Council of the European Union

Brussels, 8 February 2019
(OR. en)

5691/19

Interinstitutional Files:
2017/0351(COD)
2017/0352(COD)

LIMITE

COSI 5	**VISA 13**
FRONT 20	**FAUXDOC 3**
ASIM 7	**COPEN 19**
DAPIX 19	**CSCI 12**
ENFOPOL 26	**SAP 1**
ENFOCUSTOM 18	**JAI 55**
SIRIS 15	**CT 4**
SCHENGEN 2	**COMIX 37**
DATAPROTECT 13	**CODEC 187**

NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee
No. prev. doc.:	15273/18
Subject:	Amended proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399, Regulation (EU) 2017/2226, Regulation (EU) 2018/XX [the ETIAS Regulation], Regulation (EU) 2018/XX [the Regulation on SIS in the field of border checks] and Regulation (EU) 2018/XX [the eu-LISA Regulation] Amended proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) and amending [Regulation (EU) 2018/XX [the Eurodac Regulation], Regulation (EU) 2018/XX [the Regulation on SIS in the field of law enforcement], Regulation (EU) 2018/XX [the ECRIS-TCN Regulation] and Regulation (EU) 2018/XX [the eu-LISA Regulation] - Confirmation of the final compromise text with a view to agreement

1. On 12 December 2017, the Commission presented two legislative proposals for Regulations of the European Parliament and of the Council establishing a framework for interoperability between EU information systems: one focusing on large-scale information systems relating to borders and visa[1], the second on information systems relating to police and judicial cooperation, asylum and migration[2] (the 'Interoperability Proposals').

2. Considering the importance and the priority status of the proposals, the Bulgarian Presidency worked intensively in order to reach a compromise on both texts that would be acceptable to Member States, with a view to starting negotiations with the European Parliament as soon as it was ready. The initial compromise was endorsed by the Permanent Representatives Committee at its meeting on 14 June 2018[3].

3. On 13 June 2018, the Commission amended the Interoperability Proposals in order to include some further necessary amendments to other legal instruments (ETIAS, SIS, ECRIS-TCN, Eurodac and eu-LISA)[4]. This was required to take into account the results of the ongoing negotiations between the co-legislators on some of the information systems concerned.
A revised mandate was therefore adopted by the Permanent Representatives Committee as an 'I' item on 12 September 2018[5].

4. The Committee on Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament adopted its report on 15 October 2018.

---

1 15119/17
2 15729/17
3 10453/18
4 10178/18 and 10190/18
5 11312/18

5. Four trilogues took place on 24 October, 15 and 27 November and 13 December 2018 under the Austrian Presidency. Following intense preparatory work at technical level, agreement was reached on major political issues during the fourth trilogue (access to the Common Identity Repository for identification and law enforcement purposes, transitional period for the use of the European Search Portal and for the tasks of the ETIAS Central Unit, time-limits for the verification of multiple identities at the borders, keeping of logs for data monitoring purposes, access by third country jurisdictions, web portal for exercising data subjects' rights, penalties and liability, the delegated acts and implementing acts package, including the no opinion clause, and the non-discrimination provision) and confirmed by Coreper on 19 December 2018 [6].

6. Six JHA Counsellors meetings were organised and seven technical meetings took place with the European Parliament and the Commission in order to solve the outstanding issues and finalise the drafting of the texts (i.e. links, data quality, deadlines for the right of access, right to information, query of Interpol databases, monitoring and evaluation, start of operations, illegal immigration vs. irregular migration, Eurodac references, the recitals and the provisions of the Police text diverging from the Borders text). A fifth and final trilogue took place on 5 February which confirmed the outcome of the intricate negotiations that had taken place at technical level under the Romanian Presidency.

7. Against this background, the Permanent Representatives Committee is invited to:

   (a) approve the final compromise texts, as set out in Annexes I and II to this note, and

   (b) confirm that the Presidency can indicate to the European Parliament that, should the European Parliament adopt its position at first reading as regards the regulations as set out in Annexes I and II to this note, subject to revision of those texts by the lawyer-linguists of both institutions, the Council would approve the European Parliament's position and the acts shall be adopted in the wording which corresponds to the European Parliament's position.

---

[6] 15273/18

ANNEX I

2017/0351 (COD)

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

After consulting the European Data Protection Supervisor,

Having regard to the opinion of the European Economic and Social Committee,[7]

Acting in accordance with the ordinary legislative procedure,

[7] OJ C , , p. .

Whereas:

(1) In its Communication of 6 April 2016 entitled Stronger and Smarter Information Systems for Borders and Security[8], 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 the interoperability between EU information systems for security, border and migration management, with the aim to address the structural shortcomings related to these 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[9], 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[10], 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) The European Council of 15 December 2016[11] called for continued delivery on the interoperability of EU information systems and databases.

(5) In its final report of 11 May 2017[12], the high-level expert group on information systems and interoperability concluded that it is necessary and technically feasible to work towards practical solutions for interoperability and that they can, in principle, both deliver operational gains and be established in compliance with data protection requirements.

---

8 COM(2016)205, 6.4.2016.

9 Roadmap of 6 June 2016 to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area — 9368/1/16 REV 1.

10 European Parliament resolution of 6 July 2016 on the strategic priorities for the Commission Work Programme 2017 (2016/2773(RSP)).

11 http://www.consilium.europa.eu/en/press/press-releases/2016/12/15/euco-conclusions-final/.

12 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

(6) In its Communication of 16 May 2017 entitled Seventh progress report towards an effective and genuine Security Union[13], the Commission set out, in line with its Communication of 6 April 2016 and confirmed by 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 where all EU information systems for security, border and migration management are interoperable in full respect of fundamental rights.

(7) In its Conclusions of 9 June 2017[14] 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 as proposed by the high-level expert group.

(8) The European Council of 23 June 2017[15] underlined the need to improve the interoperability between databases and invited the Commission to prepare, as soon as possible, draft legislation enacting the proposals made by the high-level expert group on information systems and interoperability.

(9) With a view to improve the effectiveness and efficiency of checks at the external borders, to contribute to preventing and combating illegal immigration and to contribute to a high level of security within the area of freedom, security and justice of the Union, including the maintenance of public security and public policy and safeguarding the security in the territories of the Member States, to improve the implementation of the common visa policy, to assist in examining applications for international protection, to contribute in the prevention, detection and investigation of terrorist offences or other serious criminal offences, to aid in the identificaton of unknown persons who are unable to identify themselves or unidentified human remains in cases of natural disasters, accidents or terrorist attacks, 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 the individual, 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.

---

13 COM(2017) 261 final, 16.5.2017.

14 http://www.consilium.europa.eu/media/22186/st10136en17-vf.pdf.

