIs, for the web service referred to in Article 13 and the data repository referred to in Article 63(2).';

(14) in Article 46(1) the following point is added:

'(f) a reference to the use of the ESP to query the EES as referred to in Article 7(2) of Regulation (EU) 2019/817.';

(15) Article 63 is amended as follows:

(a) paragraph 2 is replaced by the following:

'2. For the purpose of paragraph 1 of this Article, eu-LISA shall store the data referred to in that paragraph in the central repository for reporting and statistics referred to in Article 39 of the Regulation (EU) 2019/817.';

(b) in paragraph 4 the following subparagraph is added:

'The daily statistics shall be stored in the central repository for reporting and statistics.'.

Article 61

Amendments to Regulation (EU) 2018/1240

Regulation (EU) 2018/1240 is amended as follows:

(1) in Article 1, the following paragraph is added:

'3. By storing identity data and travel document data in the common identity repository (CIR) established by Article 17(1) of Regulation (EU) 2019/817 of the European Parliament and of the Council (*), ETIAS contributes to facilitating and assisting in the correct identification of persons registered in ETIAS under the conditions and for the purposes of Article 20 of that Regulation.

(*) Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27).';

(2) in Article 3(1), the following points are added:

'(23) 'CIR' means the common identity repository established by Article 17(1) of Regulation (EU) 2019/817;

(24) 'ESP' means the European search portal established by Article 6(1) of Regulation (EU) 2019/817;

(25) 'ETIAS Central System' means the Central System referred to in point (a) of Article 6(2) together with the CIR to the extent that the CIR contains the data referred to in Article 6(2a);

(26) 'identity data' means the data referred to in points (a), (b) and (c) of Article 17(2);

(27) 'travel document data' means the data referred to in points (d) and (e) of Article 17(2) and the three letter code of the country issuing the travel document as referred to in point (c) of Article 19(3).';

(3) in Article 4, the following point is added:

'(g) contribute to the correct identification of persons.';

(4) Article 6 is amended as follows:

(a) paragraph 2 is amended as follows:

(i) point (a) is replaced by the following:

'(a) a Central System, including the ETIAS watchlist referred to in Article 34;';

(ii) the following point is inserted:

'(aa) the CIR;';

(iii) point (d) is replaced by the following:

'(d) a secure communication infrastructure between the Central System and the central infrastructures of the ESP and the CIR;';

(b) the following paragraph is inserted:

'2a. The CIR shall contain the identity data and travel document data. The remaining data shall be stored in the Central System.';

(5) Article 13 is amended as follows:

(a) the following paragraph is inserted:

'4a. Access to the ETIAS identity data and travel document data stored in the CIR shall also be reserved exclusively for the duly authorised staff of the national authorities of each Member State and for the duly authorised staff of the Union agencies that are competent for the purposes laid down in Article 20 and Article 21 of Regulation (EU) 2019/817. Such access shall be limited according to the extent that the data are required for the performance of their tasks for those purposes, and proportionate to the objectives pursued.';

(b) paragraph 5 is replaced by the following:

'5. Each Member State shall designate the competent national authorities referred to in paragraphs 1, 2, 4 and 4a of this Article and shall communicate a list of these authorities to eu-LISA without delay, in accordance with Article 87(2). That list shall specify for which purpose the duly authorised staff of each authority shall have access to the data in ETIAS Information System in accordance with paragraphs 1, 2, 4 and 4a of this Article.';

(6) in Article 17, paragraph 2 is amended as follows:

(a) point (a) is replaced by the following:

'(a) surname (family name), first name(s) (given name(s)), surname at birth; date of birth, place of birth, sex, current nationality;';

(b) the following point is inserted:

'(aa) country of birth, first name(s) of the parents of the applicant;';

(7) in Article 19(4) the words 'point (a) of Article 17(2)' are replaced by the words 'points (a) and (aa) of Article 17(2)';

(8) Article 20 is amended as follows:

(a) in paragraph 2, the first subparagraph is replaced by the following:

'2. The ETIAS Central System shall launch a query by using the ESP to compare the relevant data referred to in points (a), (aa), (b), (c), (d), (f), (g), (j), (k) and (m) of Article 17(2) and in Article 17(8) to the data present in a record, file or alert registered in an application file stored in the ETIAS Central System, SIS, the EES, VIS, Eurodac, Europol data and in the Interpol SLTD and TDAWN databases.';

(b) in paragraph 4, the words 'points (a), (b), (c), (d), (f), (g), (j), (k) and (m) of Article 17(2)' are replaced by the words 'points (a), (aa), (b), (c), (d), (f), (g), (j), (k) and (m) of Article 17(2)';

(c) in paragraph 5, the words 'points (a), (c), (f), (h) and (i) of Article 17(2)' are replaced by the words 'points (a), (aa), (c), (f), (h) and (i) of Article 17(2)';

(9) in Article 23, paragraph 1 is replaced by the following:

'1. The ETIAS Central System shall launch a query by using the ESP to compare the relevant data referred to in points (a), (aa), (b) and (d) of Article 17(2) to the data present in SIS in order to determine whether the applicant is the subject of one of the following alerts:

(a) an alert on missing persons;

(b) an alert on persons sought to assist with a judicial procedure;

(c) an alert on persons for discreet checks or specific checks.';

(10) in Article 52, the following paragraph is inserted:

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

(11) in Article 53, the following paragraph is inserted:

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

(12) in the fifth subparagraph of Article 65(3), the words 'points (a), (b), (d), (e) and (f) of Article 17(2)' are replaced by the words 'points (a), (aa), (b), (d), (e) and (f) of Article 17(2)';

(13) in Article 69(1), the following point is inserted:

'(ca) where relevant, a reference to the use of the ESP to query the ETIAS Central System as referred to in Article 7(2) of Regulation (EU) 2019/817';

(14) in Article 73(2), the words 'the central repository of data' are replaced by the words 'the central repository for reporting and statistics referred to in Article 39 of Regulation (EU) 2019/817, insofar as it contains data obtained from the ETIAS Central System under Article 84 of this Regulation';

(15) in Article 74(1), the first subparagraph is replaced by the following:

'1. Following the entry into operations of ETIAS, eu-LISA shall be responsible for the technical management of the ETIAS Central System and the NUIs. It shall also be responsible for any technical testing required for the establishment and update of the ETIAS screening rules. It shall ensure, in cooperation with the Member States that, at all times, the best available technology is used, subject to a cost-benefit analysis. eu-LISA shall also be responsible for the technical management of the communication infrastructure between the ETIAS Central System and the NUIs as well as for the public website, the app for mobile devices, the email service, the secure account service, the verification tool for applicants, the consent tool for applicants, the assessment tool for the ETIAS watchlist, the carrier gateway, the web service and the software to process the applications.';

(16) in Article 84(2), the first subparagraph is replaced by the following:

'2. For the purpose of paragraph 1 of this Article, eu-LISA shall store the data referred to in that paragraph in the central repository for reporting and statistics referred to in Article 39 of Regulation (EU) 2019/817. In accordance with Article 39(1) of that Regulation, cross-system statistical data and analytical reporting shall allow the authorities listed in paragraph 1 of this Article to obtain customisable reports and statistics, to support the implementation of the ETIAS screening rules referred to in Article 33, to improve the assessment of the security, illegal immigration and high epidemic risks, to enhance the efficiency of border checks and to help the ETIAS Central Unit and the ETIAS National Units process travel authorisation applications.';

(17) in Article 84(4), the following subparagraph is added:

'The daily statistics shall be stored in the central repository for reporting and statistics referred to in Article 39 of Regulation (EU) 2019/817.'.

Article 62

Amendments to Regulation (EU) 2018/1726

Regulation (EU) 2018/1726 is amended as follows:

(1) Article 12 is replaced by the following:

'*Article 12*

Data quality

1. Without prejudice to Member States' responsibilities with regard to the data entered into the systems under the Agency's operational responsibility, the Agency, closely involving its Advisory Groups, shall establish for all systems under the Agency's operational responsibility automated data quality control mechanisms and procedures, common data quality indicators and the minimum quality standards to store data, in accordance with the relevant provisions of the legal instruments governing those information systems and of Article 37 of Regulations (EU) 2019/817 (*) and (EU) 2019/818 (**) of the European Parliament and of the Council.

2. The Agency shall establish a central repository containing only anonymised data for reporting and statistics in accordance with Article 39 of Regulations (EU) 2019/817 and (EU) 2019/818, subject to specific provisions in the legal instruments governing the development, establishment, operation and use of large-scale IT systems managed by the Agency.

(*) Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27).

(**) Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (OJ L 135, 22.5.2019, p. 85).';

(2) in Article 19, paragraph 1 is amended as follows:

(a) the following point is inserted:

'(eea) adopt reports on the state of play of the development of the interoperability components pursuant to Article 78(2) of Regulation (EU) 2019/817 and Article 74(2) of Regulation (EU) 2019/818;';

(b) point (ff) is replaced by the following:

'(ff) adopt reports on the technical functioning of SIS pursuant to Article 60(7) of Regulation (EU) 2018/1861 of the European Parliament and of the Council (*) and Article 74(8) of Regulation (EU) 2018/1862 of the European Parliament and of the Council (**), of the VIS pursuant to Article 50(3) of Regulation (EC) No 767/2008 and Article 17(3) of Decision 2008/633/JHA, of EES pursuant to Article 72(4) of Regulation (EU) 2017/2226, of ETIAS pursuant to Article 92(4) of Regulation (EU) 2018/1240, of ECRIS-TCN and of the ECRIS reference implementation pursuant to Article 36(8) of Regulation (EU) 2019/816 of the European Parliament and of the Council (***) and of the interoperability components pursuant to Article 78(3) of Regulation (EU) 2019/817 and Article 74(3) of Regulation (EU) 2019/818;

(*) Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 (OJ L 312, 7.12.2018, p. 14).

(**) Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56).

(***) Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 (OJ L 135, 22.5.2019, p. 1).';

(c) point (hh) is replaced by the following:

'(hh) adopt formal comments on the European Data Protection Supervisor's reports on its audits pursuant to Article 56(2) of Regulation (EU) 2018/1861, Article 42(2) of Regulation (EC) No 767/2008, Article 31(2) of Regulation (EU) No 603/2013, Article 56(2) of Regulation (EU) 2017/2226, Article 67 of Regulation (EU) 2018/1240, Article 29(2) of Regulation (EU) 2019/816 and Article 52 of Regulations (EU) 2019/817 and (EU) 2019/818 and ensure appropriate follow up of those audits;';

(d) point (mm) is replaced by the following:

'(mm) ensure annual publication of the list of competent authorities authorised to search directly the data contained in SIS pursuant to Article 41(8) of Regulation (EU) 2018/1861 and Article 56(7) of Regulation (EU) 2018/1862, together with the list of Offices of the national systems of SIS (N.SIS) and SIRENE Bureaux pursuant to Article 7(3) of Regulation (EU) 2018/1861 and Article 7(3) of Regulation (EU) 2018/1862 respectively as well as the list of competent authorities pursuant to Article 65(2) of Regulation (EU) 2017/2226, the list of competent authorities pursuant to Article 87(2) of Regulation (EU) 2018/1240, the list of central authorities pursuant to Article 34(2) of Regulation (EU) 2019/816 and the list of authorities pursuant to Article 71(1) of Regulation (EU) 2019/817 and Article 67(1) of Regulation (EU) 2019/818;';

(3) in Article 22, paragraph 4 is replaced by the following:

'4. Europol and Eurojust may attend the meetings of the Management Board as observers when a question concerning SIS II, in relation to the application of Decision 2007/533/JHA is on the agenda.

The European Border and Coast Guard Agency may attend the meetings of the Management Board as an observer when a question concerning SIS in relation to the application of Regulation (EU) 2016/1624 is on the agenda.

Europol may attend the meetings of the Management Board as an observer when a question concerning VIS, in relation to the application of Decision 2008/633/JHA or a question concerning Eurodac, in relation to the application of Regulation (EU) No 603/2013 is on the agenda.

Europol may attend the meetings of the Management Board as an observer when a question concerning EES in relation to the application of Regulation (EU) 2017/2226 is on the agenda or when a question concerning ETIAS in relation to Regulation (EU) 2018/1240 is on the agenda.

The European Border and Coast Guard Agency may attend the meetings of the Management Board as an observer when a question concerning ETIAS in relation with the application of Regulation (EU) 2018/1240 is on the agenda.

Eurojust, Europol and the European Public Prosecutor's Office may attend the meetings of the Management Board as observers when a question concerning Regulation (EU) 2019/816 is on the agenda.

Europol, Eurojust and the European Border and Coast Guard Agency may attend the meetings of the Management Board as observers when a question concerning Regulations (EU) 2019/817 and (EU) 2019/818 is on the agenda.

The Management Board may invite any other person whose opinion may be of interest to attend its meetings as an observer.';

(4) in Article 24(3), point (p) is replaced by the following:

'(p) without prejudice to Article 17 of the Staff Regulations of Officials, establishing confidentiality requirements in order to comply with Article 17 of Regulation (EC) No 1987/2006, Article 17 of Decision 2007/533/JHA, Article 26(9) of Regulation (EC) No 767/2008, Article 4(4) of Regulation (EU) No 603/2013, Article 37(4) of Regulation (EU) 2017/2226, Article 74(2) of Regulation (EU) 2018/1240, Article 11(16) of Regulation (EU) 2019/816 and Article 55(2) of Regulations (EU) 2019/817 and (EU) 2019/818;';

(5) Article 27 is amended as follows:

(a) in paragraph 1, the following point is inserted:

'(da) Interoperability Advisory Group;';

(b) paragraph 3 is replaced by the following:

'3. Europol, Eurojust and the European Border and Coast Guard Agency may each appoint a representative to the SIS II Advisory Group.

Europol may also appoint a representative to the VIS and Eurodac and EES-ETIAS Advisory Groups.

The European Border and Coast Guard Agency may also appoint a representative to the EES-ETIAS Advisory Group.

Eurojust, Europol, and the European Public Prosecutors Office may each appoint a representative to the ECRIS-TCN Advisory Group.

Europol, Eurojust and the European Border and Coast Guard Agency may each appoint a representative to the Interoperability Advisory Group.'.

Article 63

Amendments to Regulation (EU) 2018/1861

Regulation (EU) 2018/1861 is amended as follows:

(1) in Article 3, the following points are added:

'(22) 'ESP' means the European search portal established by Article 6(1) of Regulation (EU) 2019/817 of the European Parliament and of the Council (*);

(23) 'shared BMS' means the shared biometric matching service established by Article 12(1) of Regulation (EU) 2019/817;

(24) 'CIR' means the common identity repository established by Article 17(1) of Regulation (EU) 2019/817;

(25) 'MID' means the multiple-identity detector established by Article 25(1) of Regulation (EU) 2019/817.

(*) Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27).';

(2) Article 4 is amended as follows:

(a) in paragraph 1, points (b) and (c) are replaced by the following:

'(b) a national system (N.SIS) in each of the Member States, consisting of the national data systems which communicate with Central SIS, including at least one national or shared backup N.SIS;

(c) a communication infrastructure between CS-SIS, backup CS-SIS and NI-SIS ('the Communication Infrastructure') that provides an encrypted virtual network dedicated to SIS data and the exchange of data between SIRENE Bureaux, as referred to in Article 7(2); and

(d) a secure communication infrastructure between CS-SIS and the central infrastructures of the ESP, the shared BMS and the MID.';

(b) the following paragraphs are added:

'8. Without prejudice to paragraphs 1 to 5, SIS data may also be searched via the ESP.

9. Without prejudice to paragraphs 1 to 5, SIS data may also be transmitted via the secure communication infrastructure referred to in point (d) of paragraph 1. These transmissions shall be limited to the extent that the data are required for the purposes of Regulation (EU) 2019/817.';

(3) in Article 7, the following paragraph is inserted:

'2a. The SIRENE Bureaux shall also ensure the manual verification of different identities in accordance with Article 29 Regulation (EU) 2019/817. To the extent necessary to carry out this task, the SIRENE Bureaux shall have access to the data stored in the CIR and the MID for the purposes laid down in Articles 21 and 26 of Regulation (EU) 2019/817.';

(4) in Article 12, paragraph 1 is replaced by the following:

'1. Member States shall ensure that every access to and all exchanges of personal data within CS-SIS are logged in their N.SIS for the purposes of checking whether the search was lawful, monitoring the lawfulness of data processing, self-monitoring, ensuring the proper functioning of N.SIS, as well as for data integrity and security. This requirement does not apply to the automatic processes referred to in points (a), (b) and (c) of Article 4(6).

Member States shall ensure that every access to personal data via the ESP is also logged for the purposes of checking whether the search was lawful, monitoring the lawfulness of data processing, self-monitoring, and data integrity and security.';

(5) in Article 34(1), the following point is added:

'(g) verifying different identities and combating identity fraud in accordance with Chapter V of Regulation (EU) 2019/817.';

(6) in Article 60, paragraph 6 is replaced by the following:

'6. For the purpose of Article 15(4) and of paragraphs 3, 4 and 5 of this Article, eu-LISA shall store data referred to in Article 15(4) and in paragraph 3 of this Article which shall not allow for the identification of individuals in the central repository for reporting and statistics referred to in Article 39 of Regulation (EU) 2019/817.

eu-LISA shall allow the Commission and the bodies referred to in paragraph 5 of this Article to obtain bespoke reports and statistics. Upon request, eu-LISA shall grant access to the central repository for reporting and statistics in accordance with Article 39 of Regulation (EU) 2019/817 to Member States, the Commission, Europol, and the European Border and Coast Guard Agency.'.

Article 64

Amendments to Decision 2004/512/EC

In Article 1 of Decision 2004/512/EC, paragraph 2 is replaced by the following:

'2. The Visa Information System shall be based on a centralised architecture and consist of:

(a) the common identity repository central infrastructure as referred to in Article 17(2)(a) of Regulation (EU) 2019/817 of the European Parliament and of the Council (*);

(b) a central information system, hereinafter referred to as 'the Central Visa Information System' (CS-VIS);

(c) an interface in each Member State, hereinafter referred to as the 'National Interface' (NI-VIS), to provide the connection to the relevant central national authority of the respective Member State;

(d) a communication infrastructure between the Central Visa Information System and the National Interfaces;

(e) a Secure Communication Channel between the EES Central System and the CS-VIS;

(f) a secure communication infrastructure between the VIS Central System and the central infrastructure of the European search portal established by Article 6(1) of Regulation (EU) 2019/817 and of the common identity repository established by Article 17(1) of Regulation (EU) 2019/817.

(*) Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27).'.

Article 65

Amendments to Decision 2008/633/JHA

Decision 2008/633/JHA is amended as follows:

(1) in Article 5, the following paragraph is inserted:

'1a. In cases where the designated authorities have launched a query of the common identity repository (CIR) in accordance with Article 22 of Regulation (EU) 2019/817 of the European Parliament and of the Council (*), and where the conditions for access laid down in this Article are met, they may access the VIS for consultation where the reply received as referred to in Article 22(2) of that Regulation reveals that data are stored in the VIS.

