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