15 European Council conclusions, 22-23 June 2017.

(10) The interoperability between the EU information systems should allow said systems to supplement each other in order to facilitate the correct identification of persons, including unknown persons who are not able to identify themselves or unidentified remains, contribute to fighting identity fraud, improve and harmonise 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 the access for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences to the EES, the VIS, the ETIAS and Eurodac, and support the purposes of the EES, the VIS, the ETIAS, Eurodac, the SIS and the ECRIS-TCN system.

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

(12) The interoperability components should concern persons in respect of whom personal data may be processed in the EU information systems and by Europol, namely persons whose personal data are processed in the EU information systems and by Europol.

(13) The European search portal (ESP) should be established to facilitate technically the ability of Member State authorities and Union agencies to have fast, seamless, efficient, systematic and controlled access to the EU information systems, the Europol data and the Interpol databases insofar as this is needed to perform their tasks, in accordance with their access rights, and to support the objectives of the EES, the VIS, the ETIAS, Eurodac, the SIS, the ECRIS-TCN system and the Europol data. Enabling the simultaneous querying of all relevant EU information systems in parallel, as well as of the Europol data and the Interpol databases, the ESP should act as a single window or 'message broker' to search 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.

(13a) When querying the Interpol databases, the design of the ESP should ensure that the data used by the user of the ESP to launch a query is not shared with the owners of Interpol data. The design of the ESP shall also ensure that the Interpol databases are only queried in accordance with applicable Union and national law.

(14) The International Criminal Police Organisation (Interpol) database of Stolen and Lost Travel Documents (SLTD) enables authorised entities responsible for preventing, detecting or investigating terrorist offences or other serious criminal offences in Member States, including immigration and border control officers, to establish the validity of a travel document. The ETIAS queries the SLTD and Interpol's Travel Documents Associated with Notices (TDAWN) database in the context of assessing whether a person applying for a travel authorisation is likely for instance to migrate irregularly or could pose a threat to security. The centralised European search portal (ESP) should enable the query against the SLTD and TDAWN databases using an individual's identity data or travel document data. Where personal data are transferred from the Union to Interpol through the ESP, the provisions on international transfers in Chapter V of Regulation (EU) 2016/679 of the European Parliament and of the Council[16], or the national provisions transposing Chapter V of Directive (EU) 2016/680 of the European Parliament and of the Council[17] should apply. This should be without prejudice to the specific rules laid down in Council Common Position 2005/69/JHA[18] and Council Decision 2007/533/JHA[19].

(15) The European search portal (ESP) should be developed and configured in such a way that it does not allow the use of fields of data for the query that are not related to persons or travel documents or that are not present in an EU information system, in the Europol data or in the Interpol database.

(16) To ensure the systematic use of the relevant EU information systems, the European search portal (ESP) should be used to query the common identity repository, the EES, the VIS, the ETIAS, Eurodac and the ECRIS-TCN system. However, the 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 the Central SIS in accordance with their access rights and in order to perform their tasks. The ESP should be an additional means to query the Central SIS, the Europol data and the Interpol systems, complementing the existing dedicated interfaces.

---

16 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).

17 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).

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

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

(17) Biometric data, such as fingerprints and facial images, are unique and therefore much more reliable than alphanumeric data for identifying a person. The shared biometric matching service (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 may be registered in different databases, by matching their biometric data across different systems and by relying on one unique technological component instead of five different ones in each of the underlying systems. 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, the VIS and the 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, facilitating cross-system comparisons using biometric templates and enabling economies of scale in developing and maintaining the EU central systems.

(17a) The biometric templates stored in the shared BMS which are comprised of data derived from a feature extraction of actual biometric samples should be obtained in such a way that reverting the 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 the SIS, are only used for SIS purposes and cannot be used to be cross-checked with data present in other information systems, in line with the principles of necessity and proportionality, the shared BMS should not store DNA profiles or biometric templates obtained from palm print data.

(18) Biometric data constitute sensitive personal data. This R~~r~~egulation should lay down the basis for and the safeguards for processing of such data for the purpose of uniquely identifying the persons concerned.

(19) The systems established by Regulation (EU) 2017/2226 of the European Parliament and of the Council[20], Regulation (EC) No 767/2008 of the European Parliament and of the Council[21], Regulation (EU) 2018/1240, the system established by the Eurodac Regulation and the system established by the ECRIS-TCN Regulation require the accurate identification of the persons whose personal data are stored therein.

---

20 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).

21 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).

(20) The common identity repository (CIR) should therefore facilitate and assist in the correct identification of persons registered in the EES, the VIS, the ETIAS, Eurodac and the ECRIS-TCN system.

(21) Personal data stored in these EU information systems may relate to the same person 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. The common identity repository (CIR) should store the personal data concerning persons present in the systems that are necessary to enable the more accurate identification of those individuals, therefore including their identity, travel document and biometric data, regardless of the system in which the data was 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 ~~is~~ deleted in the underlying systems in accordance with their logical separation.

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

(23) In that connection, creating an individual file in the common identity repository (CIR) for each person that is recorded in the EES, the VIS, the ETIAS, Eurodac or the ECRIS-TCN system, is necessary to achieve the purpose of correct identification within the Schengen area, and to support the multiple-identity detector for the dual purpose of facilitating identity checks for bona fide travellers and combating identity fraud. The individual file should store in one single place and make accessible to the duly authorised end-users all the possible identities linked to a person.

(24) The common identity repository (CIR) should thus support the functioning of the multiple-identity detector and to 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, investigation or detection of serious crime.

(25) The common identity repository (CIR) should provide for a shared container for identity, travel document and biometric data of persons registered in the EES, the VIS, the ETIAS, Eurodac and the ECRIS-TCN system. It should be part of the technical architecture of these systems and serve as the shared component between them for storage of the identity, travel document and biometric data, and to allow their querying.

(26) All records in the common identity repository (CIR) should be logically separated by automatically tagging each record with the underlying system owning that record. The access control of the CIR should use these tags to allow the record to be accessible or not.

(27) 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 and provide 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 interest of the child.

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

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

(30) This Regulation should also introduce a new possibility for streamlined access to data beyond identity data or travel document data present in the EES, the VIS, the ETIAS or Eurodac by Member State designated authorities responsible for preventing, detecting or investigating terrorist offences or other serious criminal offences and Europol. Data, including data other than identity data or travel document data contained in those systems, 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 consultation will contribute to the prevention, detection or investigation of the criminal offences or other serious criminal offences in question, 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.