(*) Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27).';

(2) in Article 7, the following paragraph is inserted:

'1a. In cases where Europol has launched a query of the CIR in accordance with Article 22 of Regulation (EU) 2019/817, and where the conditions for access laid down in this Article are met, Europol may access the VIS for consultation where the reply received as referred to in Article 22(2) of that Regulation reveals that data are stored in the VIS.'.

CHAPTER X

Final provisions

Article 66

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 ESP, solely for the purposes of reporting and statistics:

(a) number of queries per ESP user profile;

(b) number of queries to each of the Interpol databases.

It shall not be possible to identify individuals from the data.

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 CIR, solely for the purposes of reporting and statistics:

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

(b) nationality, gender 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.

It shall not be possible to identify individuals from the 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 MID, solely for the purposes of reporting and statistics:

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

(b) the number of each type of link and the EU information systems containing the linked data;

(c) the period of time for which a yellow and red link remained in the system.

It shall not be possible to identify individuals from the data.

4. The duly authorised staff of the European Border and Coast Guard Agency shall have access to consult the data referred to in paragraphs 1, 2 and 3 of this Article for the purpose of carrying out risk analyses and vulnerability assessments as referred to in Articles 11 and 13 of Regulation (EU) 2016/1624 of the European Parliament and of the Council ([40]).

5. The duly authorised staff of Europol shall have access to consult the data referred to in paragraphs 2 and 3 of this Article for the purpose of carrying out strategic, thematic and operational analyses as referred to in Article 18(2)(b) and (c) of Regulation (EU) 2016/794.

6. For the purpose of paragraphs 1, 2 and 3, eu-LISA shall store the data referred to in those paragraphs in the CRRS. It shall not be possible to identify individuals from the data included in the CRRS, but the data shall allow the authorities listed in paragraphs 1, 2 and 3 to obtain customisable reports and statistics to enhance the efficiency of border checks, to help authorities processing visa applications and to support evidence-based policy-making on migration and security in the Union.

7. Upon request, relevant information shall be made available by the Commission to the European Union Agency for Fundamental Rights in order to evaluate the impact of this Regulation on fundamental rights.

Article 67

Transitional period for the use of the European search portal

1. For a period of two years from the date the ESP commences operations, the obligations referred to in Article 7(2) and (4) shall not apply and the utilisation of the ESP shall be optional.

2. The Commission is empowered to adopt a delegated act in accordance with Article 73 in order to amend this Regulation by extending the period referred to in paragraph 1 of this Article once, by no longer than one year, when an assessment of the implementation of the ESP has shown that such an extension is necessary, especially in view of the impact that bringing the ESP into operation would have on the organisation and length of border checks.

Article 68

Transitional period applicable to the provisions on access to the common identity repository for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences

Article 22, points 8 and 9 of Article 60, points 10 and 11 of Article 61 and Article 65 shall apply from the date of the start of operations of the CIR referred to in Article 72(3).

([40]) 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).

Article 69

Transitional period for multiple-identity detection

1. For a period of one year following notification by eu-LISA of the completion of the test of the MID referred to in Article 72(4)(b) and before the start of operations of the MID, the ETIAS Central Unit shall be responsible for carrying out multiple-identity detection using the data stored in the EES, VIS, Eurodac and SIS. The multiple-identity detections shall be carried out using only biometric data.

2. Where the query reports one or several matches and the identity data in the linked files are the same or similar, a white link shall be created in accordance with Article 33.

Where the query reports one or several matches and the identity data in the linked files cannot be considered to be similar, a yellow link shall be created in accordance with Article 30 and the procedure referred to in Article 29 shall apply.

Where several matches are reported, a link shall be created between each piece of data triggering the match.

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

4. Where a link is created to an alert in SIS other than an alert created under Article 3 of Regulation (EU) 2018/1860, Articles 24 and 25 of Regulation (EU) 2018/1861, or Article 38 of Regulation (EU) 2018/1862, 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, in the cases referred to in paragraph 4 of this Article 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. The ETIAS Central Unit shall notify the Commission in accordance with Article 71(3) only once all yellow links have been manually verified and their status updated as either green, white or red links.

7. Member States shall assist the ETIAS Central Unit where necessary in carrying out multiple-identity detection under this Article.

8. The Commission is empowered to adopt a delegated act in accordance with Article 73 in order to amend this Regulation by extending the period referred to in paragraph 1 of this Article by six months, renewable twice by six months each time. Such an extension shall only be granted following an assessment of the estimated completion time for multiple-identity detection under this Article, which demonstrates that the multiple-identity detection cannot be completed before expiry of the period remaining either under paragraph 1 of this Article or any ongoing extension, for reasons independent of the ETIAS Central Unit, and that no corrective measures can be applied. The assessment shall be carried out no later than three months before the expiry of such period or ongoing extension.

Article 70

Costs

1. The costs incurred in connection with the establishment and operation of the ESP, the shared BMS, the CIR and the MID shall be borne by the general budget of the Union.

2. Costs incurred in connection with the integration of the existing national infrastructures and their connection to the national uniform interfaces as well as in connection with hosting the national uniform interfaces shall be borne by the general budget of the Union.

The following costs shall be excluded:

(a) Member States' project management office (meetings, missions, offices);

(b) hosting of national IT systems (space, implementation, electricity, cooling);

(c) operation of national IT systems (operators and support contracts);

(d) design, development, implementation, operation and maintenance of national communication networks.

3. Without prejudice to further funding for this purpose from other sources of the general budget of the European Union, an amount of EUR 32 077 000 shall be mobilised from the envelope of EUR 791 000 000 foreseen under Article 5(5)(b) of Regulation (EU) No 515/2014 to cover the costs of implementation of this Regulation, as foreseen under paragraphs 1 and 2 of this Article.

4. From the envelope referred to in paragraph 3, EUR 22 861 000 shall be allocated to eu-LISA, EUR 9 072 000 shall be allocated to Europol and EUR 144 000 shall be allocated to the European Union Agency for Law Enforcement Training (CEPOL) to support these agencies in performing their respective tasks under this Regulation. Such funding shall be implemented under indirect management.

5. The costs incurred by the designated authorities shall be borne by the designating Member States respectively. The costs of connecting each designated authority to the CIR shall be borne by each Member State.

The costs incurred by Europol, including of connection to the CIR, shall be borne by Europol.

Article 71

Notifications

1. The Member States shall notify eu-LISA of the authorities referred to in Articles 7, 20, 21 and 26 that may use or have access to the ESP, the CIR and the MID respectively.

A consolidated list of those authorities shall be published in the *Official Journal of the European Union* within a period of three months from the date on which each interoperability component commenced operations in accordance with Article 72. Where there are amendments to the list, eu-LISA shall publish an updated consolidated list once a year.

2. eu-LISA shall notify the Commission of the successful completion of the tests referred to in Article 72(1)(b), (2)(b), (3)(b), (4)(b), (5)(b) and (6)(b).

3. The ETIAS Central Unit shall notify the Commission of the successful completion of the transitional period laid down in Article 69.

4. The Commission shall make the information notified pursuant to paragraph 1 available to the Member States and to the public, via a constantly updated public website.

Article 72

Start of operations

1. The Commission shall determine the date from which the ESP is to start operations by means of an implementing act once the following conditions have been met:

(a) the measures referred to in Articles 8(2), 9(7) and 43(5) have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the ESP, which it has conducted in cooperation with the Member States authorities and the Union agencies that may use the ESP;

(c) eu-LISA has validated the technical and legal arrangements to collect and transmit the data referred to in Article 8(1) and has notified them to the Commission.

The ESP shall only query the Interpol databases once the technical arrangements allow compliance with Article 9(5). Any impossibility of complying with Article 9(5) shall have the result that the ESP does not query the Interpol databases but shall not delay the start of operations of the ESP.

The Commission shall set the date referred to in the first subparagraph to be within 30 days from adoption of the implementing act.

2. The Commission shall determine the date from which the shared BMS is to start operations by means of an implementing act once the following conditions have been met:

(a) the measures referred to in Articles 13(5) and 43(5) have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the shared BMS, which it has conducted in cooperation with the Member States authorities;

(c) eu-LISA has validated the technical and legal arrangements to collect and transmit the data referred to in Article 13 and has notified them to the Commission;

(d) eu-LISA has declared the successful completion of the test referred to in paragraph 5(b).

The Commission shall set the date referred to in the first subparagraph to be within 30 days from adoption of the implementing act.

3. The Commission shall determine the date from which the CIR is to start operations by means of an implementing act once the following conditions have been met:

(a) the measures referred to in Articles 43(5) and 78(10) have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the CIR, which it has conducted in cooperation with the Member States authorities;

(c) eu-LISA has validated the technical and legal arrangements to collect and transmit the data referred to in Article 18 and has notified them to the Commission;

(d) eu-LISA has declared the successful completion of the test referred to in paragraph 5(b).

The Commission shall set the date referred to in the first subparagraph to be within 30 days from adoption of the implementing act.

4. The Commission shall determine the date from which the MID is to start operations by means of an implementing act once the following conditions have been met:

(a) the measures referred to in Articles 28(5) and (7), 32(5), 33(6), 43(5) and 49(6) have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the MID, which it has conducted in cooperation with the Member States authorities and the ETIAS Central Unit;

(c) eu-LISA has validated the technical and legal arrangements to collect and transmit the data referred to in Article 34 and has notified them to the Commission;

(d) the ETIAS Central Unit has notified the Commission in accordance with Article 71(3);

(e) eu-LISA has declared the successful completion of the tests referred to in paragraphs 1(b), 2(b), 3(b) and 5(b).

The Commission shall set the date referred to in the first subparagraph to be within 30 days from adoption of the implementing act.

5. The Commission shall determine by means of implementing acts the date from which the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum data quality standards are to be used, once the following conditions have been met:

(a) the measures referred to in Articles 37(4) have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum data quality standards, which it has conducted in cooperation with the Member States authorities.

The Commission shall set the date referred to in the first subparagraph to be within 30 days from adoption of the implementing act.

6. The Commission shall determine the date from which the CRRS is to start operations by means of an implementing act once the following conditions have been met:

(a) the measures referred to in Articles 39(5) and 43(5) have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the CRRS, which it has conducted in cooperation with the Member States authorities;

(c) eu-LISA has validated the technical and legal arrangements to collect and transmit the data referred to in Article 39 and has notified them to the Commission.

The Commission shall set the date referred to in the first subparagraph to be within 30 days from adoption of the implementing act.

7. The Commission shall inform the European Parliament and the Council of the results of the tests carried out pursuant to paragraphs 1(b), 2(b), 3(b), 4(b), 5(b) and 6(b).

8. Member States, the ETIAS Central Unit and Europol shall start using each of the interoperability components from the date determined by the Commission in accordance with paragraphs 1, 2, 3 and 4 respectively.

Article 73

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Articles 28(5), 39(5), 49(6), 67(2) and 69(8) shall be conferred on the Commission for a period of five years from 11 June 2019. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

3. The delegation of power referred to in Articles 28(5), 39(5), 49(6), 67(2) and 69(8) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Articles 28(5), 39(5), 49(6), 67(2) and 69(8) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 74

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Where the committee delivers no opinion, the Commission shall not adopt the draft implementing act and the third subparagraph of Article 5(4) of Regulation (EU) No 182/2011 shall apply.

Article 75

Advisory Group

An Interoperability Advisory Group shall be established by eu-LISA. During the design and development phase of the interoperability components, Article 54(4), (5) and (6) shall apply.

Article 76

Training

eu-LISA shall perform tasks related to the provision of training on the technical use of the interoperability components in accordance with Regulation (EU) 2018/1726.

Member States authorities and Union agencies shall provide their staff authorised to process data using the interoperability components, with appropriate training programmes concerning data security, data quality, data protection rules, the procedures applicable to data processing and the obligations to inform under Articles 32(4), 33(4) and 47.

Where appropriate, joint training courses on these topics shall be organised at Union level to enhance cooperation and the exchange of best practices between the staff of Member States authorities and Union agencies who are authorised to process data using the interoperability components. Particular attention shall be paid to the process of multiple-identity detection, including the manual verification of different identities and the accompanying need to maintain appropriate safeguards of fundamental rights.

Article 77

Practical handbook

The Commission shall, in close cooperation with the Member States, eu-LISA and other relevant Union agencies, make available a practical handbook for the implementation and management of the interoperability components. The practical handbook shall provide technical and operational guidelines, recommendations and best practices. The Commission shall adopt the practical handbook in the form of a recommendation.

Article 78

Monitoring and evaluation

1. eu-LISA shall ensure that procedures are in place to monitor the development of the interoperability components and their connection to the national uniform interface 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 12 December 2019 and every six months thereafter during the development phase of the interoperability components, eu-LISA shall submit a report to the European Parliament and to the Council on the state of play of the development of the interoperability components, as well as their connection to the national uniform interface. Once the development is finalised, a report shall be submitted to the European Parliament and to the Council explaining in detail how the objectives, in particular relating to planning and costs, were achieved, as well as justifying any divergences.

3. Four years after the start of operations of each interoperability component in accordance with Article 72 and every four years thereafter, eu-LISA shall submit to the European Parliament, to the Council and to the Commission a report on the technical functioning of the interoperability components, including their security.

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

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

(b) an examination of the results achieved against the objectives of this Regulation and its impact on fundamental rights, including in particular an assessment of the impact of the interoperability components on the right to non-discrimination;

(c) an assessment of the functioning of the web portal, including figures regarding the use of the web portal and the number of requests that were resolved;

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

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

(f) an assessment of the use of the CIR for identification;

(g) an assessment of the use of the CIR for preventing, detecting or investigating terrorist offences or other serious criminal offences;

(h) 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 general budget of the Union;

(i) an assessment of the search of the Interpol databases via the ESP, including information on the number of matches against Interpol databases and information on any problems encountered.

The overall evaluation under the first subparagraph of this paragraph 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.

5. By 12 June 2020 and every year thereafter until the implementing acts of the Commission referred to in Article 72 have been adopted, the Commission shall submit a report to the European Parliament and to the Council on the state of play of preparations for the full implementation of this Regulation. That report shall contain also detailed information about the costs incurred and information as to any risks which may impact the overall costs.

6. Two years after the start of operations of the MID in accordance with Article 72(4), the Commission shall produce an examination of the impact of the MID on the right to non-discrimination. Following this first report, the examination of the impact of the MID on the right to non-discrimination shall be part of the examination referred to in paragraph 4(b) of this Article.

7. The Member States and Europol shall provide eu-LISA and the Commission with the information necessary to draft the reports referred to in paragraphs 3 to 6. This information shall not jeopardise working methods or include information that reveals sources, staff members or investigations of the designated authorities.

8. eu-LISA shall provide the Commission with the information necessary to produce the overall evaluation referred to in paragraph 4.

9. While respecting the provisions of national law on the publication of sensitive information, and without prejudice to limitations necessary to protect security and public order, prevent crime and guarantee that no national investigation will be jeopardised, each Member State and Europol shall prepare annual reports on the effectiveness of access to data stored in the CIR for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences, containing information and statistics on:

(a) the exact purposes of the consultations including the types of terrorist offences or other serious criminal offences;

(b) the reasonable grounds given for a substantiated suspicion that a suspect, perpetrator or victim is covered by Regulation (EU) 2017/2226, Regulation (EC) No 767/2008 or Regulation (EU) 2018/1240;

(c) the number of requests for access to the CIR for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences;

(d) the number and types of cases that have ended in successful identifications;

(e) the need and use made of the exceptions for cases of urgency including those cases where that urgency was not accepted by the *ex post* verification carried out by the central access point.

The annual reports prepared by the Member State and Europol shall be transmitted to the Commission by 30 June of the subsequent year.

10. A technical solution shall be made available to Member States in order to manage user access requests referred to in Article 22 and to facilitate the collection of the information under paragraphs 7 and 9 of this Article for the purpose of generating reports and statistics referred to in those paragraphs. The Commission shall adopt implementing acts to lay down the specifications of the technical solution. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 74(2).

Article 79

Entry into force and applicability

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

The provisions of this Regulation related to the ESP shall apply from the date determined by the Commission in accordance with Article 72(1).

The provisions of this Regulation related to the shared BMS shall apply from the date determined by the Commission in accordance with Article 72(2).

The provisions of this Regulation related to the CIR shall apply from the date determined by the Commission in accordance with Article 72(3).

The provisions of this Regulation related to the MID shall apply from the date determined by the Commission in accordance with Article 72(4).

The provisions of this Regulation related to the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum data quality standards shall apply respectively from the dates determined by the Commission in accordance with Article 72(5).

The provisions of this Regulation related to the CRRS shall apply from the date determined by the Commission in accordance with Article 72(6).

Articles 6, 12, 17, 25, 38, 42, 54, 56, 57, 70, 71, 73, 74, 75, 77 and 78(1) shall apply from 11 June 2019.

This Regulation shall apply in relation to Eurodac from the date the recast of Regulation (EU) No 603/2013 becomes applicable.

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

Done at Brussels, 20 May 2019.

For the European Parliament	*For the Council*
The President	*The President*
A. TAJANI	G. CIAMBA

REGULATION (EU) 2019/818 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 20 May 2019

on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2), Article 74, Article 78(2)(e), Article 79(2)(c), Article 82(1)(d), Article 85(1), Article 87(2)(a) and Article 88(2) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee ([1]),

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure ([2]),

Whereas:

(1) In its Communication of 6 April 2016 entitled Stronger and Smarter Information Systems for Borders and Security, the Commission underlined the need to improve the Union's data management architecture for border management and security. The Communication initiated a process towards achieving interoperability between EU information systems for security, border and migration management, with the aim to address the structural shortcomings related to those systems that impede the work of national authorities and to ensure that border guards, customs authorities, police officers and judicial authorities have the necessary information at their disposal.

(2) In its Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area of 6 June 2016, the Council identified various legal, technical and operational challenges in the interoperability of EU information systems and called for the pursuit of solutions.

(3) In its Resolution of 6 July 2016 on the strategic priorities for the Commission Work Programme 2017 ([3]), the European Parliament called for proposals to improve and develop existing EU information systems, address information gaps and move towards their interoperability, as well as proposals for compulsory information sharing at EU level, accompanied by the necessary data protection safeguards.

(4) In its conclusions of 15 December 2016 the European Council called for work to continue on delivering interoperability of EU information systems and databases.

(5) In its final report of 11 May 2017, the high-level expert group on information systems and interoperability concluded that it was necessary and technically feasible to work towards practical solutions for interoperability and that interoperability could, in principle, both deliver operational gains and be established in compliance with data protection requirements.

(6) In its Communication of 16 May 2017 entitled Seventh progress report towards an effective and genuine Security Union, the Commission set out, in line with its Communication of 6 April 2016 and the findings and recommendations of the high-level expert group on information systems and interoperability, a new approach to the management of data for borders, security and migration whereby all EU information systems for security, border and migration management were to be interoperable in a manner fully respecting fundamental rights.