(31) Full access to the necessary data contained in the EU information systems necessary for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences, beyond the relevant identity data or travel document data covered under common identity repository (CIR), should continue to be governed by the provisions in the respective 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 in the conduct of their tasks. The end-user authorised by the designated authority should therefore be allowed to see in which of the EU information systems the data corresponding to the query introduced are recorded. The concerned system would thus be flagged following the automated verification of the presence of a match in the system (a so-called match-flag functionality).

(31a) The reply will not be interpreted and used as a ground or reason to draw conclusions on or undertake measures towards 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 legislative instruments governing such access. Any such act will be subject to measures set out in Chapter VII and measures in Regulation (EU) 2016/679, Directive (EU) 2016/680 or Regulation (EU) 2018/1725.

(31b) As a general rule, where a match-flag indicates that the data are recorded in the EES, ETIAS VIS or Eurodac, the designated authorities or Europol should request full access to at least one of the EU information systems concerned. Where exceptionally such full access is not requested, for example because designated authorities or Europol have already obtained the data by other means, or obtaining the data is no longer permitted under national law, the justification for not requesting access should be recorded.

(32) The logs of the queries of the common identity repository should indicate the purpose of the query. 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, therefore indicating that such query was launched for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences.

(33) The query of the common identity repository (CIR) by Member State designated authorities and Europol in order to obtain a match-flag type of response indicating the data are recorded in the EES, the VIS, the ETIAS or Eurodac requires automated processing of personal data. A match-flag would 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 concerned individual 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 would therefore realise a very limited interference with the right to protection of personal data of the concerned individual, while it would be necessary to allow the designated authority and Europol to address its request for access to personal data more effectively directly to the system that was flagged as containing it.

(34) (…)

(35) The multiple-identity detector (MID) should be established to support the functioning of the common identity repository and to support the objectives of the EES, the VIS, the ETIAS, Eurodac, the SIS and the ECRIS-TCN system. 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 therein.

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

(37) The multiple-identity detector (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 the links between individuals present in more than one EU information system, strictly limited to the data necessary to verify that a person is recorded in a justified or unjustified manner under different biographical identities in different systems, or to clarify that two persons having similar biographical data may not be the same person. Data processing through the European search portal (ESP) and the shared biometric matching service (shared BMS) in order to link individual files across individual systems should be kept to an absolute minimum and therefore is limited to a multiple-identity detection at the time new data are ~~is~~ added to one of the information systems included in the common identity repository and in the SIS. The MID should include safeguards against potential discrimination or unfavourable decisions for persons with multiple lawful identities.

(38) 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. 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, the effective implementation of the Union's asylum and visa policies.

(39) The European search portal (ESP) and shared biometric matching service (shared BMS) should compare data in common identity repository (CIR) and SIS on persons when new records are created or uploaded by a national authority or an Union agency. Such comparison should be automated. The CIR and the SIS should use the shared BMS to detect possible links on the basis of biometric data. The CIR and the SIS should use the ESP to detect possible links on the basis of alphanumeric data. The CIR and the SIS should be able to identify identical or similar data on the 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 the 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 concerned person.

(40) The national authority or Union agency that recorded the data in the respective EU information system should confirm or change these links. This authority should have access to the data stored in the common identity repository (CIR) or the SIS and in the multiple-identity detector (MID) for the purpose of the manual identity verification.

(41) (…)

(42) The manual verification of multiple identities should be ensured by the authority creating or updating the data that triggered a match resulting in a link with data already stored in another EU information system. The authority responsible for the verification of multiple identities should assess whether there are multiple identities referring to the same person in a justified or unjustified manner. Such assessment should be performed where possible in the presence of the persons and where necessary by requesting additional clarifications or information. Such assessment should be performed without delay, in line with legal requirements for the accuracy of information under Union and national law. Especially at borders, the persons involved would be restricted in their movement for the duration of the verification which should not last indefinitely. The existence of a yellow link in the MID should not constitute in itself a ground for refusal of entry and any decision on authorising or refusing entry should exclusively be taken on the basis of the applicable provisions of the Schengen Borders Code.

(43) For the links obtained in relation to the Schengen Information System (SIS) related to the alerts in respect of persons wanted for arrest or 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 verification of multiple identities should be the SIRENE Bureau of the Member State that created the alert. Indeed those categories of SIS alerts are sensitive and should not necessarily be shared with the authorities creating or updating the data 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 the SIS Regulations.

(43a) The creation of those links requires transparency towards the individuals affected. In order to facilitate the implementation of the necessary safeguards in accordance with Union data protection rules, individuals who are subject to a red link or a white link following manual verification should be informed in writing without prejudice to limitations to protect security and public order, prevent crime and guarantee that any national investigation will not be 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.

(43b) In addition to the access to the MID foreseen for the authority responsible for the verification of multiple identities where a yellow link is created, access to the MID by Member State authorities and Union agencies having access to at least one EU information system included in the CIR or to the SIS is foreseen where a red link exists. The red links indicates that a person is using different identities in an unjustified manner or that a person is using somebody else's identity.

(43c) Access to the MID by Member State authorities and Union agencies is also foreseen where a white or green link exists between data from two EU information systems where such authority has access to both information systems. Such access is granted for the sole purpose of allowing that Member State authority or Union agency to detect potential cases where the link was incorrect or that the data processed in the MID, CIR and SIS were processed in breach of this Regulation and take necessary actions to correct the situation and replace the link.

(44) eu-LISA should establish automated data quality control mechanisms and common data quality indicators. eu-LISA should be responsible to develop a central monitoring capacity for data quality and to produce regular data analysis reports to improve the control of implementation and application by Member States of EU information systems. The common quality indicators should include the minimum quality standards to store data in the EU information systems or the interoperability components. The goal of such a data quality standards should be for the EU information systems and interoperability components to automatically identify apparently incorrect or inconsistent data submissions so that the originating Member State is able to verify the data and carry out any necessary remedial actions.

(45) The Commission should evaluate eu-LISA 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.

(46) The Universal Message Format (UMF) should establish a standard for structured, cross-border information exchange between information systems, authorities and/or organisations in the field of Justice and Home affairs. 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 the exchange in a consistent and semantically equivalent manner.

(46a) The implementation of the UMF standard may be considered in the VIS, the SIS and in any existing or new cross-border information exchange models and information systems in the area of Justice and Home Affairs, developed by Member States.

(47) 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 respective legal instruments. eu-LISA should establish, implement and host the CRRS in its technical sites containing anonymous statistical data from the above-mentioned systems, the common identity repository, the multiple-identity detector and the shared biometric matching service. 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.

(48) Regulation (EU) 2016/679 should apply to the processing of personal data 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, in which case Directive (EU) 2016/680 of the European Parliament and of the Council should apply.

(48a) Where the processing of personal data by the Member States for the purpose of interoperability 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.[22]

(48b) Regulation (EU) 2016/679 or, where relevant, Directive (EU) 2016/680 should also apply to the transfers of personal data to third countries or international organisations carried out in accordance with 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.

(49) The specific provisions on data protection of Regulation (EU) 2017/2226, Regulation (EC) No 767/2008, Regulation (EU) 2018/1240, and Regulation (EU) 2018/1861 should apply to the processing of personal data in those respective systems.

[22] The following recital has been included as part of the political agreement in the ETIAS file: "Where the processing of personal data by the Member States for the purpose of assessing applications 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."

(50) Regulation (EU) 2018/1725 should apply 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 should apply to the processing of personal data by Europol.

(51) The national supervisory authorities established in accordance with Regulation (EU) 2016/679 or Directive (EU) 2016/680 should monitor the lawfulness of the processing of personal data by the Member States, whilst the European Data Protection Supervisor as established by Regulation (EU) 2018/1725 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 him under this Regulation, sufficient resources, including both human and financial resources, are required.

(52) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 16 April 2018.

(52a) The Article 29 Data Protection Working Party provided an opinion on the Commission proposal on 11 April 2018.

(53) (…)

(54) 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 regarding the development, design and management of the interoperability components. eu-LISA obligations in this respect should include adopting the measures necessary to prevent access by unauthorised persons, such as staff of external service providers, to personal data processed through the interoperability components. When awarding contracts for the provision of services, the Member States and eu-LISA should consider any measures necessary to secure compliance with laws or regulations relating to the protection of personal data and the privacy of individuals or to safeguard essential security interests, in line with the Financial regulation and applicable international conventions. eu-LISA should apply the principles of privacy by design and by default during the development of the interoperability components.

(55) The implementation of the interoperability components provided for in this Regulation will have an impact on the way checks are carried out at border crossing points. These impacts will result from a combined application of the existing rules of Regulation (EU) 2016/399 of the European Parliament and of the Council[23] and the rules on interoperability provided for in this Regulation.

(56) As a consequence of this combined application of the rules, the European search portal (ESP) should constitute the main access point for the compulsory systematic consultation of databases for persons at border crossing points provided for by the Schengen Borders Code. In addition, the identity data or travel document data that led to the classification of a link in the multiple-identity detector (MID) as a red link should be taken into account by the border guards for assessing whether or not the person fulfils the conditions of entry defined in the Schengen Borders Code. However the presence of a red link should not in itself constitute a ground for refusal of entry and the existing grounds for refusal of entry listed in the Schengen Borders Code should therefore not be amended.

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

(58) (…)

(59) Should the query of the multiple-identity detector (MID)[24] through the European search portal (ESP) result in a yellow link or detect a red link, the border guard should consult the common identity repository or the Schengen Information System or both in order to assess the information on the person being checked, to manually verify his/her different identity and to adapt the colour of the link if required.

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

---

23 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, OJ L 77, 23.3.2016, p.1.

24 How the components are mentioned (in full or acronyms) will be cross-checked by the lawyer-linguists.

(61) In order to allow competent authorities and the Union agencies to adapt to the new requirements on the use of the European search portal (ESP), it is necessary to provide for a transitional period. Similarly, in order to allow for the coherent and optimal functioning of the multiple-identity detector (MID), transitional measures should be established for the start of its operations.

(61a) Since the objectives 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. 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 those objectives.

(62) The remaining amount on the budget earmarked for Smart Borders in Regulation (EU) No 515/2014 of the European Parliament and the Council[25] should be reallocated to this Regulation, pursuant to Article 5(5)(b) of Regulation (EU) No 515/2014 to cover the costs for the development of the interoperability components.

(63) 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 should be delegated to the Commission in respect of the extension of the transitional period for the use of the European Search Portal (ESP), as well as for the ETIAS Central Unit and extension of the transitional period for the use of multiple-identity detection (MID). In particular, power should be delegated to the Commission in respect of the procedures to determine the cases where identity data can be considered as identical or similar, the rules on the operation of the CRRS, including specific safeguards for processing of personal data and 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 on Better Law-Making of 13 April 2016[26]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council should receive all documents at the same time as Member State experts, and their experts should systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

---

25 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).

26 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.123.01.0001.01.ENG.

(64) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to adopt detailed rules on: technical details of profiles for the users of the European search portal (ESP); specifications of the technical solution to facilitate the querying of EU information systems, Europol data and Interpol databases by the ESP and format of the ESP replies; technical rules for creating links in MID between data from different EU information systems; the content of the form and the modalities for informing the data subject where a red link is created; performance requirements and performance monitoring of the shared BMS; automated data quality control mechanisms, procedures and indicators; development of the UMF standard; cooperation procedure in case of security incidents; determining the dates from which the ESP, sBMS, CIR, MID, CRRS are to start operations; and the specifications of the technical solution for Member States in order 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.

(65) (…)

(65a) As interoperability components will involve the processing of significant amounts of sensitive personal data, it is important that persons whose data is processed through those components can effectively exercise their rights as data subjects as laid down in Regulation (EU) 2016/679, Directive (EU) 2016/680 and Regulation (EU) 2018/1725. The data subjects should be provided with web portal that facilitates them in exercising their rights to access to and rectification, erasure and restriction of their personal data. eu-LISA should establish and manage such a web portal.

(65b) One of the core principles of data protection is data minimisation as highlighted in Article 5(1)(c) of Regulation (EU) 2016/679 in accordance with which 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 do 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 purpose of this Regulation.

(65c) This Regulation should contain clear provisions on liability and right to compensation for unlawful processing of personal data or from any other act incompatible with it, 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. With regard to the role of eu-LISA as a data processor, this latter should be responsible for the damage it provoked where it has not complied with the specific obligations of this Regulation directed to it, or where it has acted outside or contrary to lawful instructions of the Member State which is the data controller.

(66) This Regulation is without prejudice to the application of Directive 2004/38/EC.

(67) This Regulation constitutes a development of the provisions of the Schengen acquis.

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

(69) This Regulation constitutes a development of the provisions of the Schengen acquis in which the United Kingdom does not take part, in accordance with Council Decision 2000/365/EC[27]; the United Kingdom is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(70) This Regulation constitutes a development of the provisions of the Schengen acquis in which Ireland does not take part, in accordance with Council Decision 2002/192/EC[28]; Ireland is therefore not taking part in the adoption of this Regulation and is not bound by it nor subject to its application.

(71) As regards Iceland and Norway, this Regulation constitutes a development of the provisions of the Schengen acquis within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis[29] which fall within the area referred to in Article 1, points A, B, C and G of Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of that Agreement[30].

---

27 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).

28 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).