([1]) OJ C 283, 10.8.2018, p. 48.
([2]) Position of the European Parliament of 16 April 2019 (not yet published in the Official Journal) and decision of the Council of 14 May 2019.
([3]) OJ C 101, 16.3.2018, p. 116.

(7) In its Conclusions of 9 June 2017 on the way forward to improve information exchange and ensure the interoperability of EU information systems, the Council invited the Commission to pursue the solutions for interoperability proposed by the high-level expert group.

(8) In its conclusions of 23 June 2017 the European Council underlined the need to improve interoperability between databases and invited the Commission to prepare draft legislation on the basis of the proposals made by the high-level expert group on information systems and interoperability as soon as possible.

(9) With a view to improving the effectiveness and efficiency of checks at the external borders, to contributing to prevention and combating illegal immigration and to contributing 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 security in the territories of the Member States, to improving the implementation of the common visa policy, to assisting in the examination of applications for international protection, to contributing to the prevention, detection and investigation of terrorist offences and other serious criminal offences, to facilitating the identificaton of unknown persons who are unable to identify themselves or unidentified human remainsin the case of a natural disaster, accident or terrorist attack, in order to maintain public trust in the Union migration and asylum system, Union security measures and Union capabilities to manage the external border, interoperability between EU information systems, namely 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) should be established in order for these EU information systems and their data to supplement each other while respecting the fundamental rights of individuals, in particular the right to protection of personal data. To achieve this, a European search portal (ESP), a shared biometric matching service (shared BMS), a common identity repository (CIR) and a multiple-identity detector (MID) should be established as interoperability components.

(10) Interoperability between the EU information systems should allow those systems to supplement each other in order to facilitate the correct identification of persons, including unknown persons who are unable to identify themselves or unidentified human remains, contribute to combating identity fraud, improve and harmonise the data quality requirements of the respective EU information systems, facilitate the technical and operational implementation by Member States of EU information systems, strengthen the data security and data protection safeguards that govern the respective EU information systems, streamline access for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences to the EES, VIS, ETIAS and Eurodac, and support the purposes of the EES, VIS, ETIAS, Eurodac, SIS and ECRIS-TCN.

(11) The interoperability components should cover the EES, VIS, ETIAS, Eurodac, SIS, and ECRIS-TCN. They should also cover Europol data, but only to the extent of enabling Europol data to be queried simultaneously with those EU information systems.

(12) The interoperability components should process the personal data of persons whose personal data are processed in the underlying EU information systems and by Europol.

(13) The ESP should be established to facilitate technically the fast, seamless, efficient, systematic and controlled access by Member State authorities and Union agencies to the EU information systems, to Europol data and to the International Criminal Police Organization (Interpol) databases, insofar as this is needed to perform their tasks in accordance with their access rights. The ESP should also be established to support the objectives of the EES, VIS, ETIAS, Eurodac, SIS, ECRIS-TCN and Europol data. By enabling all relevant EU information systems, Europol data and the Interpol databases to be queried in parallel, the ESP should act as a single window or 'message broker' to search the various central systems and retrieve the necessary information seamlessly and in full respect of the access control and data protection requirements of the underlying systems.

(14) The design of the ESP should ensure that, when querying the Interpol databases, the data used by an ESP user to launch a query is not shared with the owners of Interpol data. The design of the ESP should also ensure that the Interpol databases are only queried in accordance with applicable Union and national law.

(15) Those ESP users who have the right to access Europol data under Regulation (EU) 2016/794 of the European Parliament and of the Council ([4]) should be able to query Europol data simultaneously with the EU information systems to which they have access. Any further data processing following such a query should take place in accordance with Regulation (EU) 2016/794, including restrictions on access or use imposed by the data provider.

(16) The ESP should be developed and configured in such a way that it only allows such queries to be performed using data related to persons or travel documents held in an EU information system, in Europol data or in the Interpol databases.

(17) To ensure the systematic use of the relevant EU information systems, the ESP should be used to query the CIR, the EES, VIS, ETIAS, Eurodac and ECRIS-TCN. However, a national connection to the different EU information systems should remain in order to provide a technical fall back. The ESP should also be used by Union agencies to query Central SIS in accordance with their access rights and in order to perform their tasks. The ESP should be an additional means to query Central SIS, Europol data and the Interpol databases, complementing the existing dedicated interfaces.

(18) Biometric data, such as fingerprints and facial images, are unique and therefore much more reliable than alphanumeric data for the purposes of identifying a person. The shared BMS should be a technical tool to reinforce and facilitate the work of the relevant EU information systems and the other interoperability components. The main purpose of the shared BMS should be to facilitate the identification of an individual who is registered in several databases, by using a single technological component to match that individual's biometric data across different systems, instead of several components. The shared BMS should contribute to security, as well as financial, maintenance and operational benefits. All automated fingerprint identification systems, including those currently used for Eurodac, VIS and SIS, use biometric templates comprised of data derived from a feature extraction of actual biometric samples. The shared BMS should regroup and store all these biometric templates – logically separated according to the information system from which the data originated – in one single location, thereby facilitating cross-system comparisons using biometric templates and enabling economies of scale in developing and maintaining the EU central systems.

(19) The biometric templates stored in the shared BMS should be comprised of data derived from a feature extraction of actual biometric samples and obtained in such a way that reversing the extraction process is not possible. Biometric templates should be obtained from biometric data but it should not be possible to obtain that same biometric data from the biometric templates. As palm print data and DNA profiles are only stored in SIS and cannot be used to perform cross-checks with data present in other information systems, following the principles of necessity and proportionality, the shared BMS should not store DNA profiles or biometric templates obtained from palm print data.

(20) Biometric data constitute sensitive personal data. This Regulation should lay down the basis and the safeguards for processing such data for the purpose of uniquely identifying the persons concerned.

(21) The EES, VIS, ETIAS, Eurodac and ECRIS-TCN require accurate identification of the persons whose personal data are stored in them. The CIR should therefore facilitate the correct identification of persons registered in those systems.

(22) Personal data stored in those EU information systems may relate to the same persons but under different or incomplete identities. Member States dispose of efficient ways to identify their citizens or registered permanent residents in their territory. The interoperability between EU information systems should contribute to the correct identification of persons present in those systems. The CIR should store the personal data that are necessary to enable the more accurate identification of the individuals whose data are stored in those systems, including their identity data, travel document data and biometric data, regardless of the system in which the data were originally collected. Only the personal data strictly necessary to perform an accurate identity check should be stored in the CIR. The personal data recorded in the CIR should be kept for no longer than is strictly necessary for the purposes of the underlying systems and should be automatically deleted when the data are deleted from the underlying systems in accordance with their logical separation.

([4]) Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).

(23) A new processing operation consisting of the storage of such data in the CIR instead of the storage in each of the separate systems is necessary to increase the accuracy of identification through the automated comparison and matching of the data. The fact that identity data, travel document data and biometric data are stored in the CIR should not hinder in any way the processing of data for the purposes of the EES, VIS, ETIAS, Eurodac or ECRIS-TCN, as the CIR should be a new shared component of those underlying systems.

(24) It is therefore necessary to create an individual file in the CIR for each person registered in the EES, VIS, ETIAS, Eurodac or ECRIS-TCN, to achieve the purpose of correct identification of persons within the Schengen area and to support the MID for the dual purpose of facilitating identity checks for *bona fide* travellers and combating identity fraud. The individual file should store all the identity information linked to a person in a single place and make it accessible to duly authorised end-users.

(25) The CIR should thus facilitate and streamline access by authorities responsible for preventing, detecting or investigating terrorist offences or other serious criminal offences to the EU information systems that are not established exclusively for purposes of prevention, detection or investigation of serious crime.

(26) The CIR should provide for a shared container for identity data, travel document data and biometric data of persons registered in the EES, VIS, ETIAS, Eurodac and the ECRIS-TCN. It should be part of the technical architecture of these systems and serve as the shared component between them for storing and querying the identity data, travel document data and biometric data they process.

(27) All records in the CIR should be logically separated by automatically tagging each record with the name of the underlying system owning that record. The access controls of the CIR should use these tags to determine whether to allow access to the record.

(28) Where a Member State police authority is unable to identify a person due to the lack of a travel document or another credible document proving that person's identity, or where there are doubts about the identity data provided by that person or as to the authenticity of the travel document or the identity of its holder, or where the person is unable or refuses to cooperate, that police authority should be able to query the CIR in order to identify the person. For those purposes, police authorities should capture fingerprints using live-scan fingerprinting techniques, provided that the procedure was initiated in the presence of that person. Such queries of the CIR should not be permitted for the purposes of identifying minors under the age of 12 years old, unless in the best interests of the child.

(29) Where the biometric data of a person cannot be used or if a query with that data fails, the query should be carried out with identity data of the person in combination with travel document data. Where the query indicates that data on that person are stored in the CIR, Member State authorities should have access to the CIR to consult the identity data and travel document data of that person, without the CIR providing any indication as to which EU information system the data belong.

(30) Member States should adopt national legislative measures designating the authorities competent to perform identity checks using the CIR and laying down the procedures, conditions and criteria for such checks, which should follow the principle of proportionality. In particular, the power to collect biometric data during an identity check of a person present before a staff member of those authorities should be provided for by national law.

(31) This Regulation should also introduce a new possibility for streamlined access to data beyond the identity data or travel document data present in the EES, VIS, ETIAS or Eurodac by Member State designated authorities responsible for preventing, detecting or investigating terrorist offences or other serious criminal offences and Europol. Such data may be necessary for the prevention, detection or investigation of terrorist offences or other serious criminal offences in a specific case where there are reasonable grounds to believe that consulting them will contribute to the prevention, detection or investigation of the terrorist offences or other serious criminal offences, in particular where there is a suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence is a person whose data are stored in the EES, VIS, ETIAS or Eurodac.

(32) Full access to data contained in the EU information systems that is necessary for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences, beyond access to identity data or travel document data held in the CIR, should continue to be governed by the applicable legal instruments. The designated authorities responsible for preventing, detecting or investigating terrorist offences or other serious criminal offences and Europol do not know in advance which of the EU information systems contains data of the persons they need to inquire upon. This results in delays and inefficiencies. The end-user authorised by the designated authority should therefore be allowed to see in which of those EU information systems the data corresponding to the result of a query are recorded. The system concerned would thus be flagged following the automated verification of the presence of a match in the system (a so-called match-flag functionality).

(33) In this context, a reply from the CIR should not be interpreted or used as a ground or reason to draw conclusions on or undertake measures in respect of a person, but should be used only for the purpose of submitting an access request to the underlying EU information systems, subject to the conditions and procedures laid down in the respective legal instruments governing such access. Any such access request should be subject to Chapter VII of this Regulation and as applicable, Regulation (EU) 2016/679 of the European Parliament and of the Council ([5]), Directive (EU) 2016/680 of the European Parliament and of the Council ([6]) or Regulation (EU) 2018/1725 of the European Parliament and of the Council ([7]).

(34) As a general rule, where a match-flag indicates that the data are recorded in Eurodac, the designated authorities or Europol should request full access to at least one of the EU information systems concerned. Where exceptionally such full access is not requested, for example because designated authorities or Europol have already obtained the data by other means, or obtaining the data is no longer permitted under national law, the justification for not requesting access should be recorded.

(35) The logs of the queries of the CIR should indicate the purpose of the queries. Where such a query was performed using the two-step data consultation approach, the logs should include a reference to the national file of the investigation or case, thereby indicating that the query was launched for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences.

(36) The query of the CIR by the designated authorities and Europol in order to obtain a match-flag type of response indicating that the data are recorded in the EES, VIS, ETIAS or Eurodac requires automated processing of personal data. A match-flag should not reveal personal data of the concerned individual other than an indication that some of his or her data are stored in one of the systems. No adverse decision for the individual concerned should be made by the authorised end-user solely on the basis of the simple occurrence of a match-flag. Access by the end-user to a match-flag will therefore constitute a very limited interference with the right to protection of personal data of the individual concerned, while allowing the designated authorities and Europol to request access to personal data more effectively.

(37) The MID should be established to support the functioning of the CIR and to support the objectives of the EES, VIS, ETIAS, Eurodac, SIS and ECRIS-TCN. In order to be effective in fulfilling their respective objectives, all of these EU information systems require the accurate identification of the persons whose personal data are stored in them.

(38) To better attain the objectives of EU information systems, the authorities using those systems should be able to conduct sufficiently reliable verifications of the identities of the persons whose data are stored in different systems. The set of identity data or travel document data stored in a given individual system may be incorrect,

([5]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

([6]) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

([7]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons 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 (OJ L 295, 21.11.2018, p. 39).

incomplete or fraudulent, and there is currently no way of detecting incorrect, incomplete or fraudulent identity data or travel document data by way of comparison with data stored in another system. To remedy this situation, it is necessary to have a technical instrument at Union level allowing accurate identification of persons for these purposes.

(39) The MID should create and store links between data in the different EU information systems in order to detect multiple identities, with the dual purpose of facilitating identity checks for *bona fide* travellers and combating identity fraud. The MID should only contain links between data on individuals present in more than one EU information system. The linked data should be strictly limited to the data necessary to verify that a person is recorded in a justified or unjustified manner under different identities in different systems, or to clarify that two persons having similar identity data may not be the same person. Data processing through the ESP and the shared BMS in order to link individual files across different systems should be kept to an absolute minimum and therefore limited to multiple-identity detection, to be conducted at the time new data are added in one of the systems which has data stored in the CIR or added in SIS. The MID should include safeguards against potential discrimination and unfavourable decisions for persons with multiple lawful identities.

(40) This Regulation provides for new data processing operations aimed at identifying the persons concerned correctly. This constitutes an interference with their fundamental rights as protected by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Since the effective implementation of the EU information systems is dependent upon correct identification of the individuals concerned, such interference is justified by the same objectives for which each of those systems have been established, the effective management of the Union's borders, the internal security of the Union and the effective implementation of the Union's asylum and visa policies.

(41) The ESP and the shared BMS should compare data on persons in the CIR and SIS when new records are created or uploaded by a national authority or a Union agency. Such comparison should be automated. The CIR and SIS should use the shared BMS to detect possible links on the basis of biometric data. The CIR and SIS should use the ESP to detect possible links on the basis of alphanumeric data. The CIR and SIS should be able to identify the same or similar data on a person stored across several systems. Where such is the case, a link indicating that it is the same person should be established. The CIR and SIS should be configured in such a way that small transliteration or spelling mistakes are detected in such a way as not to create any unjustified hindrance to the person concerned.

(42) The national authority or Union agency that recorded the data in the respective EU information system should confirm or change the links. This national authority or Union agency should have access to the data stored in the CIR or SIS and in the MID for the purpose of a manual verification of different identities.

(43) A manual verification of different identities should be ensured by the authority creating or updating the data that triggered a match resulting in a link with data stored in another EU information system. The authority responsible for the manual verification of different identities should assess whether there are multiple identities referring to the same person in a justified or unjustified manner. Such an assessment should be performed where possible in the presence of the person concerned and where necessary by requesting additional clarifications or information. The assessment should be performed without delay, in line with legal requirements for the accuracy of information under Union and national law.

(44) For links obtained through SIS related to alerts in respect of persons wanted for arrest for surrender or extradition purposes, on missing or vulnerable persons, on persons sought to assist with a judicial procedure or on persons for discreet checks, inquiry checks or specific checks, the authority responsible for the manual verification of different identities should be the SIRENE Bureau of the Member State that created the alert. These categories of SIS alerts are sensitive and should not necessarily be shared with the authorities creating or

updating data that are linked to them in one of the other EU information systems. The creation of a link with SIS data should be without prejudice to the actions to be taken in accordance with Regulations (EU) 2018/1860 ([8]), (EU) 2018/1861 ([9]) and (EU) 2018/1862 ([10]) of the European Parliament and of the Council.

(45) The creation of such links requires transparency towards the individuals affected. In order to facilitate the implementation of the necessary safeguards in accordance with applicable Union data protection rules, individuals who are subject to a red link or a white link following manual verification of different identities should be informed in writing without prejudice to limitations to protect security and public order, prevent crime and guarantee that national investigations are not jeopardised. Those individuals should receive a single identification number allowing them to identify the authority to which they should address themselves to exercise their rights.

(46) Where a yellow link is created, the authority responsible for the manual verification of different identities should have access to the MID. Where a red link exists, Member State authorities and Union agencies having access to at least one EU information system included in the CIR or to SIS should have access to the MID. A red link should indicate that a person is using different identities in an unjustified manner or that a person is using somebody else's identity.

(47) Where a white or green link exists between data from two EU information systems, Member State authorities and Union agencies should have access to the MID where the authority or agency concerned has access to both information systems. Such access should be granted for the sole purpose of allowing that authority or agency to detect potential cases where data have been linked incorrectly or processed in the MID, CIR and SIS in breach of this Regulation and of taking action to correct the situation and update or delete the link.

(48) The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) should establish automated data quality control mechanisms and common data quality indicators. eu-LISA should be responsible for developing a central monitoring capacity for data quality and for producing regular data analysis reports to improve the control of the implementation by Member States of EU information systems. The common data quality indicators should include minimum quality standards for storing data in the EU information systems or interoperability components. The goal of such data quality standards should be for the EU information systems and interoperability components to identify automatically apparently incorrect or inconsistent data submissions, so that the originating Member State is able to verify the data and carry out any necessary remedial action.

(49) The Commission should evaluate eu-LISA's quality reports and should issue recommendations to Member States where appropriate. Member States should be responsible for preparing an action plan describing actions to remedy any deficiencies in data quality and should report on its progress regularly.

(50) The universal message format (UMF) should serve as a standard for structured, cross-border information exchange between information systems, authorities or organisations in the field of Justice and Home Affairs. The UMF should define a common vocabulary and logical structures for commonly exchanged information with the objective to facilitate interoperability by enabling the creation and reading of the contents of exchanges in a consistent and semantically equivalent manner.

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

([8]) Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals (OJ L 312, 7.12.2018, p. 1).

([9]) Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 (OJ L 312, 7.12.2018, p. 14).

([10]) Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56).

(52) A central repository for reporting and statistics (CRRS) should be established to generate cross-system statistical data and analytical reporting for policy, operational and data quality purposes in accordance with the applicable legal instruments. eu-LISA should establish, implement and host the CRRS in its technical sites. It should contain anonymised statistical data from the EU information systems, the CIR, the MID and the shared BMS. The data contained in the CRRS should not enable the identification of individuals. eu-LISA should render the data anonymous in an automated manner and should record such anonymised data in the CRRS. The process for rendering the data anonymous should be automated and no direct access by eu-LISA staff should be granted to any personal data stored in the EU information systems or in the interoperability components.

(53) Regulation (EU) 2016/679 applies to the processing of personal data for the purpose of interoperability under this Regulation by national authorities unless such processing is carried out by the designated authorities or central access points of the Member States for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences.

(54) Where the processing of personal data by the Member States for the purpose of interoperability under this Regulation is carried out by the competent authorities for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences, Directive (EU) 2016/680 applies.