29 OJ L 176, 10.7.1999, p. 36.

30 OJ L 176, 10.7.1999, p. 31.

(72) As regards Switzerland, this Regulation constitutes a development of the provisions of the Schengen acquis within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis[31] which fall within the area referred to in Article 1, points A, B, C and G of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/146/EC[32].

(73) As regards Liechtenstein, this Regulation constitutes a development of the provisions of the Schengen acquis within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis[33] which fall within the area referred to in Article 1, points A, B, C and G of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU[34].

(74) 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.

(75) In order to have this Regulation fit into the existing legal framework, Regulation (EU) 2016/399, Regulation (EU) 2017/2226, Council Decision 2008/633/JHA, Regulation (EC) No 767/2008 and Council Decision 2004/512/EC should be amended accordingly,

HAVE ADOPTED THIS REGULATION:

---

31 OJ L 53, 27.2.2008, p. 52.
32 OJ L 53, 27.2.2008, p. 1.
33 OJ L 160, 18.6.2011, p. 21.
34 OJ L 160, 18.6.2011, p. 19.

CHAPTER I
General provisions

Article 1

Subject matter

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

2. 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 lays down the responsibilities of the Member States and of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), with respect to the design, development and operation of the interoperability components.

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

4a. This Regulation also lays down a framework for verifying identities and for identifying persons.

Article 2

Objectives

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

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

(b) to contribute to preventing and combating 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 the security in the territories of the Member States;

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

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

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

(eb) to aid in the identification of unknown persons who are unable to identify themselves or unidentified human remains in cases of natural disasters, accidents or terrorist attacks.

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

(a) ensuring the correct identification of persons;

(b) contributing to combating identity fraud;

(c) improving the 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 bases of the individual systems, data protection standards and principles;

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

(e) strengthening and simplifying and making more uniform the data security and data protection conditions that govern the respective EU information systems, without prejudice to 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 the necessary and proportionate conditions for that;

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

Article 3

Scope

1. This Regulation applies to EES, VIS, ETIAS and SIS.

2. This Regulation applies to persons in respect of whom personal data may be processed in the EU information systems referred to in paragraph 1 and whose data are collected for the purposes defined in Article 1 of Regulation (EC) No 767/2008, Article 1 of Regulation (EU) 2017/2226, Article 1 of Regulation (EU) 2018/1240, Article 1 of Regulation (EU) 2018/1860 and Article 1 of (EU) 2018/1861.

Article 4

Definitions

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

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

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

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

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

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

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

(7) (…)

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

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

(10) ’fingerprint data' means fingerprints 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;

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

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

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

(14) ‘travel document’ means a passport or other equivalent document entitling the holder to cross the external borders and to which a visa may be affixed;

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

(16) (…)

(17) (…)

(18) 'EU information systems' means the EES, VIS, ETIAS, Eurodac, SIS and ECRIS-TCN operationally managed by eu-LISA;

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

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

(21) '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;

(22) (..)

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

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

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

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

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

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

(29) 'the European Travel Information and Authorisation System' ('ETIAS') means the European Travel Information and Authorisation System as referred to in Regulation (EU) 2018/1240;

(30) 'Eurodac' means Eurodac as referred to in Regulation (EU) No 603/2013;

(31) 'Schengen Information System' ('SIS') means the Schengen Information System as referred to in Regulation (EU) 2018/1860, Regulation (EU) 2018/1861 and Regulation (EU) 2018/1862;

(32) 'ECRIS-TCN System' means the centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons as referred to in the ECRIS-TCN Regulation[35].

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 and persons with a disability and persons in need of international protection. The best interests of the child shall be a primary consideration.

[35] OJ: please include the reference number of this Regulation when it is published.

CHAPTER II
European Search Portal

Article 6

European search portal

1. A 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 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, the VIS, the ETIAS, Eurodac, the SIS, the ECRIS-TCN system as well as of the Europol data and the Interpol databases;

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

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

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

2. The authorities referred to in paragraph 1 shall use the ESP to search data related to persons or their travel documents in the central systems of the EES, VIS and ETIAS in accordance with their access rights as referred to in the legal instruments governing these 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 Regulation (EU) 2018/1860 and Regulation (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 authorities referred to in paragraph 1 may use the ESP to search data related to travel documents in the Interpol databases where provided for and in accordance with their access rights under Union and national law.

Article 8

Profiles for the users of the European search portal

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

(a) the fields of data used for querying;

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

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

(c) the fields 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 for the users of the ESP referred to in Article 7(1) in accordance with their access rights as laid down in the legal instruments governing EU information systems and in accordance with national law. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

2a. 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 users of the ESP shall launch a query by submitting alphanumeric and/or biometric data to the ESP. Where a query has been launched, the ESP shall query simultaneously, with the data submitted by the user of the ESP and in accordance with the user profile, the EES*, the ETIAS, the VIS, the SIS, Eurodac, the ECRIS-TCN system and the CIR as well as the Europol data and the Interpol databases*.

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

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

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

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

The ESP shall provide no information regarding data in information systems to which the user has no access in accordance with 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 is available from one of the EU information systems, Europol data and 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 querying the EU information systems, Europol data and Interpol databases by the ESP and the format of the ESP replies. This implementing act shall be adopted in accordance with the examination procedure referred to in Article 64(2).

Article 10

Keeping of logs

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

(a) the Member State or Union agency launching the query and the ESP profile used as referred to in Article 8;

(b) the date and time of the query;

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

1a. Each Member State and Union Agency shall keep logs of queries of the authority and the staff duly authorised to use the ESP.

2. The logs referred to in paragraphs 1 and 1a 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, unless they are required for monitoring procedures that have already begun in which case they shall be erased once the monitoring procedures no longer require these 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 referred to in Article 9(1) or the CIR, because of a failure of the ESP, the users of the ESP 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, 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 referred to in Article 9(1) or the CIR where they are required to do so according to 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 BMS storing biometric templates obtained from the biometric data referred to in Article 13, that are stored in the CIR and the SIS, and enabling querying with biometric data across several EU information systems is established for the purposes of supporting the CIR and MID and the objectives of the EES, the VIS, Eurodac, the SIS and the ECRIS-TCN system.

2. The shared BMS shall be composed of:

(a) a central infrastructure, that shall replace the central systems of respectively the EES, VIS, SIS, Eurodac and ECRIS-TCN to the extent that it shall store biometric templates and allow to search 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 – logically separated – according to the information system from which the data originates, that it shall obtain from the following biometric data:

(a) the data referred to in Article 16(1)(d), Article 17(1)(b) and (c) and Article 18(2)(a), (b) and

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

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

(e) the data referred to in Article 4(t) and (u) of Regulation (EU) 2018/1860;

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 and a reference to the actual record in the EU information systems in which the corresponding biometric data are is stored.