(55) Regulation (EU) 2016/679, Regulation (EU) 2018/1725 or, where relevant, Directive (EU) 2016/680 apply to any transfer of personal data to third countries or international organisations carried out under this Regulation. Without prejudice to the grounds for transfer pursuant to Chapter V of Regulation (EU) 2016/679 or, where relevant, Directive (EU) 2016/680, any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data should only be recognised or enforceable in any manner if based on an international agreement in force between the requesting third country and the Union or a Member State.

(56) The specific provisions on data protection of Regulation (EU) 2018/1862 and Regulation (EU) 2019/816 of the European Parliament and of the Council ([11]) apply to the processing of personal data in the systems governed by those Regulations.

(57) Regulation (EU) 2018/1725 applies to the processing of personal data by eu-LISA and other institutions and bodies of the Union when carrying out their responsibilities under this Regulation, without prejudice to Regulation (EU) 2016/794, which applies to the processing of personal data by Europol.

(58) The supervisory authorities referred to in Regulation (EU) 2016/679 or Directive (EU) 2016/680 should monitor the lawfulness of the processing of personal data by the Member States. The European Data Protection Supervisor should monitor the activities of the Union institutions and bodies in relation to the processing of personal data. The European Data Protection Supervisor and the supervisory authorities should cooperate with each other in the monitoring of the processing of personal data by interoperability components. For the European Data Protection Supervisor to fulfil the tasks entrusted to it under this Regulation, sufficient resources, including both human and financial resources, are required.

(59) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council ([12]) and delivered an opinion on 16 April 2018 ([13]).

(60) The Article 29 Data Protection Working Party provided an opinion on 11 April 2018.

(61) Both the Member States and eu-LISA should maintain security plans in order to facilitate the implementation of security obligations and should cooperate with each other in order to address security issues. eu-LISA should also make sure there is a continuous use of the latest technological developments to ensure data integrity in the context of the development, design and management of the interoperability components. eu-LISA's obligations

([11]) Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 (see page 1 of this Official Journal).

([12]) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

([13]) OJ C 233, 4.7.2018, p. 12.

in this respect should include adopting the measures necessary to prevent access by unauthorised persons, such as staff of external service providers, to personal data processed through the interoperability components. When awarding contracts for the provision of services, the Member States and eu-LISA should consider all measures necessary to secure compliance with laws or regulations relating to the protection of personal data and to the privacy of individuals or to safeguard essential security interests, pursuant to Regulation (EU) 2018/1046 of the European Parliament and of the Council ([14]) and applicable international conventions. eu-LISA should apply the principles of privacy by design and by default during the development of the interoperability components.

(62) To support the purposes of statistics and reporting, it is necessary to grant access to authorised staff of the competent authorities, Union institutions and agencies referred to in this Regulation to consult certain data related to certain interoperability components without enabling the identification of individuals.

(63) In order to allow Member State authorities and Union agencies to adapt to the new requirements on the use of the ESP, it is necessary to provide for a transitional period. Similarly, in order to allow for a coherent and optimal functioning of the MID, transitional measures should be established for the start of its operations.

(64) Since the objective of this Regulation, namely, the establishment of a framework for interoperability between EU information systems cannot be sufficiently achieved by the Member States but can rather, by reason of the scale and effects of the action, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(65) The remaining amount in the budget earmarked for smart borders in Regulation (EU) No 515/2014 of the European Parliament and the Council ([15]) should be reallocated to this Regulation pursuant to Article 5(5)(b) of Regulation (EU) No 515/2014, to cover the costs of the development of the interoperability components.

(66) In order to supplement certain detailed technical aspects of this Regulation, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union (TFEU) should be delegated to the Commission in respect of:

— extending the transitional period for the use of the ESP;

— extending the transitional period for multiple-identity detection carried out by the ETIAS Central Unit;

— the procedures for determining the cases where identity data can be considered as the same or similar;

— the rules on the operation of the CRRS, including specific safeguards for processing of personal data and the security rules applicable to the repository; and

— detailed rules on the operation of the web portal.

It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making ([16]). In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member State' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(67) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to determine the dates from which the ESP, the shared BMS, the CIR, the MID and the CRRS are to start operations.

([14]) Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 (OJ L 193, 30.7.2018, p. 1).

([15]) Regulation (EU) No 515/2014 of the European Parliament and of the Council of 16 April 2014 establishing as part of the Internal Security Fund, the Instrument for financial support for external borders and visa and repealing Decision No 574/2007/EC (OJ L 150, 20.5.2014, p. 143).

([16]) OJ L 123, 12.5.2016, p. 1.

(68) Implementing powers should also be conferred on the Commission relating to the adoption of detailed rules on: the technical details of the ESP user profiles; the specifications of the technical solution allowing the EU information systems, Europol data and Interpol databases to be queried through the ESP and the format of the ESP's replies; the technical rules for creating links in the MID between data from different EU information systems; the content and presentation of the form to be used to inform the data subject when a red link is created; the performance requirements and performance monitoring of the shared BMS; automated data quality control mechanisms, procedures and indicators; the development of the UMF standard; the cooperation procedure to be used in the case of a security incident; and the specifications of the technical solution for Member States to manage users access requests. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council ([17]).

(69) As the interoperability components will involve the processing of significant amounts of sensitive personal data, it is important that persons whose data are processed through those components can effectively exercise their rights as data subjects as required under Regulation (EU) 2016/679, Directive (EU) 2016/680 and Regulation (EU) 2018/1725. The data subjects should be provided with a web portal that facilitates their exercise of their rights of access to, rectification, erasure and restriction of processing of their personal data. eu-LISA should establish and manage such a web portal.

(70) One of the core principles of data protection is data minimisation: under Article 5(1)(c) of Regulation (EU) 2016/679, the processing of personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. For this reason, the interoperability components should not provide for the storage of any new personal data, with the exception of the links which will be stored in the MID and which are the minimum necessary for the purposes of this Regulation.

(71) This Regulation should contain clear provisions on liability and the right to compensation for unlawful processing of personal data and for any other act incompatible with it. Such provisions should be without prejudice to the right to compensation from, and liability of the controller or processor under Regulation (EU) 2016/679, Directive (EU) 2016/680 and Regulation (EU) 2018/1725. eu-LISA should be responsible for any damage it causes in its capacity as a data processor where it has not complied with the obligations specifically imposed on it by this Regulation, or where it has acted outside or contrary to lawful instructions of the Member State which is the data controller

(72) This Regulation is without prejudice to the application of Directive 2004/38/EC of the European Parliament and of the Council ([18]).

(73) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the TEU and to the TFEU, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Given that this Regulation, insofar as its provisions relate to SIS as governed by Regulation (EU) 2018/1862, builds upon the Schengen *acquis*, Denmark shall, in accordance with Article 4 of that Protocol, decide within a period of six months after the Council has decided on this Regulation whether it will implement it in its national law.

(74) Insofar as its provisions relate to SIS as governed by Regulation (EU) 2018/1862, the United Kingdom is taking part in this Regulation, in accordance with Article 5(1) of Protocol No 19 on the Schengen *acquis* integrated into the framework of the European Union, annexed to the TEU and to the TFEU and Article 8(2) of Council Decision 2000/365/EC ([19]). Furthermore, insofar as its provisions relate to Eurodac and to ECRIS-TCN, in accordance with Article 3 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the TEU and to the TFEU, the United Kingdom has notified, by letter of 18 May 2018, its wish to take part in the adoption and application of this Regulation.

([17]) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

([18]) Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (OJ L 158, 30.4.2004, p. 77).

([19]) Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis* (OJ L 131, 1.6.2000, p. 43).

(75) Insofar as its provisions relate to SIS as governed by Regulation (EU) 2018/1862, Ireland could, in principle, take part in this Regulation, in accordance with Article 5(1) of Protocol No 19 on the Schengen *acquis* integrated into the framework of the European Union, annexed to the TEU and to the TFEU, and Article 6(2) of Council Decision 2002/192/EC ([20]). Furthermore, insofar as its provisions relate to Eurodac and to ECRIS-TCN, in accordance with Articles 1 and 2 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the TEU and the TFEU, and without prejudice to Article 4 of that Protocol, Ireland is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Since it is not possible, under these circumstances, to ensure that this Regulation is applicable in its entirety to Ireland, as required by Article 288 of the TFEU, Ireland is not taking part in the adoption of this Regulation and is not bound by it or subject to its application, without prejudice to its rights under Protocols No 19 and No 21.

(76) As regards Iceland and Norway, this Regulation constitutes, insofar as it relates to SIS as governed by Regulation (EU) 2018/1862, a development of the provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latters' association with the implementation, application and development of the Schengen *acquis* ([21]) which fall within the area referred to in Article 1, point G of Council Decision 1999/437/EC ([22]).

(77) As regards Switzerland, this Regulation constitutes insofar as it relates to SIS as governed by Regulation (EU) 2018/1862, a development of the provisions of the Schengen *acquis* within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* ([23]) which fall within the area referred to in Article 1, point G of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/149/JHA ([24]).

(78) As regards Liechtenstein, this Regulation constitutes insofar as it relates to SIS as governed by Regulation (EU) 2018/1862, a development of the provisions of the Schengen *acquis* within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* ([25]) which fall within the area referred to in Article 1, point G of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU ([26]).

(79) This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union and should be applied in accordance with those rights and principles.

(80) In order to have this Regulation fit into the existing legal framework, Regulation (EU) 2018/1726 of the European Parliament and of the Council ([27]) and Regulations (EU) 2018/1862 and (EU) 2019/816 should be amended accordingly,

---

([20]) Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen *acquis* (OJ L 64, 7.3.2002, p. 20).

([21]) OJ L 176, 10.7.1999, p. 36.

([22]) Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis* (OJ L 176, 10.7.1999, p. 31).

([23]) OJ L 53, 27.2.2008, p. 52.

([24]) Council Decision 2008/149/JHA of 28 January 2008 on the conclusion on behalf of the European Union of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L 53, 27.2.2008, p. 50).

([25]) OJ L 160, 18.6.2011, p. 21.

([26]) Council Decision 2011/350/EU of 7 March 2011 on the conclusion, on behalf of the European Union, of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*, relating to the abolition of checks at internal borders and movement of persons (OJ L 160, 18.6.2011, p. 19).

([27]) Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011 (OJ L 295, 21.11.2018, p. 99).

HAVE ADOPTED THIS REGULATION:

CHAPTER I

General provisions

Article 1

Subject matter

1. This Regulation, together with Regulation (EU) 2019/817 of the European Parliament and of the Council ([28]), establishes a framework to ensure 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. 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).

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 on 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, development and operation of the interoperability components.

4. This Regulation also adapts the procedures and conditions for the designated authorities and for the European Union Agency for Law Enforcement Cooperation (Europol) to access the EES, VIS, ETIAS and Eurodac for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences.

5. This Regulation also lays down a framework for verifying the identity of persons and for identifying persons.

Article 2

Objectives

1. By ensuring interoperability, this Regulation has the following objectives:

(a) to improve the effectiveness and efficiency of border checks at external borders;

(b) to contribute to the prevention and the combating of illegal immigration;

(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 security in the territories of the Member States;

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

(e) to assist in the examination of applications for international protection;

(f) to contribute to the prevention, detection and investigation of terrorist offences and of other serious criminal offences;

(g) to facilitate the identification of unknown persons who are unable to identify themselves or unidentified human remains in case of a natural disaster, accident or terrorist attack.

2. The objectives referred to in paragraph 1 shall be achieved by:

(a) ensuring the correct identification of persons;

(b) contributing to combating identity fraud;

([28]) Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (see page 27 of this Official Journal).

(c) improving data quality and harmonising the quality requirements for the data stored in the EU information systems while respecting the data processing requirements of the legal instruments governing the individual systems, data protection standards and principles;

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

(e) strengthening, simplifying and making more uniform the data security and data protection conditions that govern the respective EU information systems, without affecting the special protection and safeguards afforded to certain categories of data;

(f) streamlining the conditions for designated authorities' access to the EES, VIS, ETIAS and Eurodac, while ensuring necessary and proportionate conditions for that access;

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

Article 3

Scope

1. This Regulation applies to Eurodac, SIS and ECRIS-TCN.

2. This Regulation also applies to Europol data to the extent of enabling them to be queried simultaneously with the EU information systems referred to in paragraph 1.

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.

Article 4

Definitions

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

(1) 'external borders' means external borders as defined in point (2) of Article 2 of Regulation (EU) 2016/399 of the European Parliament and of the Council ([29]);

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

(3) 'border authority' means the border guard assigned in accordance with national law to carry out border checks;

(4) 'supervisory authorities' means the supervisory authority referred to in Article 51(1) of Regulation (EU) 2016/679 and the supervisory authority referred to in 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) 'alphanumeric data' means data represented by letters, digits, special characters, spaces and punctuation marks;

(8) 'identity data' means the data referred to in Article 27(3)(a) to (e);

(9) 'fingerprint data' means fingerprint images and images of fingerprint latents, which due to their unique character and the reference points contained therein enable accurate and conclusive comparisons on a person's identity;

([29]) Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ L 77, 23.3.2016, p. 1).

(10) 'facial image' means digital images of the face;

(11) 'biometric data' means fingerprint data or facial images or both;

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

(13) 'travel document' means a passport or other equivalent document entitling the holder to cross the external borders and to which a visa can be affixed;

(14) '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;

(15) 'EU information systems' means the EES, VIS, ETIAS, Eurodac, SIS and ECRIS-TCN;

(16) 'Europol data' means personal data processed by Europol for the purpose referred to in Article 18(2)(a), (b) and (c) of Regulation (EU) 2016/794;

(17) 'Interpol databases' means the Interpol Stolen and Lost Travel Document database (SLTD database) and the Interpol Travel Documents Associated with Notices database (TDAWN database);

(18) 'match' means the existence of a correspondence as a result of an automated comparison between personal data recorded or being recorded in an information system or database;

(19) 'police authority' means the competent authority as defined in point (7) of Article 3 of Directive (EU) 2016/680;

(20) 'designated authorities' means the Member State designated authorities as defined in point (26) of Article 3(1) of Regulation (EU) 2017/2226 of the European Parliament and of the Council ([30]), point (e) of Article 2(1) of Council Decision 2008/633/JHA ([31]), and point (21) of Article 3(1) of Regulation (EU) 2018/1240 of the European Parliament and of the Council ([32]);

(21) '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 of the European Parliament and of the Council ([33]);

(22) 'serious criminal offence' means an offence which corresponds or is equivalent to one of the offences referred to in Article 2(2) of Council Framework Decision 2002/584/JHA ([34]), if it is punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years;

(23) 'Entry/Exit System' or 'EES' means the Entry/Exit System established by Regulation (EU) 2017/2226;

(24) 'Visa Information System' or 'VIS' means the Visa Information System established by Regulation (EC) No 767/2008 of the European Parliament and of the Council ([35]);

(25) 'European Travel Information and Authorisation System' or 'ETIAS' means the European Travel Information and Authorisation System established by Regulation (EU) 2018/1240;

([30]) Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (EES Regulation) (OJ L 327, 9.12.2017, p. 20).

([31]) Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (OJ L 218, 13.8.2008, p. 129).

([32]) Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018, p. 1).

([33]) Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, p. 6).

([34]) Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1).

([35]) Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) (OJ L 218, 13.8.2008, p. 60).

(26) 'Eurodac' means Eurodac established by Regulation (EU) No 603/2013 of the European Parliament and of the Council ([36]);

(27) 'Schengen Information System' or 'SIS' means the Schengen Information System established by Regulations (EU) 2018/1860, (EU) 2018/1861 and (EU) 2018/1862;

(28) 'ECRIS-TCN' means the centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons established by Regulation (EU) 2019/816.

Article 5

Non-discrimination and fundamental rights

Processing of personal data for the purposes of this Regulation shall not result in discrimination against persons on any grounds such as gender, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation. It shall fully respect human dignity and integrity and fundamental rights, including the right to respect for one's private life and to the protection of personal data. Particular attention shall be paid to children, the elderly, persons with a disability and persons in need of international protection. The best interests of the child shall be a primary consideration.

CHAPTER II

European search portal

Article 6

European search portal

1. A European search portal (ESP)is established for the purposes of facilitating the fast, seamless, efficient, systematic and controlled access of Member State authorities and Union agencies to the EU information systems, to Europol data and to the Interpol databases for the performance of their tasks and in accordance with their access rights and the objectives and purposes of the EES, VIS, ETIAS, Eurodac, SIS and ECRIS-TCN.

2. The ESP shall be composed of:

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

(b) a secure communication channel between the ESP, Member States and Union agencies that are entitled to use the ESP;

(c) a secure communication infrastructure between the ESP and the EES, VIS, ETIAS, Eurodac, Central SIS, ECRIS-TCN, Europol data and the Interpol databases as well as between the ESP and the central infrastructures of the CIR and the 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 Union agencies having access, to at least one of the EU information systemsin accordance with the legal instruments governing those EU information systems, to the CIR and the MID in accordance with this Regulation, to Europol data in accordance with Regulation (EU) 2016/794or to the Interpol databases in accordance with Union or national law governing such access.

Those Member State authorities and Union agencies may make use of the ESP and the data provided by it only for the objectives and purposes laid down in the legal instruments governing those EU information systems, in Regulation (EU) 2016/794 and in this Regulation.

([36]) Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 180, 29.6.2013, p. 1).

2. The Member State authorities and Union agencies 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 ECRIS-TCN in accordance with their access rights as referred to in the legal instruments governing those EU information systems and in 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 Regulations (EU) 2018/1860 and (EU) 2018/1861.

4. Where provided for under Union law, the Union agencies referred to in paragraph 1 shall use the ESP to search data related to persons or their travel documents in the Central-SIS.

5. The Member State authorities and Union agencies 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 8

Profiles for the users of the European search portal

1. For the purposes of enabling the use of the ESP, eu-LISA shall, in cooperation with Member States, create a profile based on each category of ESP user and on the purposes of the queries, in accordance with the technical details and access rights referred to in paragraph 2. Each profile shall, in accordance with Union and national law, comprise the following information:

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

(b) the EU information systems, Europol data and the Interpol databases that are to be queried, those that can be queried and those that are to provide a reply to the user;

(c) the specific data in the EU information systems, Europol data and the Interpol databases that may be queried;

(d) the categories of data that may be provided in each reply.

2. The Commission shall adopt implementing acts to specify the technical details of the profiles referred to in paragraph 1 in accordance with the ESP users' access rights under the legal instruments governing the EU information systems and under national law. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 70(2).

3. The profiles referred to in paragraph 1 shall be reviewed regularly by eu-LISA in cooperation with Member States, at least once per year, and if necessary updated.

Article 9

Queries

1. The ESP users shall launch a query by submitting alphanumeric or biometric data to the ESP. Where a query has been launched, the ESP shall query the EES, ETIAS, VIS, SIS, Eurodac, ECRIS-TCN, the CIR, Europol data and the Interpol databases simultaneously with the data submitted by the user and in accordance with the user profile.

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

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

4. When a query is launched by an ESP user, the EES, ETIAS, VIS, SIS, Eurodac, ECRIS-TCN, the CIR, the MID, the Europol data and the Interpol databases shall in reply to the query provide the data that they hold.