3. Biometric templates shall only be entered in the shared BMS following an automated quality check of the biometric data added to one of the 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, 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. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

Article 14

Searching biometric data with the shared biometric matching service

In order to search the biometric data stored within the CIR and the SIS, the CIR and the SIS shall use the biometric templates stored in the shared BMS. Queries with biometric data shall take place in accordance with the purposes provided for in this Regulation and in Regulation (EC) No 767/2008, Regulation (EU) 2017/2226, Regulations (EU) 2018/1860, 2018/1861 and 2018/1862 and the ECRIS-TCN Regulation.

Article 15

Data retention in the shared biometric matching service

The data referred to in Article 13(1) and (2) shall be stored in the shared BMS for as long as the corresponding biometric data are stored in the CIR or the SIS and shall be erased in an automated manner.

Article 16

Keeping of logs

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

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

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

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

(c) the date and time of the query;

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

(e) (…);

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

1a. Each Member State and Union Agency shall keep logs of queries of the authority and the staff duly authorised to use the shared BMS.

2. The logs referred to in paragraphs 1 and 1a 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, unless they are required for monitoring procedures that have already begun in which case they shall be erased once the monitoring procedures no longer require these logs.

CHAPTER IV
Common Identity Repository

Article 17

Common identity repository

1. A CIR, creating an individual file for each person that is recorded in the EES, the VIS, the ETIAS, Eurodac or the ECRIS-TCN system containing the data referred to in Article 18, is established for the purpose of facilitating and assisting the correct identification of persons registered in the EES, the VIS, the ETIAS, the Eurodac and the ECRIS-TCN system 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 non-law enforcement EU information systems, 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, the VIS, the ETIAS, Eurodac and the ECRIS-TCN system to the extent that it shall store the data referred to in Article 18;

(b) a secure communication channel between the CIR, Member States and 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, the ETIAS, the VIS, Eurodac and the ECRIS-TCN system as well as with the central infrastructures of the ESP, the shared BMS and the MID.

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

3a. Where it is technically impossible to query the CIR for the purpose of identifying a person pursuant Article 20, for the detection of multiple identities pursuant Article 21 or for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences pursuant Article 22, because of a failure of the CIR, the users of the CIR shall be notified by eu-LISA in an automated manner.

4. 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 was originated:

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

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

(c) the data referred to in Article 17(2) (a), (b), (c), (d) and (e) of Regulation (EU) 2018/1240.

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

2a. The authorities accessing the CIR shall do so in accordance with their access rights as referred to in the legal instruments governing the EU information systems and in national law and in accordance with their access rights under this Regulation for the purposes referred to in Articles 20, 21 and 22.

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

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

Article 19

Adding, amending and deleting data in the common identity repository

1. Where data are added, amended or deleted in the EES, the VIS and the ETIAS, the data referred to in Article 18 stored in the individual file of the CIR shall be added, amended or deleted accordingly in an automated manner.

2. Where a white or red link is created in the MID in accordance with Articles 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 The query of the CIR shall be carried out by a police authority in accordance with paragraphs 1 and 2 only in the following circumstances:

- 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,

- where there are doubts about the identity data provided by that person,

- where there are doubts as to the authenticity of the travel document or another credible document provided by that person,

- where there are doubts as to the identity of the holder of the travel document or another credible document, or

- where the person is unable or refuses to cooperate.

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

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

1a. Where the query indicates that data on that person is 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.

1b. Where a police authority has been so empowered by national legislative measures as referred to in paragraph 2a, 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 not able to identify themselves or unidentified human remains, query the CIR with the biometric data of those persons.

2. Member States wishing to avail themselves of the possibility provided for in paragraph 1 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 police authorities competent and lay down the procedures, conditions and criteria of such checks.

2a. Member States wishing to avail themselves of the possibility provided for in paragraph 1b 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 verification of different identities determined 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 belonging to the various EU information systems connected to a yellow link.

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

Article 22

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

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

2. (…)

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

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

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

Where exceptionally, such full access is not requested, the designated authorities shall record the justification therefor traceable to the national file and Europol shall record the justification in the relevant file.

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

Article 23

Data retention in the common identity repository

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

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

Article 24

Keeping of logs

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

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

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

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

(b) the date and time of the query;

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

(d) the results of the query.

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

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

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

(b) the date and time of the query;

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

(d) where a link is created, the results of the query indicating the EU information system from which the data was received.

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

(a) (…)

(b) the date and time of the query;

(c) the data used to launch the query;

(d) the results of the query;

(e) the Member State or Union agency querying the CIR;

(f) (…).

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) to (3) are fulfilled.

5. Each Member State and Union agency shall keep logs of queries of the authority and the staff duly authorised to use the CIR pursuant to Articles 20, 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;

(ab) the purpose of access;

(b) 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.

5a. In accordance with Regulation (EU) 2016/794, for any access to the CIR pursuant to Article 22, 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.

6. The logs referred to in paragraphs 2, 3, 4, 5 and 5a 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, unless they are required for monitoring procedures that have already begun in which case they shall be erased once the monitoring procedures no longer require these logs.

7. eu-LISA shall keep the logs related to the history of the data stored in individual files, for the purposes defined in paragraph 6. eu-LISA shall erase the logs related to the history of the data stored in an automated manner, once the data are erased.

CHAPTER V
Multiple-identity Detector

Article 25

Multiple-identity detector

1. A MID creating and storing an identity confirmation file as refered to in Article 34 containing links between data in the EU information systems included in the CIR and the SIS and as a consequence detecting multiple identities, with the dual purpose of facilitating identity checks and combating identity fraud, is established for the purpose of supporting the functioning of the CIR and the objectives of the EES, the VIS, the ETIAS, Eurodac, the SIS and the ECRIS-TCN system.

2. The MID shall be composed of:

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

(b) a secure communication infrastructure to connect the MID with the 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 identity verification referred to in Article 29, access to the data referred to in Article 34 stored in the MID shall be granted to:

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

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

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

(d) (…)

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

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

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 informations systems 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 informations systems between which the green link was created and a query towards those information systems revealed a match against the two sets of data linked.

Article 27

Multiple-identity detection

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

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

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

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

(d) (…)

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

(f) (…).

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

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

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

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

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

(d) (…)

(e) surname(s); forename(s); name(s) at birth, previously used names and aliases; date of birth, place of birth, nationality(ies) and gender as referred to in Article 20(2) of Regulation (EU) 2018/1861;

(f) (…)

(g) surname(s); forename(s); name(s) at birth, previously used names and aliases; date of birth, place of birth, nationality(ies) and gender as referred to in Article 4 of Regulation (EU) 2018/1860.

(h) (…)

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

4. 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 (3a) do not report any match, the procedures referred to in Article 27(1) shall continue in accordance with the respective Regulations governing them.