Without prejudice to Article 20, the reply provided by the ESP shall indicate to which EU information system or database the data belong.

The ESP shall provide no information regarding data in EU information systems, Europol data and the Interpol databases to which the user has no access under the applicable Union and national law.

5. Any queries of the Interpol databases launched via the ESP shall be performed in such a way that no information shall be revealed to the owner of the Interpol alert.

6. The ESP shall provide replies to the user as soon as data are available from one of the EU information systems, Europol data or Interpol databases. Those replies shall contain only the data to which the user has access under Union and national law.

7. The Commission shall adopt an implementing act to specify the technical procedure for the ESP to query the EU information systems, Europol data and Interpol databases and the format of the ESP replies. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 70(2).

Article 10

Keeping of logs

1. Without prejudice to Articles 12 and 18 of Regulation (EU) 2018/1862, Article 29 of Regulation (EU) 2019/816 and Article 40 of Regulation (EU) 2016/794, eu-LISA shall keep logs of all data processing operations in the ESP. Those logs shall include the following:

(a) the Member State or Union agency launching the query and the ESP profile used;

(b) the date and time of the query;

(c) the EU information systems and the Europol data queried.

2. Each Member State shall keep logs of queries that its authorities and the staff of those authorities duly authorised to use the ESP make. Each Union agency shall keep logs of queries that its duly authorised staff make.

3. The logs referred to in paragraphs 1 and 2 may be used only for data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, and for ensuring data security and integrity. Those logs shall be protected by appropriate measures against unauthorised access and erased one year after their creation. If, however, they are required for monitoring procedures that have already begun, they shall be erased once the monitoring procedures no longer require the logs.

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 or the CIR, because of a failure of the ESP, the ESP users shall be notified in an automated manner by eu-LISA.

2. Where it is technically impossible to use the ESP to query one or several EU information systems or the CIR, because of a failure of the national infrastructure in a Member State, that Member State shall notify eu-LISA and the Commission in an automated manner.

3. In the cases referred to in paragraphs 1 or 2 of this Article, and until the technical failure is addressed, the obligation referred to in Article 7(2) and (4) shall not apply and Member States shall access the EU information systems or the CIR directly where they are required to do so under Union or national law.

4. Where it is technically impossible to use the ESP to query one or several EU information systems or the CIR, because of a failure of the infrastructure of a Union agency, that agency shall notify eu-LISA and the Commission in an automated manner.

CHAPTER III

Shared biometric matching service

Article 12

Shared biometric matching service

1. A shared biometric matching service (shared BMS) storing biometric templates obtained from the biometric data referred to in Article 13, that are stored in the CIR and SIS and enabling querying with biometric data across several EU information systems is established for the purposes of supporting the CIR and the MID and the objectives of the EES, VIS, Eurodac, SIS and ECRIS-TCN.

2. The shared BMS shall be composed of:

(a) a central infrastructure, which shall replace the central systems of the EES, VIS, SIS, Eurodac and ECRIS-TCN respectively, to the extent that it shall store biometric templates and allow searches with biometric data;

(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

Storing biometric templates in the shared biometric matching service

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

(a) the data referred to in Article 20(3)(w) and (y), excluding data on palm prints, of Regulation (EU) 2018/1862;

(b) the data referred to in Article 5(1)(b) and (2) of Regulation (EU) 2019/816.

The biometric templates shall be stored in the shared BMS in logically separated form according to the EU information system from which the data originate.

2. For each set of data referred to in paragraph 1, the shared BMS shall include in each biometric template a reference to the EU information systems in which the corresponding biometric data are stored and a reference to the actual records in those EU information systems.

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 EU 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).

5. The Commission shall lay down, by means of an implementing act, the performance requirements and practical arrangements for monitoring the performance of the shared BMS in order to ensure that the effectiveness of biometric searches respect time-critical procedures such as border checks and identifications. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 70(2).

Article 14

Searching biometric data with the shared biometric matching service

In order to search the biometric data stored within the CIR and SIS, the CIR and 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 Regulations (EC) No 767/2008, (EU) 2017/2226, (EU) 2018/1860, (EU) 2018/1861, (EU) 2018/1862 and (EU) 2019/816.

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 only for as long as the corresponding biometric data are stored in the CIR or SIS. The data shall be erased from the shared BMS in an automated manner.

Article 16

Keeping of logs

1. Without prejudice to Articles 12 and 18 of Regulation (EU) 2018/1862 and Article 29 of Regulation (EU) 2019/816, eu-LISA shall keep logs of all data processing operations in the shared BMS. Those logs shall include the following:

(a) the Member State or Union agency launching the query;

(b) the history of the creation and storage of biometric templates;

(c) the EU information systems queried with the biometric templates stored in the shared BMS;

(d) the date and time of the query;

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

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

2. Each Member State shall keep logs of queries that its authorities and the staff of those authorities duly authorised to use the shared BMS make. Each Union agency shall keep logs of queries that its duly authorised staff make.

3. The logs referred to in paragraphs 1 and 2 may be used only for data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, and for ensuring data security and integrity. Those logs shall be protected by appropriate measures against unauthorised access and erased one year after their creation. If, however, they are required for monitoring procedures that have already begun, they shall be erased once the monitoring procedures no longer require the logs.

CHAPTER IV

Common identity repository

Article 17

Common identity repository

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

2. The CIR shall be composed of:

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

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

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

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

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

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

Article 18

The common identity repository data

1. The CIR shall store the following data, logically separated according to the information system from which the data have originated: the data referred to in Article 5(1)(b) and (2) and the following data listed in Article 5(1)(a) of Regulation (EU) 2019/816: surname (family name), first names (given names), date of birth, place of birth (town and country), nationality or nationalities, gender, previous names, if applicable, where available pseudonyms or aliases, as well as, where available, information on travel documents.

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

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

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

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

Article 19

Adding, amending and deleting data in the common identity repository

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

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

Article 20

Access to the common identity repository for identification

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

(a) where a police authority is unable to identify a person due to the lack of a travel document or another credible document proving that person's identity;

(b) where there are doubts about the identity data provided by a person;

(c) where there are doubts as to the authenticity of the travel document or another credible document provided by a person;

(d) where there are doubts as to the identity of the holder of a travel document or of another credible document; or

(e) where a person is unable or refuses to cooperate.

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

2. Where one of the circumstances listed in paragraph 1 arises and a police authority has been so empowered by national legislative measures as referred to in paragraph 5, it may, solely for the purpose of identifying a person, query the CIR with the biometric data of that person taken live during an identity check, provided that the procedure was initiated in the presence of that person.

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

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

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

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

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

Article 21

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

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

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

Article 22

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

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

2. Where, in reply to a query the CIR indicates that data on that person are present in Eurodac, the CIR shall provide to designated authorities and Europol a reply in the form of a reference as referred to in Article 18(2) indicating that Eurodac contains matching data. The CIR shall reply in such a way that the security of the data is not compromised.

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

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

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

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

Article 23

Data retention in the common identity repository

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

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

Article 24

Keeping of logs

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

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

(a) the Member State or Union agency launching the query;

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

(c) the date and time of the query;

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

(e) the results of the query.

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

(a) the Member State or Union agency launching the query;

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

(c) the date and time of the query;

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

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

(a) the date and time of the query;

(b) the data used to launch the query;

(c) the results of the query;

(d) the Member State or Union agency querying the CIR.

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

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

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

(a) the national file reference;

(b) the purpose of access;

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

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

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

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

CHAPTER V

Multiple-identity detector

Article 25

Multiple-identity detector

1. A multiple-identity detector (MID) creating and storing identity confirmation files as referred to in Article 34, containing links between data in the EU information systems included in the CIR and SIS and allowing detection of 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, VIS, ETIAS, Eurodac, SIS and ECRIS-TCN.

2. The MID shall be composed of:

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

(b) a secure communication infrastructure to connect the MID with SIS and the central infrastructures of the ESP 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 verification of different identities referred to in Article 29, access to the data referred to in Article 34 stored in the MID shall be granted to:

(a) the SIRENE Bureau of the Member State creating or updating an alert in accordance with Regulation (EU) 2018/1862;

(b) the central authorities of the convicting Member State when recording or modifying data in ECRIS-TCN in accordance with Article 5 or 9 of Regulation (EU) 2019/816.

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

3. Member State authorities and Union agencies shall have access to the white links referred to in Article 33 where they have access to the two EU information systems containing data between which the white link was created.

4. Member State authorities and Union agencies shall have access to the green links referred to in Article 31 where they have access to the two EU information systems containing data between which the green link was created and a query of those information systems has revealed a match with the two sets of linked data.

Article 27

Multiple-identity detection

1. Multiple-identity detection in the CIR and SIS shall be launched where:

(a) an alert on a person is created or updated in SIS in accordance with Chapters VI to IX of Regulation (EU) 2018/1862;

(b) a data record is created or modified in ECRIS-TCN in accordance with Article 5 or 9 of Regulation (EU) 2019/816.

2. Where the data contained within an EU information system referred to in paragraph 1 contains biometric data, the CIR and Central SIS shall use the shared BMS in order to perform 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 data belonging to the same person are already stored in the CIR or in Central-SIS.

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

(a) surnames, forenames, names at birth, previously used names and aliases, place of birth, date of birth, gender and any nationalities held as referred to in Article 20(3) of Regulation (EU) 2018/1862;

(b) surname (family name), first names (given names), date of birth, place of birth (town and country), nationality or nationalities and gender as referred to in Article 5(1)(a) of Regulation (EU) 2019/816.

4. In addition to the process referred to in paragraphs 2 and 3, the CIR and Central SIS shall use the ESP to search the data stored in Central SIS and the CIR respectively using travel document data.

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

Article 28

Results of the multiple-identity detection

1. Where the queries referred to in Article 27(2), (3) and (4) do not report any match, the procedures referred to in Article 27(1) shall continue in accordance with the legal instruments governing them.

2. Where the query laid down in Article 27(2), (3) and (4) reports one or several matches, the CIR and, where relevant, SIS shall create a link between the data used to launch the query and the data triggering the match.

Where several matches are reported, a link shall be created between all data triggering the match. Where the data were 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), (3) and (4) reports one or several matches and the identity data of the linked files are the same or similar, a white link shall be created in accordance with Article 33.

4. Where the query referred to in Article 27(2), (3) and (4) reports one or several match(es) and the identity data of the linked files cannot be considered to be 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 adopt delegated acts in accordance with Article 69 laying down the procedures to determine the cases in which identity data can be considered to be the same or similar.

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

7. The Commission shall, in cooperation with eu-LISA, lay down the technical rules for creating links between data from different EU information systems, by implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 70(2).

Article 29

Manual verification of different identities and the authorities responsible

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

(a) the SIRENE Bureau of the Member State for matches that occurred when creating or updating a SIS alert in accordance with Regulation (EU) 2018/1862;

(b) the central authorities of the convicting Member State for matches that occurred when recording or modifying data in ECRIS-TCN in accordance with Article 5 or 9 of Regulation (EU) 2019/816.

The MID shall indicate the authority responsible for the manual verification of different identities in the identity confirmation file.

2. The authority responsible for the manual 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 in an alert:

(a) in respect of persons wanted for arrest for surrender or extradition purposes referred to in Article 26 of Regulation (EU) 2018/1862;

(b) on missing or vulnerable persons referred to in Article 32 of Regulation (EU) 2018/1862;

(c) on persons sought to assist with a judicial procedure referred to in Article 34 of Regulation (EU) 2018/1862;

(d) on persons for discreet checks, inquiry checks or specific checks referred to in Article 36 of Regulation (EU) 2018/1862.

3. The authority responsible for the manual verification of different identities shall have access to the linked data contained in the relevant identity confirmation file and to the identity data linked in the CIR and, where relevant, in SIS. It shall assess the different identities without delay. Once such assessment is completed, it shall update the link in accordance with Articles 31, 32 and 33 and add it to the identity confirmation file without delay.

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

5. Where data reporting a match were already linked, the authority responsible for the manual verification of different identities shall take into account the existing links when assessing the creation of new links.

Article 30

Yellow link

1. Where manual verification of different identities has not yet taken place, a link between data from two or more EU information systems shall be classified as yellow in any of the following cases:

(a) the linked data share the same biometric data but have similar or different identity data;

(b) the linked data have different identity data but share the same travel document data, and at least one of the EU information systems does not contain biometric data on the person concerned;

(c) the linked data share the same identity data but have different biometric data;

(d) the linked data have similar or different identity data, and share the same travel document data, but have different biometric data.

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 EU information systems shall be classified as green where:

(a) the linked data have different biometric data but share the same identity data and the authority responsible for the manual verification of different identities has concluded that the linked data refer to two different persons;

(b) the linked data have different biometric data, have similar or different identity data, share the same travel document data and the authority responsible for the manual verification of different identities has concluded that the linked data refer to two different persons;

(c) the linked data have different identity data but share the same travel document data, at least one of the EU information systems does not contain biometric data on the person concerned and the authority responsible for the manual verification of different identities has concluded that the linked data refer to two different persons.

2. Where the CIR or SIS are queried and where a green link exists between data in two or more of the EU information systems, the MID shall indicate that the identity data of the linked data do not correspond to the same person.

3. If a Member State authority has evidence to suggest that a green link has been incorrectly recorded in the MID, that a green link is out of date or that data were processed in the MID or the EU information systems 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 of different identities without delay.

Article 32

Red link

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

(a) the linked data share the same biometric data but have similar or different identity data and the authority responsible for the manual verification of different identities has concluded that the linked data refer to the same person in an unjustified manner;

(b) the linked data have the same, similar or different identity data and the same travel document data, but different biometric data and the authority responsible for the manual verification of different identities has concluded that the linked data refer to two different persons, at least one of whom is using the same travel document in an unjustified manner;

(c) the linked data share the same identity data, but have different biometric data and different or no travel document data and the authority responsible for the manual verification of different identities has concluded that the linked datarefer to two different persons in an unjustified manner;

(d) the linked data have different identity data, but share the same travel document data, at least one of the EU information systems does not contain biometric data on the person concerned and the authority responsible for the manual verification of different identities has concluded that the linked datarefer to the same person in an unjustified manner.

2. Where the CIR or SIS are queried and where a red link exists between data in two or more of the EU information systems, the MID shall indicate the data referred to in Article 34. Follow-up to a red link shall take place in accordance with Union and national law, with any legal consequence for the person concerned being based only on the relevant data on that person. No legal consequence for the person concerned shall derive solely from the existence of a red link.

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

4. Without prejudice to the provisions related to the handling of alerts in SIS contained in Regulations (EU) 2018/1860, (EU) 2018/1861 and (EU) 2018/1862, and without prejudice to limitations necessary to protect security and public order, prevent crime and guarantee that no national investigation will be jeopardised, where a red link is created, the authority responsible for the manual verification of different identities shall inform the person concerned of the presence of multiple unlawful identity data and shall provide the person with the single identification number referred to in Article 34(c) of this Regulation, a reference to the authority responsible for the manual verification of different identities referred to in Article 34(d) of this Regulation and the website address of the web portal established in accordance with Article 49 of this Regulation.

5. The information referred to in paragraph 4 shall be provided in writing by means of a standard form by the authority responsible for the manual verification of different identities. The Commission shall determine the content and presentation of that form by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 70(2).

6. Where a red link is created, the MID shall notify the authorities responsible for the linked data in an automated manner.

7. If a Member State authority or Union agency having access to the CIR or SIS has evidence to suggest that a red link has been incorrectly recorded in the MID or that data were processed in the MID, the CIR or SIS in breach of this Regulation, that authority or agency shall check the relevant data stored in the CIR and SIS and shall:

(a) where the link relates to one of the SIS alerts referred to in Article 29(2), immediately inform the relevant SIRENE Bureau of the Member State that created the SIS alert;.

(b) in all other cases, either rectify or erase the link from the MID immediately.

If a SIRENE Bureau is contacted pursuant to point (a) of the first subparagraph, it shall verify the evidence provided by the Member State authority or the Union agency and where relevant rectify or erase the link from the MID immediately.

The Member State authority obtaining the evidence shall inform the Member State authority responsible for the manual verification of different identities without delay of any relevant rectification or erasure of a red link.

Article 33

White link

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

(a) the linked data share the same biometric data and the same or similar identity data;

(b) the linked data share the same or similar identity data, the same travel document data, and at least one of the EU information systems does not have biometric data on the person concerned;

(c) the linked data shares the same biometric data, the same travel document data and similar identity data;

(d) the linked data share the same biometric data but have similar or different identity data and the authority responsible for the manual verification of different identities has concluded that linked data refer to the same person in a justified manner.

2. Where the CIR or SIS are queried and where a white link exists between data in two or more of the EU information systems, the MID shall indicate that the identity data of the linked data correspond to the same person. The queried EU information systems shall reply indicating, where relevant, all the linked data on the person, thereby triggering a match against the data that are linked by the white link, if the authority launching the query has access to the linked data under Union or national law.

3. Where a white link is created between data in the EES, VIS, ETIAS, Eurodac or ECRIS-TCN, the individual file stored in the CIR shall be updated in accordance with Article 19(2).

4. Without prejudice to the provisions related to the handling of alerts in SIS contained to in Regulations (EU) 2018/1860, (EU) 2018/1861 and (EU) 2018/1862, and without prejudice to limitations necessary to protect security and public order, prevent crime and guarantee that no national investigation will be jeopardised, where a white link is created following a manual verification of different identities, the authority responsible for the manual verification of different identities shall inform the person concerned of the presence of similar or different identity data and shall provide the person with the single identification number referred to in Article 34(c) of this Regulation, a reference to the authority responsible for the manual verification of different identities referred to in Article 34(d) of this Regulation and the website address of the web portal established in accordance with Article 49 of this Regulation.

5. If a Member State authority has evidence to suggest that a white link has been incorrectly recorded in the MID, that a white link is out of date or that data were processed in the MID or the EU information systems 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 of different identities without delay.

6. The information referred to in paragraph 4 shall be in writing by means of a standard form by the authority responsible for the manual verification of different identities. The Commission shall determine the content and presentation of that form by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 70(2).

Article 34

Identity confirmation file

The identity confirmation file shall contain the following data:

(a) the links referred to in Articles 30 to 33;

(b) a reference to the EU information systems in which the linked data are held;

(c) a single identification number allowing retrieval of the linked data from the corresponding EU information systems;

(d) the authority responsible for the manual verification of different identities;

(e) the date of creation of the link or of any update to it.

Article 35

Data retention in the multiple-identity detector

The identity confirmation files and the data in them, including the links, shall be stored in the MID only for as long as the linked data are stored in two or more EU information systems. They shall be erased from the MID in an automated manner.

Article 36

Keeping of logs

1. eu-LISA shall keep logs of all data processing operations in the MID. Those logs shall include the following:

(a) the Member State launching the query;

(b) the purpose of user's access;

(c) the date and time of the query;

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

(e) the reference to the linked data;

(f) the history of the identity confirmation file.