2. Where the query laid down in Article 27(2), (3) and (3a) reports one or several match(es), the CIR and, where relevant, the 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 data was already linked, the existing link shall be extended to the data used to launch the query.

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

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

5. The Commission shall lay down the procedures to determine the cases where identity data can be considered as the same, similar or presenting some differences in delegated acts. Those delegated acts shall be adopted in accordance with Article 63.

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 64(2).

Article 29

Authorities responsible and manual verification of different identities

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

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

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

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

(d) (…)

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

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

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

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

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

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

(d) (…)

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

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

4. Where the authority responsible for the verification of different identities in the identity confirmation file is the competent authority referred to in Article 9(2) of Regulation (EU) 2017/2226 creating or updating an individual file in the EES in accordance with Article 14 of Regulation (EU) 2017/2226, and where a yellow link is created, that authority shall carry out additional verifications. That authority shall, for that purpose only, have access to the related data contained in the relevant identity confirmation file and shall assess the different identities and shall update the link in accordance with Articles 31 to 33 and add it to the identity confirmation file without delay.

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

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

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

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

Article 30

Yellow link

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

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

(b) the linked data has different identity data but the same travel document data, no manual verification of different identity has taken place and at least one of the EU information systems does not have biometric data on the person;

(ba) the linked data have the same identity data but different biometric data and no manual verification of different identities has taken place;

(c) the linked data has similar or different identity data, the same travel document data, but different biometric data and no manual verification of different identity has taken place.

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

Article 31

Green link

1. A link between data from two or more EU information systems shall be classified as green where:

(a) the linked data do not share the same biometric data but have the same identity data and the authority responsible for the verification of different identities concluded it refers to two different persons;

(b) the linked data do not share the same biometric data, have the similar or different identity data and have the same travel document data and the authority responsible for the verification of different identities concluded it refers to two different persons;

(c) the linked data have different identity data but have the same travel document data and at least one of the EU information systems does not have biometric data on the person and the authority responsible for the verification of different identities concluded it refers to two different persons.

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

3. If a Member State authority has evidence to suggest that a green link recorded in the MID is factually inaccurate, not up-to-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 the SIS and shall, if necessary, rectify or erase the link from the MID without delay. That Member State authority shall inform the Member State responsible for the manual verification without delay.

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 shares the same biometric but similar or different identity data and the authority responsible for the verification of different identities concluded it refers to the same person in an unjustified manner;

(b) the linked data has the same, similar or different identity data and the same travel document data but different biometric data and the authority responsible for the verification of different identities concluded it refers to two different persons using the same travel document in an unjustified manner;

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

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

2. Where the CIR or the SIS are queried and where a red link exists between two or more of the information systems constituting the CIR or with the SIS, the MID shall reply indicating the data referred to in Article 34. Follow-up to a red link shall take place in accordance with Union and national law, basing any legal consequence for the person 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 from the EES, the VIS, the ETIAS, Eurodac or the ECRIS-TCN System, the individual file stored in the CIR shall be updated in accordance with Article 19(2).

4. Without prejudice to the provisions related to the handling of alerts in the SIS referred to in Regulations (EU) 2018/1860, 2018/1861 and 2018/1862, and without prejudice to limitations necessary to protect security and public order, prevent crime and guarantee that any national investigation will not be jeopardised, where a red link is created, the authority responsible for verification of different identities shall inform the person of the presence of multiple unlawful identities and shall provide the person in writing with a single identification number as referred to in Article 34(c), a reference to the authority responsible for the verification of different identities as referred to in Article 34(d) and the website address of the web portal established in accordance with Article 47a.

4a. The information shall be given by means of a standard form by the authority responsible for verification of different identities. The Commission shall determine the content of that form and the modalities for the information by implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

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

5a. Where a Member State authority or Union agency having access to CIR or SIS obtains evidence showing that a red link recorded in MID is incorrect or the data processed in MID, CIR and SIS is processed in breach of this Regulation, that authority shall:

- where the link relates to EU information systems, either rectify or erase the link from MID immediately, or

-where the link relates to one of the SIS alerts referred to in Article 29(2), inform the relevant SIRENE Bureau of the Member State that created the SIS alert immediately. That SIRENE Bureau shall verify the evidence provided by the Member State authority and where relevant rectify or erase the link from the MID immediately.

The Member State authority obtaining the evidence shall inform the Member State responsible for the manual verification without delay indicating where relevant any 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 shares the same biometric and the same or similar identity data;

(b) the linked data shares 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;

(ba) the linked data shares the same biometric, the same travel document data but similar identity data;

(c) the linked data shares the same biometric but similar or different identity data and the authority responsible for the verification of different identities concluded it refers to the same person having different identity data in a justified manner.

2. Where the CIR or the SIS are queried and where a white link exists between two or more of the EU information systems constituting the CIR or with the SIS, 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, hence triggering a match against the data that is subject to 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 from the EES, the VIS, the ETIAS, Eurodac or the ECRIS-TCN system, the individual file stored in the CIR shall be updated in accordance with Article 19(2).

4. Without prejudice to the provisions related to the handling of alerts in the SIS referred to in Regulations (EU) 2018/1860, 2018/1861 and 2018/1862, and without prejudice to limitations necessary to protect security and public order, prevent crime and guarantee that any national investigation will not be jeopardised, where a white link is created following a manual verification of multiple identities, the authority responsible for verification of different identities shall inform the person of the presence of similar identities and shall provide the person in writing with a single identification number as referred to in Article 34(c), a reference to the authority responsible for the verification of different identities as referred to in Article 34(d) and the website address of the web portal established in accordance with Article 47a.

4a. If a Member State authority has evidence to suggest that a white link recorded in the MID is factually inaccurate, not up-to-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 the SIS and shall, if necessary, rectify or erase the link from the MID without delay. That Member State authority shall inform the Member State responsible for the manual verification without delay.

4a. The information shall be given by means of a standard form by the authority responsible for verification of different identities. The Commission shall determine the content of that form and the modalities for the information by implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

Article 34

Identity confirmation file

The identity confirmation file shall contain the following data:

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

(b) a reference to the EU information systems whose data are linked;

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

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

(e) the date of creation or update of the link.

Article 35

Data retention in the multiple-identity detector

The identity confirmation files and their data, 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 and be deleted thereafter in an automated manner.

Article 36

Keeping of logs

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

(-a) the Member State launching the query;

(a) the purpose of access of the user;

(b) the date and time of the query;

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

(d) the reference to the data linked;

(e) the history of the identity confirmation file.

2. Each Member State and Union Agency shall keep logs of queries of the authority and the staff duly authorised to use the MID.