2. Each Member State shall keep logs of queries that its authorities and the staff of those authorities duly authorised to use the MID make. Each Union agency shall keep logs of queries that its duly authorised staff make.

3. The logs referred to in paragraphs 1 and 2 may be used only for data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, and for ensuring data security and integrity. Those logs shall be protected by appropriate measures against unauthorised access and erased one year after their creation. If, however, they are required for monitoring procedures that have already begun, they shall be erased once the monitoring procedures no longer require the logs.

CHAPTER VI

Measures supporting interoperability

Article 37

Data quality

1. Without prejudice to Member States' responsibilities with regard to the quality of data entered into the systems, eu-LISA shall establish automated data quality control mechanisms and procedures on the data stored in the SIS, Eurodac, ECRIS-TCN, the shared BMS and the CIR.

2. eu-LISA shall implement mechanisms for evaluating the accuracy of the shared BMS, common data quality indicators and the minimum quality standards for storage of data in the SIS, Eurodac, ECRIS-TCN, the shared BMS and the CIR.

Only data fulfilling the minimum quality standards may be entered in the SIS, Eurodac, ECRIS-TCN, 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. eu-LISA shall also provide that report to the European Parliament and to the Council upon request. No reports provided under this paragraph shall contain any personal data.

4. The details of the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum quality standards for storage of data in the SIS, Eurodac, ECRIS-TCN, the shared BMS and the CIR, 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 70(2).

5. One year after the establishment of the automated data quality control mechanisms and procedures, common data quality indicators and the minimum data quality standards, and every year thereafter, the Commission shall evaluate Member States' implementation of data quality and 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, in particular, data quality issues deriving from erroneous data in EU information systems. The Member States shall regularly report to the Commission 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, to the European Data Protection Board and to the European Union Agency for Fundamental Rights established by Council Regulation (EC) No 168/2007 ([37]).

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 or organisations in the field of Justice and Home Affairs.

([37]) 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).

2. The UMF standard shall be used in the development of Eurodac, ECRIS-TCN, the ESP, the CIR, the MID and, if appropriate, in the development by eu-LISA or by any other Union agency of new information exchange models and information systems in the area of Justice and Home Affairs.

3. The Commission shall adopt an implementing act to lay down and develop the UMF standard referred to in paragraph 1 of this Article. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 70(2).

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 the SIS, Eurodac and ECRIS-TCN, in accordance with the respective legal instruments governing those systems, and to provide cross-system statistical data and analytical reporting for policy, operational and data quality purposes.

2. eu-LISA shall establish, implement and host in its technical sites the CRRS containing the data and statistics referred to in Article 74 of Regulation (EU) 2018/1862 and Article 32 of Regulation (EU) 2019/816 logically separated by EU information system. Access to the CRRS shall be granted by means of controlled, secured access and specific user profiles, solely for the purpose of reporting and statistics, to the authorities referred to in Article 74 of Regulation (EU) 2018/1862 and Article 32 of Regulation (EU) 2019/816.

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

The data contained in CRRS shall not allow for the identification of individuals.

4. The CRRS shall be composed of:

(a) the tools necessary for anonymising data;

(b) a central infrastructure, consisting of a data repository of anonymous data;

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

5. The Commission shall adopt a delegated act in accordance with Article 69 laying down detailed rules on the operation of the CRRS, including specific safeguards for the processing of personal data under paragraphs 2 and 3 of this Article and security rules applicable to the repository.

CHAPTER VII

Data protection

Article 40

Data controller

1. In relation to the processing of data in the shared BMS, the Member State authorities that are controllers for Eurodac, SIS and ECRIS-TCN respectively, shall be controllers in accordance with point (7) of Article 4 of Regulation (EU) 2016/679 or point (8) of Article 3 of Directive (EU) 2016/680 in relation to the biometric templates obtained from the data referred to in Article 13 of this Regulation that they enter into the underlying 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 CIR, the Member State authorities that are controllers for Eurodac and ECRIS-TCN respectively, shall be controllers in accordance with point (7) of Article 4 of Regulation (EU) 2016/679 or point (8) of Article 3 of Directive (EU) 2016/680 in relation to data referred to in Article 18 of this Regulation that they enter into the underlying systems and shall have responsibility for the processing of those personal data in the CIR.

3. In relation to the processing of data in the MID:

(a) the European Border and Coast Guard Agency shall be a data controller within the meaning of point (8) of Article 3 of Regulation (EU) 2018/1725 in relation to the processing of personal data by the ETIAS Central Unit;

(b) the Member State authorities adding or modifying the data in the identity confirmation file shall be controllers in accordance with point (7) of Article 4 of Regulation (EU) 2016/679 or point (8) of Article 3 of Directive (EU) 2016/680 and shall have responsibility for the processing of the personal data in the MID.

4. For the purposes of data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, the data controllers shall have access to the logs referred to in Articles 10, 16, 24 and 36 for self-monitoring as referred to in Article 44.

Article 41

Data processor

In relation to the processing of personal data in the shared BMS, the CIR and the MID, eu-LISA shall be the data processor within the meaning of point (12)(a) of Article 3 of Regulation (EU) 2018/1725.

Article 42

Security of processing

1. eu-LISA, the ETIAS Central Unit, Europol and the Member State authorities shall ensure the security of the processing of personal data that takes place pursuant to this Regulation. eu-LISA, the ETIAS Central Unit, Europol and the Member State authorities shall cooperate on security-related tasks.

2. Without prejudice to Article 33 of Regulation (EU) 2018/1725, eu-LISA shall take the necessary measures to ensure the security of the interoperability components and their related communication infrastructure.

3. In particular, eu-LISA shall adopt the necessary measures, including a security plan, a business continuity plan and a disaster recovery plan, in order to:

(a) physically protect data, including by making contingency plans for the protection of critical infrastructure;

(b) deny unauthorised persons access to data-processing equipment and installations;

(c) prevent the unauthorised reading, copying, modification or removal of data media;

(d) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of recorded personal data;

(e) prevent the unauthorised processing of data and any unauthorised copying, modification or deletion of data;

(f) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment;

(g) ensure that persons authorised to access the interoperability components have access only to the data covered by their access authorisation, by means of individual user identities and confidential access modes only;

(h) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment;

(i) ensure that it is possible to verify and establish what data have been processed in the interoperability components, when, by whom and for what purpose;

(j) prevent the unauthorised reading, copying, modification or deletion of personal data during the transmission of personal data to or from the interoperability components or during the transport of data media, in particular by means of appropriate encryption techniques;

(k) ensure that, in the event of interruption, installed systems can be restored to normal operation;

(l) ensure reliability by making sure that any faults in the functioning of the interoperability components are properly reported;

(m) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Regulation and to assess those security measures in the light of new technological developments.

4. Member States, Europol and the ETIAS Central Unit shall take measures equivalent to those referred to in paragraph 3 as regards security in respect of the processing of personal data by the authorities having a right to access any of the interoperability components.

Article 43

Security incidents

1. Any event that has or may have an impact on the security of the interoperability components and may cause damage to or loss of data stored in them shall be considered to be a security incident, in particular where unauthorised access to data may have occurred or where the availability, integrity and confidentiality of data has or may have been compromised.

2. Security incidents shall be managed so as to ensure a quick, effective and proper response.

3. Without prejudice to the notification and communication of a personal data breach pursuant to Article 33 of Regulation (EU) 2016/679, Article 30 of Directive (EU) 2016/680, or both, Member States shall notify the Commission, eu-LISA, the competent supervisory authorities and the European Data Protection Supervisor of any security incidents without delay.

Without prejudice to Articles 34 and 35 of Regulation (EU) 2018/1725 and Article 34 of Regulation (EU) 2016/794, the ETIAS Central Unit and Europol shall notify the Commission, eu-LISA and the European Data Protection Supervisor of any security incidents without delay.

In the event of a security incident in relation to the central infrastructure of the interoperability components, eu-LISA shall notify the Commission and the European Data Protection Supervisor without delay.

4. Information regarding a security incident that has or may have an impact on the operation of the interoperability components or on the availability, integrity and confidentiality of the data shall be provided to the Member States, the ETIAS Central Unit and Europol without delay and reported in compliance with the incident management plan to be provided by eu-LISA.

5. The Member States concerned, the ETIAS Central Unit, Europol and eu-LISA shall cooperate in the event of a security incident. The Commission shall lay down the specifications of this cooperation procedure by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 70(2).

Article 44

Self-monitoring

Member States and the relevant Union agencies shall ensure that each authority entitled to access the interoperability components takes the measures necessary to monitor its compliance with this Regulation and cooperates, where necessary, with the supervisory authority.

The data controllers referred to in Article 40 shall take the necessary measures to monitor the compliance of data processing pursuant to this Regulation, including through frequent verification of the logs referred to in Articles 10, 16, 24 and 36, and cooperate, where necessary, with the supervisory authorities and with the European Data Protection Supervisor.

Article 45

Penalties

Member States shall ensure that any misuse of data, processing of data or exchange of data contrary to this Regulation is punishable in accordance with national law. The penalties provided shall be effective, proportionate and dissuasive.

Article 46

Liability

1. Without prejudice to the right to compensation from, and liability of the controller or processor under Regulation (EU) 2016/679, Directive (EU) 2016/680 and Regulation (EU) 2018/1725:

(a) any person or Member State that has suffered material or non-material damage as a result of an unlawful personal data processing operation or any other act incompatible with this Regulation by a Member State shall be entitled to receive compensation from that Member State;

(b) any person or Member State that has suffered material or non-material damage as a result of any act by Europol, the European Border and Coast Guard Agency or eu-LISA incompatible with this Regulation shall be entitled to receive compensation from the agency in question.

The Member State concerned, Europol, the European Border and Coast Guard Agency or eu-LISA shall be exempted from their liability under the first subparagraph, in whole or in part, if they prove that they are not responsible for the event which gave rise to the damage.

2. If any failure of a Member State to comply with its obligations under this Regulation causes damage to the interoperability components, that Member State shall be liable for such damage, unless and insofar as eu-LISA or another Member State bound by this Regulation failed to take reasonable measures to prevent the damage from occurring or to minimise its impact.

3. Claims for compensation against a Member State for the damage referred to in paragraphs 1 and 2 shall be governed by the national law of the defendant Member State. Claims for compensation against the controller or eu-LISA for the damage referred to in paragraphs 1 and 2 shall be subject to the conditions provided for in the Treaties.

Article 47

Right to information

1. The authority collecting the personal data to be stored in the shared BMS, the CIR or the MID shall provide the persons whose data are collected with the information required under Articles 13 and 14 of Regulation (EU) 2016/679, Articles 12 and 13 of Directive (EU) 2016/680 and Articles 15 and 16 of Regulation (EU) 2018/1725. The authority shall provide the information at the time that such data are collected.

2. All information shall be made available, using clear and plain language, in a linguistic version the person concerned understands or is reasonably expected to understand. This shall include providing information in a manner which is appropriate to the age of the data subjects who are minors.

3. The rules on the right to information contained in the applicable Union data protection rules shall apply to the personal data recorded in ECRIS-TCN and processed for the purposes of this Regulation.

Article 48

Right of access to, rectification and erasure of personal data stored in the MID and restriction of processing thereof

1. In order to exercise their rights under Articles 15 to 18 of Regulation (EU) 2016/679, Articles 17 to 20 of Regulation (EU) 2018/1725 and Articles 14, 15 and 16 of Directive (EU) 2016/680, any person shall have the right to address himself or herself to the competent authority of any Member State, which shall examine and reply to the request.

2. The Member State which examines such a request shall reply without undue delay and in any event within 45 days of receipt of the request. That period may be extended by 15 further days where necessary, taking into account the complexity and number of the requests. The Member State which examines the request shall inform the data subject of any such extension within 45 days of receipt of the request, together with the reasons for the delay. Member States may decide that replies are to be given by central offices.

3. If a request for rectification or erasure of personal data is made to a Member State other than the Member State responsible for the manual verification of different identities, the Member State to which the request has been made shall contact the authorities of the Member State responsible for the manual verification of different identities within seven days. The Member State responsible for the manual verification of different identities shall check the accuracy of the data and the lawfulness of the data processing without undue delay and in any event within 30 days of such contact. That period may be extended by 15 further days where necessary, taking into account the complexity and number of the requests. The Member State responsible for the manual verification of different identities shall inform the Member State which contacted it of any such extension together with the reasons for the delay. The person concerned shall be informed by the Member State which contacted the authority of the Member State responsible for the manual verification of different identities about the further procedure.

4. If a request for rectification or erasure of personal data is made to a Member State where the ETIAS Central Unit was responsible for the manual verification of different identities, the Member State to which the request has been made shall contact the ETIAS Central Unit within seven days to ask for its opinion. The ETIAS Central Unit shall give its opinion without undue delay and in any event within 30 days of being contacted. That period may be extended by 15 further days where necessary, taking into account the complexity and number of the requests. The person concerned shall be informed by the Member State which contacted the ETIAS Central Unit about the further procedure.

5. Where, following an examination, it is found that the data stored in the MID are inaccurate or have been recorded unlawfully, the Member State responsible for the manual verification of different identities or, where there was no Member State responsible for the manual verification of different identities or where the ETIAS Central Unit was responsible for the manual verification of different identities, the Member State to which the request has been made shall rectify or erase those data without any undue delay. The person concerned shall be informed in writing that his or her data have been rectified or erased.

6. Where data stored in the MID are amended by a Member State during their retention period, that Member State shall carry out the processing laid down in Article 27 and, where relevant, Article 29 to determine whether the amended data are to be linked. Where the processing does not report any match, that Member State shall erase the data from the identity confirmation file. Where the automated processing reports one or several matches, that Member State shall create or update the relevant link in accordance with the relevant provisions of this Regulation.

7. Where the Member State responsible for the manual verification of different identities or, where applicable, the Member State to which the request has been made does not agree that data stored in the MID are inaccurate or have been recorded unlawfully, that Member State shall adopt an administrative decision explaining in writing to the person concerned without delay why it is not prepared to rectify or erase data relating to him or her.

8. The decision referred to in paragraph 7 shall also provide the person concerned with information explaining the possibility to challenge the decision taken in respect of the request for access to, rectification, erasure or restriction of processing of personal data and, where relevant, information on how to bring an action or a complaint before the competent authorities or courts, and any assistance, including from the supervisory authorities.

9. Any request for access to, rectification, erasure or restriction of processing of personal data shall contain the necessary information to identify the person concerned. That information shall be used exclusively to enable the exercise of the rights referred to in this Article and shall be erased immediately afterwards.

10. The Member State responsible for the manual verification of different identities or, where applicable, the Member State to which the request has been made shall keep a written record that a request for access to, rectification, erasure or restriction of processing of personal data was made and how it was addressed, and shall make that record available to supervisory authorities without delay.

11. This Article is without prejudice to any limitations and restrictions to the rights set out in this Article pursuant to Regulation (EU) 2016/679 and Directive (EU) 2016/680.

Article 49

Web portal

1. A web portal is established for the purpose of facilitating the exercise of the rights of access to, rectification, erasure or restriction of processing of personal data.

2. The web portal shall contain information on the rights and procedures referred to in Articles 47 and 48 and a user interface enabling persons whose data are processed in the MID and who have been informed of the presence of a red link in accordance with Article 32(4) to receive the contact information of the competent authority of the Member State responsible for the manual verification of different identities.

3. In order to obtain the contact information of the competent authority of the Member State responsible for the manual verification of different identities, the person whose data are processed in the MID should enter the reference to the authority responsible for the manual verification of different identities referred to in Article 34(d). The web portal shall use this reference in order to retrieve the contact information of the competent authority of the Member State responsible for the manual verification of different identities. The web portal shall also include a template e-mail to facilitate communication between the portal user and the competent authority of the Member State responsible for the manual verification of different identities. Such e-mail shall include a field for the single identification number referred to in Article 34(c) in order to allow the competent authority of the Member State responsible for the manual verification of different identities to identify the data concerned.

4. Member States shall provide eu-LISA with the contact details of all authorities that are competent to examine and reply to any request referred to in Articles 47 and 48 and shall regularly review whether those contact details are up to date.

5. eu-LISA shall develop the web portal and ensure its technical management.

6. The Commission shall adopt a delegated act in accordance with Article 69 laying down detailed rules on the operation of the web portal, including the user interface, the languages in which the web portal shall be available and the template e-mail.

Article 50

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

Without prejudice to Article 31 of Regulation (EC) No 767/2008, Articles 25 and 26 of Regulation (EU) 2016/794, Article 41 of Regulation (EU) 2017/2226, Article 65 of Regulation (EU) 2018/1240 and the querying of Interpol databases through the ESP in accordance with Article 9(5) of this Regulation which comply with the provisions of Chapter V of Regulation (EU) 2018/1725 and Chapter V of Regulation (EU) 2016/679, personal data stored in, processed 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.

Article 51

Supervision by the supervisory authorities

1. Each Member State shall ensure that the supervisory authorities independently monitor the lawfulness of the processing of personal data under this Regulation by the Member State concerned, including their transmission to and from the interoperability components.

2. Each Member State shall ensure that the national laws, regulations and administrative provisions adopted pursuant to Directive (EU) 2016/680 are also applicable, where relevant, to access to the interoperability components by police authorities and designated authorities, including in relation to the rights of the persons whose data are so accessed.

3. The supervisory authorities shall ensure that an audit of the personal data processing operations by the responsible national authorities for the purposes of this Regulation is carried out in accordance with relevant international auditing standards at least every four years.

The supervisory authorities shall publish annually the number of requests for rectification, erasure or restriction of processing of personal data, the action subsequently taken and the number of rectifications, erasures and restrictions of processing made in response to requests by the persons concerned.

4. Member States shall ensure that their supervisory authorities have sufficient resources and expertise to fulfil the tasks entrusted to them under this Regulation.

5. Member States shall supply any information requested by a supervisory authority referred to in Article 51(1) of Regulation (EU) 2016/679 and shall, in particular, provide it with information on the activities carried out in accordance with their responsibilities under this Regulation. Member States shall grant the supervisory authorities referred to in Article 51(1) of Regulation (EU) 2016/679 access to their logs referred to in Articles 10, 16, 24 and 36 of this Regulation, to the justifications referred to in Article 22(2) of this Regulation and allow them to access all their premises used for interoperability purposes at all times.

Article 52

Audits by the European Data Protection Supervisor

The European Data Protection Supervisor shall ensure that an audit of personal data processing operations by eu-LISA, the ETIAS Central Unit and Europol for the purposes of this Regulation is carried out in accordance with relevant international auditing standards at least every four years. A report of that audit shall be sent to the European Parliament, to the Council, to eu-LISA, to the Commission, to the Member States and to the Union agency concerned. eu-LISA, the ETIAS Central Unit and Europol shall be given an opportunity to make comments before the reports are adopted.

eu-LISA, the ETIAS Central Unit and Europol shall supply information requested by the European Data Protection Supervisor to it, grant the European Data Protection Supervisor access to all the documents it requests and to their logs referred to in Articles 10, 16, 24 and 36 and allow the European Data Protection Supervisor access to all their premises at any time.

Article 53

Cooperation between supervisory authorities and the European Data Protection Supervisor

1. The supervisory authorities and the European Data Protection Supervisor shall, each acting within the scope of their respective competences, cooperate actively within the framework of their respective responsibilities and ensure coordinated supervision of the use of the interoperability components and the application of other provisions of this Regulation, in particular if the European Data Protection Supervisor or a supervisory authority finds major discrepancies between practices of Member States or finds potentially unlawful transfers using the communication channels of the interoperability components.

2. In the cases referred to in paragraph 1 of this Article, coordinated supervision shall be ensured in accordance with Article 62 of Regulation (EU) 2018/1725.

3. The European Data Protection Board shall send a joint report of its activities under this Article to the European Parliament, to the Council, to the Commission, to Europol, to the European Border and Coast Guard Agency and to eu-LISA by 12 June 2021 and every two years thereafter. That report shall include a chapter on each Member State prepared by the supervisory authority of the Member State concerned.

CHAPTER VIII

Responsibilities

Article 54

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 performance referred to in Article 55(1).

3. eu-LISA shall be responsible for the development of the interoperability components and for any adaptations required for establishing interoperability between the central systems of the EES, VIS, ETIAS, SIS, Eurodac, ECRIS-TCN, and the ESP, the shared BMS, the CIR, the MID and the CRRS.

Without prejudice to Article 62, eu-LISA shall not have access to any of the personal data processed through the ESP, the shared BMS, the CIR or the MID.

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 SIS, Eurodac or ECRIS-TCN 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 (7), 37(4), 38(3), 39(5) 43(5) and 74(10).

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

4. During the design and development phase, a Programme Management Board composed of a maximum of 10 members shall be established. It shall be composed of seven members appointed by eu-LISA's Management Board from among its members or its alternates, the chair of the Interoperability Advisory Group referred to in Article 71, a member representing eu-LISA appointed by its Executive Director, and one member appointed by the Commission. The members appointed by eu-LISA's Management Board shall be elected only from those Member States that are fully bound under Union law by the legal instruments governing the development, establishment, operation and use of all the EU information systems and which will participate in the interoperability components.

5. The Programme Management Board shall meet regularly and at least three times per quarter. It shall ensure the adequate management of the design and development phase of the interoperability components.

Every month, the Programme Management Board shall submit written reports on progress of the project to eu-LISA's Management Board. The Programme Management Board shall have no decision-making power, nor any mandate to represent the members of eu-LISA's Management Board.

6. eu-LISA's Management Board shall establish the rules of procedure of the Programme Management Board, which shall include in particular rules on:

(a) chairmanship;

(b) meeting venues;

(c) preparation of meetings;

(d) admission of experts to the meetings;

(e) communication plans ensuring that non-participating Members of the Management Board are kept fully informed.

The chairmanship shall be held by a Member State that is fully bound under Union law by the legal instruments governing the development, establishment, operation and use of all the EU information systems and which will participate in the interoperability components.

All travel and subsistence expenses incurred by the members of the Programme Management Board shall be paid by eu-LISA, and Article 10 of the eu-LISA Rules of Procedure shall apply *mutatis mutandis*. eu-LISA shall provide the Programme Management Board with a secretariat.

The Interoperability Advisory Group referred to in Article 71 shall meet regularly until the start of operations of the interoperability components. It shall report after each meeting to the Programme Management Board. It shall provide the technical expertise to support the tasks of the Programme Management Board and shall follow up on the state of preparation of the Member States.

Article 55

Responsibilities of eu-LISA following the entry into operations

1. Following the entry into operations of each interoperability component, eu-LISA shall be responsible for the technical management of the central infrastructure of the interoperability components, including their maintenance and technological developments. In cooperation with the Member States, it shall ensure that the best available technology is used, subject to a cost-benefit analysis. eu-LISA shall also be responsible for the technical management of the communication infrastructure referred to in Articles 6, 12, 17, 25 and 39.

Technical management of the interoperability components shall consist of all the tasks and technical solutions necessary to keep the interoperability components functioning and providing uninterrupted services to the Member States and to the Union agencies 24 hours a day, 7 days a week in accordance with this Regulation. It shall include the maintenance work and technical developments necessary to ensure that the components function at a satisfactory level of technical quality, in particular as regards the response time for interrogation of the central infrastructures in accordance with the technical specifications.

All interoperability components shall be developed and managed in such a way as to ensure fast, seamless, efficient and controlled access, full, uninterrupted availability of the components and of the data stored in the MID, the shared BMS and the CIR, and a response time in line with the operational needs of the Member States' authorities and Union agencies.

2. Without prejudice to Article 17 of the Staff Regulations of Officials of the European Union, eu-LISA shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality to its staff required to work with data stored in the interoperability components. This obligation shall also apply after such staff leave office or employment or after the termination of their activities.

Without prejudice to Article 62, eu-LISA shall not have access to any of the personal data processed through the ESP, the shared BMS, the CIR and the MID.

3. eu-LISA shall develop and maintain a mechanism and procedures for carrying out quality checks on the data stored in the shared BMS and the CIR in accordance with Article 37.

4. eu-LISA shall also perform tasks related to providing training on the technical use of the interoperability components.

Article 56

Responsibilities of Member States

1. Each Member State shall be responsible for:

(a) the connection to the communication infrastructure of the ESP and the CIR;

(b) the integration of the existing national systems and infrastructures with the ESP, the CIR and the MID;

(c) the organisation, management, operation and maintenance of its existing national infrastructure and of its connection to the interoperability components;

(d) the management of, and arrangements for, access by the duly authorised staff of the competent national authorities to the ESP, the CIR and the MID in accordance with this Regulation and the creation and regular update of a list of those staff and their profiles;

(e) the adoption of the legislative measures referred to in Article 20(5) and (6) in order to access the CIR for identification purposes;

(f) the manual verification of different identities referred to in Article 29;

(g) compliance with the data quality requirements established under Union law;

(h) compliance with the rules of each EU information system regarding the security and integrity of personal data;

(i) remedying any deficiencies identified in the Commission's evaluation report concerning data quality referred to in Article 37(5).

2. Each Member State shall connect their designated authorities to the CIR.

Article 57

Responsibilities of Europol

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

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

Article 58

Responsibilities of the ETIAS Central Unit

The ETIAS Central Unit shall be responsible for:

(a) the manual verification of different identities in accordance with Article 29;

(b) carrying out multiple-identity detection between the data stored in the EES, VIS, Eurodac and SIS, as referred to in Article 65.

CHAPTER IX

Amendments to other Union instruments

Article 59

Amendments to Regulation (EU) 2018/1726

Regulation (EU) 2018/1726 is amended as follows:

(1) Article 12 is replaced by the following:

'*Article 12*

Data quality

1. Without prejudice to Member States' responsibilities with regard to the data entered into the systems under the Agency's operational responsibility, the Agency, closely involving its Advisory Groups, shall establish for all systems under the Agency's operational responsibility automated data quality control mechanisms and procedures, common data quality indicators and the minimum quality standards to store data, in accordance with the relevant provisions of the legal instruments governing those information systems and of Article 37 of Regulations (EU) 2019/817 (*) and (EU) 2019/818 (**) of the European Parliament and of the Council.

2. The Agency shall establish a central repository containing only anonymised data for reporting and statistics in accordance with Article 39 of Regulations (EU) 2019/817 and (EU) 2019/818, subject to specific provisions in the legal instruments governing the development, establishment, operation and use of large-scale IT systems managed by the Agency.

(*) Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27).

(**) Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (OJ L 135, 22.5.2019, p. 85).';

(2) in Article 19, paragraph 1 is amended as follows:

(a) the following point is inserted:

'(eea) adopt reports on the state of play of the development of the interoperability components pursuant to Article 78(2) of Regulation (EU) 2019/817 and Article 74(2) of Regulation (EU) 2019/818;';

(b) point (ff) is replaced by the following:

'(ff) adopt reports on the technical functioning of SIS pursuant to Article 60(7) of Regulation (EU) 2018/1861 of the European Parliament and of the Council (*) and Article 74(8) of Regulation (EU) 2018/1862 of the European Parliament and of the Council (**), of the VIS pursuant to Article 50(3) of Regulation (EC) No 767/2008 and Article 17(3) of Decision 2008/633/JHA, of EES pursuant to Article 72(4) of Regulation (EU) 2017/2226, of ETIAS pursuant to Article 92(4) of Regulation (EU) 2018/1240, of the ECRIS-TCN and of the ECRIS reference implementation pursuant to Article 36(8) of Regulation (EU) 2019/816 of the European Parliament and of the Council (***) and of the interoperability components pursuant to Article 78(3) of Regulation (EU) 2019/817 and Article 74(3) of Regulation (EU) 2019/818;

(*) Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 (OJ L 312, 7.12.2018, p. 14).

(**) Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56).

(***) Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 (OJ L 135, 22.5.2019, p. 1).';

(c) point (hh) is replaced by the following:

'(hh) adopt formal comments on the European Data Protection Supervisor's reports on its audits pursuant to Article 56(2) of Regulation (EU) 2018/1861, Article 42(2) of Regulation (EC) No 767/2008, Article 31(2) of Regulation (EU) No 603/2013, Article 56(2) of Regulation (EU) 2017/2226, Article 67 of Regulation (EU) 2018/1240, Article 29(2) of Regulation (EU) 2019/816 and Article 52 of Regulations (EU) 2019/817 and (EU) 2019/818 and ensure appropriate follow-up of those audits;';

(d) point (mm) is replaced by the following:

'(mm) ensure annual publication of the list of competent authorities authorised to search directly the data contained in SIS pursuant to Article 41(8) of Regulation (EU) 2018/1861 and Article 56(7) of Regulation (EU) 2018/1862, together with the list of Offices of the national systems of SIS (N.SIS) and SIRENE Bureaux pursuant to Article 7(3) of Regulation (EU) 2018/1861 and Article 7(3) of Regulation (EU) 2018/1862 respectively as well as the list of competent authorities pursuant to Article 65(2) of Regulation (EU) 2017/2226, the list of competent authorities pursuant to Article 87(2) of Regulation (EU) 2018/1240, the list of central authorities pursuant to Article 34(2) of Regulation (EU) 2019/816 and the list of authorities pursuant to Article 71(1) of Regulation (EU) 2019/817 and Article 67(1) of Regulation (EU) 2019/818;';

(3) in Article 22, paragraph 4 is replaced by the following:

'4. Europol and Eurojust may attend the meetings of the Management Board as observers when a question concerning SIS II, in relation to the application of Decision 2007/533/JHA is on the agenda.

The European Border and Coast Guard Agency may attend the meetings of the Management Board as an observer when a question concerning SIS in relation to the application of Regulation (EU) 2016/1624 is on the agenda.

Europol may attend the meetings of the Management Board as an observer when a question concerning VIS, in relation to the application of Decision 2008/633/JHA or a question concerning Eurodac, in relation to the application of Regulation (EU) No 603/2013 is on the agenda.

Europol may attend the meetings of the Management Board as an observer when a question concerning EES in relation to the application of Regulation (EU) 2017/2226 is on the agenda or when a question concerning ETIAS in relation to Regulation (EU) 2018/1240 is on the agenda.

The European Border and Coast Guard Agency may attend the meetings of the Management Board as an observer when a question concerning ETIAS in relation with the application of Regulation (EU) 2018/1240 is on the agenda.

Eurojust, Europol and the European Public Prosecutor's Office may attend the meetings of the Management Board as observers when a question concerning Regulation (EU) 2019/816 is on the agenda.

Europol, Eurojust and the European Border and Coast Guard Agency may attend the meetings of the Management Board as observers when a question concerning Regulations (EU) 2019/817 and (EU) 2019/818 is on the agenda.

The Management Board may invite any other person whose opinion may be of interest to attend its meetings as an observer.';

(4) in Article 24(3), point (p) is replaced by the following:

'(p) without prejudice to Article 17 of the Staff Regulations of Officials, establishing confidentiality requirements in order to comply with Article 17 of Regulation (EC) No 1987/2006, Article 17 of Decision 2007/533/JHA, Article 26(9) of Regulation (EC) No 767/2008, Article 4(4) of Regulation (EU) No 603/2013, Article 37(4) of Regulation (EU) 2017/2226, Article 74(2) of Regulation (EU) 2018/1240, Article 11(16) of Regulation (EU) 2019/816 and Article 55(2) of Regulations (EU) 2019/817 and (EU) 2019/818;';

(5) Article 27 is amended as follows:

(a) in paragraph 1, the following point is inserted:

'(da) Interoperability Advisory Group;';

(b) paragraph 3 is replaced by the following:

'3. Europol, Eurojust and the European Border and Coast Guard Agency may each appoint a representative to the SIS II Advisory Group.

Europol may also appoint a representative to the VIS and Eurodac and EES-ETIAS Advisory Groups.

The European Border and Coast Guard Agency may also appoint a representative to the EES-ETIAS Advisory Group.

Eurojust, Europol, and the European Public Prosecutors Office may each appoint a representative to the ECRIS-TCN Advisory Group.

Europol, Eurojust and the European Border and Coast Guard Agency may each appoint a representative to the Interoperability Advisory Group.'.

Article 60

Amendments to Regulation (EU) 2018/1862

Regulation (EU) 2018/1862 is amended as follows:

(1) in Article 3, the following points are added:

'(18) 'ESP' means the European search portal established by Article 6(1) of Regulation (EU) 2019/818 of the European Parliament and of the Council (*);

(19) 'shared BMS' means the shared biometric matching service established by Article 12(1) of Regulation (EU) 2019/818;

(20) 'CIR' means the common identity repository established by Article 17(1) of Regulation (EU) 2019/818;

(21) 'MID' means the multiple-identity detector established by Article 25(1) of Regulation (EU) 2019/818;

(*) Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (OJ L 135, 22.5.2019, p. 85).'.

(2) Article 4 is amended as follows:

(a) in paragraph 1, points (b) and (c) are replaced by the following:

'(b) a national system (N.SIS) in each of the Member States, consisting of the national data systems which communicate with Central SIS, including at least one national or shared backup N.SIS;

(c) a communication infrastructure between CS-SIS, backup CS-SIS and NI-SIS ('the Communication Infrastructure') that provides an encrypted virtual network dedicated to SIS data and the exchange of data between SIRENE Bureaux, as referred to in Article 7(2); and

(d) a secure communication infrastructure between CS-SIS and the central infrastructures of the ESP, the shared BMS and the MID.';

(b) the following paragraphs are added:

'8. Without prejudice to paragraphs 1 to 5, SIS data on persons and identity documents may also be searched via the ESP.

9. Without prejudice to paragraphs 1 to 5, SIS data on persons and identity documents may also be transmitted via the secure communication infrastructure referred to in point (d) of paragraph 1. These transmissions shall be limited to the extent that the data are required for the purposes of Regulation (EU) 2019/818.';

(3) in Article 7, the following paragraph is inserted:

'2a. The SIRENE Bureaux shall also ensure the manual verification of different identities in accordance with Article 29 of Regulation (EU) 2019/818. To the extent necessary to carry out this task, the SIRENE Bureaux shall have access to the data stored in the CIR and the MID for the purposes laid down in Articles 21 and 26 of Regulation (EU) 2019/818';

(4) in Article 12(1), the following subparagraph is added:

'Member States shall ensure that every access to personal data via the ESP is also logged for the purposes of checking whether the search was lawful, monitoring the lawfulness of data processing, self-monitoring, and data integrity and security.';

(5) in Article 44(1), the following point is added:

'(f) verifying different identities and combating identity fraud in accordance with Chapter V of Regulation (EU) 2019/818'.

(6) In Article 74, paragraph 7 is replaced by the following:

'7. For the purpose of Article 15(4) and of paragraphs 3, 4 and 6 of this Article, eu-LISA shall store data referred to in Article 15(4) and in paragraph 3 of this Article which shall not allow for the identification of individuals in the central repository for reporting and statistics referred to in Article 39 of Regulation (EU) 2019/818.

eu-LISA shall allow the Commission and the bodies referred to in paragraph 6 of this Article to obtain bespoke reports and statistics. Upon request, eu-LISA shall grant access to the central repository for reporting and statistics in accordance with Article 39 of Regulation (EU) 2019/818 to Member States, the Commission, Europol, and the European Border and Coast Guard Agency.'.

Article 61

Amendments to Regulation (EU) 2019/816

Regulation (EU) 2019/816 is amended as follows:

(1) in Article 1, the following point is added:

'(c) the conditions under which ECRIS-TCN contributes to facilitating and assisting in the correct identification of persons registered in ECRIS-TCN under the conditions and for the purposes of Article 20 of Regulation (EU) 2019/818 of the European Parliament and of the Council (*), by storing identity data, travel document data and biometric data in the CIR.

(*) Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (OJ L 135, 22.5.2019, p. 85).';

(2) Article 2 is replaced by the following:

'*Article 2*

Scope

This Regulation applies to the processing of identity information of third-country nationals who have been subject to convictions in the Member States for the purpose of identifying the Member States where such convictions were handed down. With the exception of point (b)(ii) of Article 5(1), the provisions of this Regulation that apply to third-country nationals also apply to citizens of the Union who also hold the nationality of a third country and who have been subject to convictions in the Member States. This Regulation also facilitates and assists in the correct identification of persons in accordance with this Regulation and with Regulation (EU) 2019/818.';

(3) Article 3 is amended as follows:

(a) point (8) is deleted;

(b) the following points are added:

'(19) 'CIR' means the common identity repository established by Article 17(1) of Regulation (EU) 2019/818;

(20) 'ECRIS-TCN data' means all data stored in the central system and in the CIR in accordance with Article 5;

(21) 'ESP' means the European search portal established by Article 6(1) of Regulation (EU) 2019/818.';

(4) Article 4(1) is amended as follows:

(a) point (a) is replaced by the following:

'(a) a central system;';

(b) the following point is inserted:

'(aa) the CIR;';

(c) the following point is added:

'(e) a communication infrastructure between the central system and the central infrastructures of the ESP and the CIR;';

(5) Article 5 is amended as follows:

(a) in paragraph 1, the introductory part is replaced by the following:

'1. For each convicted third-country national, the central authority of the convicting Member State shall create a data record in ECRIS-TCN. The data record shall include:';

(b) the following paragraph is inserted:

'1a. The CIR shall contain the data referred to in point (b) of paragraph 1 and the following data of point (a) of paragraph 1: surname (family name), first names (given names), date of birth, place of birth (town and country), nationality or nationalities, gender, previous names, if applicable, where available pseudonyms or aliases, where available, the type and number of the person's travel documents, as well as the name of the issuing authority. The CIR may contain the data referred to in paragraph 3. The remaining ECRIS-TCN data shall be stored in the central system.';

(6) Article 8 is amended as follows:

(a) paragraph 1 is replaced by the following:

'1. Each data record shall be stored in the central system and the CIR for as long as the data related to the convictions of the person concerned are stored in the criminal records.';

(b) paragraph 2 is replaced by the following:

'2. Upon expiry of the retention period referred to in paragraph 1, the central authority of the convicting Member State shall erase the data record, including any fingerprint data or facial images, from the central system and the CIR. The erasure shall be done automatically, where possible, and in any event no later than one month after the expiry of the retention period.';

(7) Article 9 is amended as follows:

(a) in paragraph 1, the word 'ECRIS-TCN' is replaced by the words 'the central system and the CIR';

(b) in paragraphs (2), (3) and (4), the words 'central system' are replaced by the words 'the central system and the CIR';

(8) in Article 10(1), point (j) is deleted;

(9) in Article 12(2), the words 'central system' are replaced by the words 'the central system and the CIR';

(10) in Article 13(2), the words 'central system' are replaced by the words 'the central system, the CIR';

(11) in Article 23(2), the words 'central system' are replaced by the words 'the central system and the CIR';

(12) Article 24 is amended as follows:

(a) paragraph 1 is replaced by the following:

'1. The data entered into the central system and the CIR shall only be processed for the purposes of the identification of the Member States holding the criminal records information of third-country nationals. The data entered into the CIR shall also be processed in accordance with Regulation (EU) 2019/818 for facilitating and assisting in the correct identification of persons registered in the ECRIS-TCN in accordance with this Regulation.';

(b) the following paragraph is added:

'3. Without prejudice to paragraph 2, access for the purposes of consulting the data stored in the CIR shall also be reserved for the duly authorised staff of the national authorities of each Member State and for the duly authorised staff of the Union agencies that are competent for the purposes laid down in Articles 20 and 21 of Regulation (EU) 2019/818. Such access shall be limited according to the extent that the data are required for the performance of their tasks for those purposes, and proportionate to the objectives pursued.';

(13) in Article 32, paragraph 2 is replaced by the following:

'2. For the purpose of paragraph 1 of this Article, eu-LISA shall store the data referred to in that paragraph in the central repository for reporting and statistics referred to in Article 39 of Regulation (EU) 2019/818';

(14) in Article 33(1) the words 'central system' are replaced by the words 'central system, the CIR and';

(15) in Article 41, paragraph 2 is replaced by the following:

'2. For convictions handed down prior to the date of start of entry of data in accordance with Article 35(1), the central authorities shall create the individual data records in the central system and the CIR as follows:

(a) alphanumeric data to be entered into the central system and the CIR by the end of the period referred to in Article 35(2);

(b) fingerprint data to be entered into the CIR within two years after the start of operations in accordance with Article 35(4).'.

CHAPTER X

Final provisions

Article 62

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, solely for the purposes of reporting and statistics, the number of queries per ESP user profile.

It shall not be possible to identify individuals from the data.

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 CIR, solely for the purposes of reporting and statistics:

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

(b) nationality, gender 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.

It shall not be possible to identify individuals from the 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 MID, solely for the purposes of reporting and statistics:

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

(b) the number of each type of link and the EU information systems containing the linked data;

(c) the period of time for which a yellow and red link remained in the system.

It shall not be possible to identify individuals from the data.

4. The duly authorised staff of the European Border and Coast Guard Agency shall have access to consult the data referred to in paragraphs 1, 2 and 3 of this Article for the purpose of carrying out risk analyses and vulnerability assessments as referred to in Articles 11 and 13 of Regulation (EU) 2016/1624 of the European Parliament and of the Council ([38]).

5. The duly authorised staff of Europol shall have access to consult the data referred to in paragraphs 2 and 3 of this Article for the purpose of carrying out strategic, thematic and operational analyses as referred to in Article 18(2)(b) and (c) of Regulation (EU) 2016/794.

6. For the purpose of paragraphs 1, 2 and 3, eu-LISA shall store the data referred to in those paragraphs in the CRRS. It shall not be possible to identify individuals from the data included in the CRRS, but the data shall allow the authorities listed in paragraphs 1, 2 and 3 to obtain customisable reports and statistics to enhance the efficiency of border checks, to help authorities processing visa applications and to support evidence-based policy-making on migration and security in the Union.

7. Upon request, relevant information shall be made available by the Commission to the European Union Agency for Fundamental Rights in order to evaluate the impact of this Regulation on fundamental rights.

([38]) 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).

Article 63

Transitional period for the use of the European search portal

1. For a period of two years from the date the ESP commences operations, the obligations referred to in Article 7(2) and (4) shall not apply and the utilisation of the ESP shall be optional.

2. The Commission is empowered to adopt a delegated act in accordance with Article 69 in order to amend this Regulation by extending the period referred to in paragraph 1 of this Article once, by no longer than one year, when an assessment of the implementation of the ESP has shown that such an extension is necessary, especially in view of the impact that bringing the ESP into operation would have on the organisation and length of border checks.

Article 64

Transitional period applicable to the provisions on access to the common identity repository for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences

Article 22 shall apply from the date of the start of operations of the CIR referred to in Article 68(3).

Article 65

Transitional period for multiple-identity detection

1. For a period of one year following notification by eu-LISA of the completion of the test of the MID referred to in Article 68(4)(b) and before the start of operations of the MID, the ETIAS Central Unit shall be responsible for carrying out multiple-identity detection using the data stored in the EES, VIS, Eurodac and SIS. The multiple-identity detections shall be carried out using only biometric data.

2. Where the query reports one or several matches and the identity data in the linked files are the same or similar, a white link shall be created in accordance with Article 33.

Where the query reports one or several matches and the identity data in the linked files cannot be considered to be similar, a yellow link shall be created in accordance with Article 30 and the procedure referred to in Article 29 shall apply.

Where several matches are reported, a link shall be created between each piece of data triggering the match.

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

4. Where a link is created to an alert in SIS other than an alert created under Article 3 of Regulation (EU) 2018/1860, Articles 24 and 25 of Regulation (EU) 2018/1861, or Article 38 of Regulation (EU) 2018/1862, 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, in the cases referred to in paragraph 4 of this Article 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. The ETIAS Central Unit shall notify the Commission in accordance with Article 67(3) only once all yellow links have been manually verified and their status updated as either green, white or red links.

7. Member States shall assist the ETIAS Central Unit where necessary in carrying out multiple-identity detection under this Article.

8. The Commission is empowered to adopt a delegated act in accordance with Article 69 in order to amend this Regulation by extending the period referred to in paragraph 1 of this Article by six months, renewable twice by six months each time. Such an extension shall only be granted following an assessment of the estimated completion time for multiple-identity detection under this Article, which demonstrates that the multiple-identity detection cannot be completed before expiry of the period remaining either under paragraph 1 of this Article or any ongoing extension, for reasons independent of the ETIAS Central Unit, and that no corrective measures can be applied. The assessment shall be carried out no later than three months before the expiry of such period or ongoing extension.

Article 66

Costs

1. The costs incurred in connection with the establishment and operation of the ESP, the shared BMS, the CIR and the MID shall be borne by the general budget of the Union.

2. Costs incurred in connection with the integration of the existing national infrastructures and their connection to the national uniform interfaces as well as in connection with hosting the national uniform interfaces shall be borne by the general budget of the Union.

The following costs shall be excluded:

(a) Member States' project management office (meetings, missions, offices);

(b) hosting of national IT systems (space, implementation, electricity, cooling);

(c) operation of national IT systems (operators and support contracts);

(d) design, development, implementation, operation and maintenance of national communication networks.

3. Without prejudice to further funding for this purpose from other sources of the general budget of the European Union, an amount of EUR 32 077 000 shall be mobilised from the envelope of EUR 791 000 000 foreseen under Article 5(5)(b) of Regulation (EU) No 515/2014 to cover the costs of implementation of this Regulation, as foreseen under paragraphs 1 and 2 of this Article.

4. From the envelope referred to in paragraph 3, EUR 22 861 000 shall be allocated to eu-LISA, EUR 9 072 000 shall be allocated to Europol and EUR 144 000 shall be allocated to the European Union Agency for Law Enforcement Training (CEPOL) to support these agencies in performing their respective under this Regulation. Such funding shall be implemented under indirect management.

5. The costs incurred by the designated authorities shall be borne by the designating Member States respectively. The costs of connecting each designated authority to the CIR shall be borne by each Member State.

The costs incurred by Europol, including of connection to the CIR, shall be borne by Europol.

Article 67

Notifications

1. The Member States shall notify eu-LISA of the authorities referred to in Articles 7, 20, 21 and 26 that may use or have access to the ESP, the CIR and the MID respectively.

A consolidated list of those authorities shall be published in the *Official Journal of the European Union* within a period of three months from the date on which each interoperability component commenced operations in accordance with Article 68. Where there are amendments to the list, eu-LISA shall publish an updated consolidated list once a year.

2. eu-LISA shall notify the Commission of the successful completion of the tests referred to in Article 68(1)(b), (2)(b), (3)(b), (4)(b), (5)(b) and (6)(b).

3. The ETIAS Central Unit shall notify the Commission of the successful completion of the transitional period laid down in Article 65.

4. The Commission shall make the information notified pursuant to paragraph 1 available to the Member States and to the public, via a constantly updated public website.

Article 68

Start of operations

1. The Commission shall determine the date from which the ESP is to start operations by means of an implementing act once the following conditions have been met:

(a) the measures referred to in Articles 8(2), 9(7) and 43(5) have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the ESP, which it has conducted in cooperation with the Member States authorities and the Union agencies that may use the ESP;

(c) eu-LISA has validated the technical and legal arrangements to collect and transmit the data referred to in Article 8(1) and has notified them to the Commission.

The ESP shall only query the Interpol databases once the technical arrangements allow compliance with Article 9(5). Any impossibility of complying with Article 9(5) shall have the result that the ESP does not query the Interpol databases but shall not delay the start of operations of the ESP.

The Commission shall set the date referred to in the first subparagraph to be within 30 days from adoption of the implementing act.

2. The Commission shall determine the date from which the shared BMS is to start operations by means of an implementing act once the following conditions have been met:

(a) the measures referred to in Articles 13(5) and 43(5) have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the shared BMS, which it has conducted in cooperation with the Member States authorities;

(c) eu-LISA has validated the technical and legal arrangements to collect and transmit the data referred to in Article 13 and has notified them to the Commission;

(d) eu-LISA has declared the successful completion of the test referred to in paragraph 5(b).

The Commission shall set the date referred to in the first subparagraph to be within 30 days from adoption of the implementing act.

3. The Commission shall determine the date from which the CIR is to start operations by means of an implementing act once the following conditions have been met:

(a) the measures referred to in Articles 43(5) and 74(10) have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the CIR, which it has conducted in cooperation with the Member States authorities;

(c) eu-LISA has validated the technical and legal arrangements to collect and transmit the data referred to in Article 18 and has notified them to the Commission;

(d) eu-LISA has declared the successful completion of the test referred to in paragraph 5(b).

The Commission shall set the date referred to in the first subparagraph to be within 30 days from adoption of the implementing act.

4. The Commission shall determine the date from which the MID is to start operations by means of an implementing act once the following conditions have been met:

(a) the measures referred to in Articles 28(5) and (7), 32(5), 33(6), 43(5) and 49(6) have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the MID, which it has conducted in cooperation with the Member States authorities and the ETIAS Central Unit;

(c) eu-LISA has validated the technical and legal arrangements to collect and transmit the data referred to in Article 34 and has notified them to the Commission;

(d) the ETIAS Central Unit has notified the Commission in accordance with Article 67(3);

(e) eu-LISA has declared the successful completion of the tests referred to in paragraphs 1(b), 2(b), 3(b) and 5(b).

The Commission shall set the date referred to in the first subparagraph to be within 30 days from adoption of the implementing act.

5. The Commission shall determine by means of implementing acts the date from which the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum data quality standards are to be used, once the following conditions have been met:

(a) the measures referred to in Articles 37(4) have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum data quality standards, which it has conducted in cooperation with the Member States authorities.

The Commission shall set the date referred to in the first subparagraph to be within 30 days from adoption of the implementing act.

6. The Commission shall determine the date from which the CRRS is to start operations by means of an implementing act once the following conditions have been met:

(a) the measures referred to in Articles 39(5) and 43(5) have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the CRRS, which it has conducted in cooperation with the Member States authorities;

(c) eu-LISA has validated the technical and legal arrangements to collect and transmit the data referred to in Article 39 and has notified them to the Commission.

The Commission shall set the date referred to in the first subparagraph to be within 30 days from adoption of the implementing act.

7. The Commission shall inform the European Parliament and the Council of the results of the tests carried out pursuant to paragraphs 1(b), 2(b), 3(b), 4(b), 5(b) and 6(b).

8. Member States, the ETIAS Central Unit and Europol shall start using each of the interoperability components from the date determined by the Commission in accordance with paragraphs 1, 2, 3 and 4 respectively.

Article 69

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Articles 28(5), 39(5), 49(6), 63(2) and 65(8) shall be conferred on the Commission for a period of five years from 11 June 2019. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

3. The delegation of power referred to in Articles 28(5), 39(5), 49(6), 63(2) and 65(8) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Articles 28(5), 39(5), 49(6), 63(2) and 65(8) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 70

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Where the committee delivers no opinion, the Commission shall not adopt the draft implementing act and the third subparagraph of Article 5(4) of Regulation (EU) No 182/2011 shall apply.

Article 71

Advisory Group

An Interoperability Advisory Group shall be established by eu-LISA. During the design and development phase of the interoperability components, Article 54(4), (5) and (6) shall apply.

Article 72

Training

eu-LISA shall perform tasks related to the provision of training on the technical use of the interoperability components in accordance with Regulation (EU) 2018/1726.

Member States authorities and Union agencies shall provide their staff authorised to process data using the interoperability components, with appropriate training programmes concerning data security, data quality, data protection rules, the procedures applicable to data processing and the obligations to inform under Articles 32(4), 33(4) and 47.

Where appropriate, joint training courses on these topics shall be organised at Union level to enhance cooperation and the exchange of best practices between the staff of Member States authorities and Union agencies who are authorised to process data using the interoperability components. Particular attention shall be paid to the process of multiple-identity detection, including the manual verification of different identities and the accompanying need to maintain appropriate safeguards of fundamental rights.

Article 73

Practical handbook

The Commission shall, in close cooperation with the Member States, eu-LISA and other relevant Union agencies, make available a practical handbook for the implementation and management of the interoperability components. The practical handbook shall provide technical and operational guidelines, recommendations and best practices. The Commission shall adopt the practical handbook in the form of a recommendation.

Article 74

Monitoring and evaluation

1. eu-LISA shall ensure that procedures are in place to monitor the development of the interoperability components and their connection to the national uniform interface 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 12 December 2019 and every six months thereafter during the development phase of the interoperability components, eu-LISA shall submit a report to the European Parliament and to the Council on the state of play of the development of the interoperability components, as well as their connection to the national uniform interface. Once the development is finalised, a report shall be submitted to the European Parliament and to the Council explaining in detail how the objectives, in particular relating to planning and costs, were achieved as well as justifying any divergences.

3. Four years after the start of operations of each interoperability component in accordance with Article 68 and every four years thereafter, eu-LISA shall submit to the European Parliament, to the Council and to the Commission a report on the technical functioning of the interoperability components, including their security.

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

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

(b) an examination of the results achieved against the objectives of this Regulation and its impact on fundamental rights, including in particular an assessment of the impact of the interoperability components on the right to non-discrimination;

(c) an assessment of the functioning of the web portal, including figures regarding the use of the web portal and the number of requests that were resolved;

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

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

(f) an assessment of the use of the CIR for identification;

(g) an assessment of the use of the CIR for preventing, detecting or investigating terrorist offences or other serious criminal offences;

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

(i) an assessment of the search of the Interpol databases via the ESP, including information on the number of matches against Interpol databases and information on any problems encountered.

The overall evaluation under the first subparagraph of this paragraph 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.

5. By 12 June 2020 and every year thereafter until the implementing acts of the Commission referred to in Article 68 have been adopted, the Commission shall submit a report to the European Parliament and to the Council on the state of play of preparations for the full implementation of this Regulation. That report shall contain also detailed information about the costs incurred and information as to any risks which may impact the overall costs.

6. Two years after the start of operations of the MID in accordance with Article 68(4), the Commission shall produce an examination of the impact of the MID on the right to non-discrimination. Following this first report, the examination of the impact of the MID on the right to non-discrimination shall be part of the examination referred to in paragraph 4(b) of this Article.

7. The Member States and Europol shall provide eu-LISA and the Commission with the information necessary to draft the reports referred to in paragraphs 3 to 6. This information shall not jeopardise working methods or include information that reveals sources, staff members or investigations of the designated authorities.

8. eu-LISA shall provide the Commission with the information necessary to produce the overall evaluation referred to in paragraph 4.

9. While respecting the provisions of national law on the publication of sensitive information, and without prejudice to limitations necessary to protect security and public order, prevent crime and guarantee that no national investigation will be jeopardised, each Member State and Europol shall prepare annual reports on the effectiveness of access to data stored in the CIR for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences, containing information and statistics on:

(a) the exact purposes of the consultation including the types of terrorist offences or other serious criminal offences;

(b) the reasonable grounds given for a substantiated suspicion that a suspect, perpetrator or victim is covered by Regulation (EU) No 603/2013;

(c) the number of requests for access to the CIR for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences;

(d) the number and types of cases that have ended in successful identifications;

(e) the need and use made of the exceptions for cases of urgency including those cases where that urgency was not accepted by the ex post verification carried out by the central access point.

The annual reports prepared by the Member State and Europol shall be transmitted to the Commission by 30 June of the subsequent year.

10. A technical solution shall be made available to Member States in order to manage user access requests referred to in Article 22 and to facilitate the collection of the information under paragraphs 7 and 9 of this Article for the purpose of generating reports and statistics referred to in those paragraphs. The Commission shall adopt implementing acts to lay down the specifications of the technical solution. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 70(2).

Article 75

Entry into force and applicability

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

The provisions of this Regulation related to the ESP shall apply from the date determined by the Commission in accordance with Article 68(1).

The provisions of this Regulation related to the shared BMS shall apply from the date determined by the Commission in accordance with Article 68(2).

The provisions of this Regulation related to the CIR shall apply from the date determined by the Commission in accordance with Article 68(3).

The provisions of this Regulation related to the MID shall apply from the date determined by the Commission in accordance with Article 68(4).

The provisions of this Regulation related to the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum data quality standards shall apply respectively from the dates determined by the Commission in accordance with Article 68(5).

The provisions of this Regulation related to the CRRS shall apply from the date determined by the Commission in accordance with Article 68(6).

Articles 6, 12, 17, 25, 38, 42, 54, 56, 58, 66, 67, 69, 70, 71, 73 and 74(1) shall apply from 11 June 2019.

This Regulation shall apply in relation to Eurodac from the date the recast of Regulation (EU) No 603/2013 becomes applicable.

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

Done at Brussels, 20 May 2019.

For the European Parliament	*For the Council*
The President	*The President*
A. TAJANI	G. CIAMBA

ISSN 1977-0677 (electronic edition)
ISSN 1725-2555 (paper edition)

Publications Office of the European Union
2985 Luxembourg
LUXEMBOURG

EN