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, unless they are required for monitoring procedures that have already begun in which case they shall be erased once the monitoring procedures no longer require these logs.

CHAPTER VI
Measures supporting interoperability

Article 37

Data quality

1. In addition to Member States' responsibilities with regard to the quality of data entered into the systems, eu-LISA shall establish automated data quality control mechanisms and procedures on the data stored in the EES, the VIS, the ETIAS, the SIS, the shared BMS and the CIR.

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

Only data fulfilling the minimum quality standards may be entered in the EES, ETIAS, VIS, SIS, the shared BMS, the CIR and the MID.

3. eu-LISA shall provide regular reports on the automated data quality control mechanisms and procedures and the common data quality indicators to the Member States. eu-LISA shall also provide a regular report to the Commission covering the issues encountered and the Member States concerned. eu-LISA shall also provide that report to the European Parliament and 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 to store data in the EES, the VIS, the ETIAS, the SIS, the shared BMS and the CIR, in particular regarding biometric data, shall be laid down in implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

5. One year after the establishment of the automated data quality control mechanisms and procedures, common data quality indicators and the minimum quality standards and every year thereafter, the Commission shall evaluate Member State implementation of data quality and shall make any necessary recommendations. The Member States shall provide the Commission with an action plan to remedy any deficiencies identified in the evaluation report and, in particular, data quality issues deriving from erroneous data in existing EU information systems and 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, the European Data Protection Board and to the European Union Agency for Fundamental Rights established by Council Regulation (EC) No 168/2007.[36]

Article 38

Universal Message Format

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

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

3. (…)

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

Article 39

Central repository for reporting and statistics

1. A central repository for reporting and statistics (CRRS) is established for the purposes of supporting the objectives of the EES, the VIS, the ETIAS and the SIS, in accordance with the respective legal instruments, and to provide cross-system statistical data and analytical reporting for policy, operational and data quality purposes.

[36] 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. eu-LISA shall establish, implement and host the CRRS in its technical sites containing the data and statistics referred to in Article 63 of Regulation (EU) 2017/2226, Article 17 of Regulation (EC) No 767/2008, Article 84 of Regulation (EU) 2018/1240 and Article 54 of Regulation (EU) 2018/1861 and Article 16 of Regulation (EU) 2018/1860, logically separated. The data contained in the CRRS shall not enable the identification of individuals. Access to the CRRS shall be granted by means of secured access with control of access and specific user profiles, solely for the purpose of reporting and statistics, to the authorities referred to in Article 63 of Regulation (EU) 2017/2226, Article 17 of Regulation (EC) No 767/2008, Article 84 of Regulation (EU) 2018/1240 and Article 54 of Regulation (EU) 2018/1861.

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

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

4. The CRRS shall be composed of:

(-a) the tools necessary for anonymising data;

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

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

5. The Commission shall lay down detailed rules on the operation of the CRRS, including specific safeguards for processing of personal data referred to under paragraph 2 and 3 and security rules applicable to the repository by means of a delegated act adopted in accordance with the procedure referred to in Article 63.

CHAPTER VII
Data protection

Article 40

Data controller

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

2. In relation to the processing of data in the CIR, the Member State authorities that are controllers for the EES, the VIS and ETIAS, respectively, shall be controllers in accordance with Article 4(7) of Regulation (EU) 2016/679 in relation to data referred to in Article 18 that they enter into respective systems and shall have responsibility for the processing of 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 in accordance with Article 2(d) of Article 3(2)(b) 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 Article 4(7) of Regulation (EU) 2016/679 or Article 3(8) 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 45.

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 in accordance with Article 3(1)(a) 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 the application of 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;

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

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

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

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

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

(e) 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;

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

(g) 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;

(h) 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;

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

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

(i) 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

(…)

Article 44

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, 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 incident, 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.

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 specification 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 64(2).

Article 45

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 as referred to in Article 40 shall take the necessary measures to monitor the compliance of the data processing pursuant to this Regulation, including frequent verification of the logs referred to in Articles 10, 16, 24 and 36, and cooperate, where necessary, with the supervisory authorities referred to in Article 49 and with the European Data Protection Supervisor referred to in Article 50.

Article 45a

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 45b

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, 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 46

Right to information

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

1a. 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.

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

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

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

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

Article 47

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, 16, 17 and 18 of Regulation (EU) 2016/679, Articles 17, 18, 19 and 20 of Regulation (EU) 2018/1725 and Articles 14, 15 and 16 of Directive (EU) 2016/680 and, any person shall have the right to address himself or herself to the competent authority of any Member State, who shall examine and reply to the request.

2. The Member State which examined such 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 examined such 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 these replies are 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 controller shall inform the data subject of any such extension within 30 days of receipt of the request, 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 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 and ask for its opinion to be given 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 controller shall inform the data subject of any such extension within 30 days of receipt of the request, together with the reasons for the delay.

4a. 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 or where the ETIAS Central Unit was responsible for the manual verification-the Member State to which the request has been made shall correct or delete these data without any undue delay. The person concerned shall be informed in writing that his or her data has been rectified or erased.

5. Where data stored in the MID is amended by a Member State during its validity 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 shall be linked. Where the processing does not report any match, that Member State shall delete the data from the identity confirmation file. Where the automated processing reports one or several match(es), that Member State shall create or update the relevant link in accordance with the relevant provisions of this Regulation.

6. 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 correct or delete data relating to him or her.

7. This decision shall also provide the person concerned with information explaining the possibility to challenge the decision taken in respect of the request for access, rectification, restriction of processing or erasure 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 national supervisory authorities.

8. Any request for access, rectification, restriction of processing or erasure 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.

9. 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 record in the form of a written document that a request for access, rectification, restriction of processing or erasure of personal data was made and how it was addressed, and shall make that document available to national supervisory authorities without delay.

10. This article is without prejudice to the limitations and restrictions to the rights set out in this article which are provided for under Regulation 2016/679 and Directive (EU) 2016/680.

Article 47a

Web portal

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

2. The web portal shall contain information on the rights and procedures referred to in Article 46 and 47 and a user interface enabling persons whose data are processed in the MID and who were 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 verification of different identities.

3. In order to obtain the contact information of the competent authority of the Member State responsible for the verification of different identities, the person whose data are processed in the MID should enter the reference to the authority responsible for the 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 verification of different identities. The web portal shall also include a template e-mail to facilitate the communication between the user and the competent authority of the Member State responsible for the verification of different identities. Such e-mail shall include the single identification number referred to in Article 34(c) in order to allow the competent authority of the Member State responsible for the 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 as referred to in Articles 46 and 47 and shall regularly review whether these data 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 63 to adopt 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 to facilitate the communication between the user and the competent authority of the Member State responsible for the verification of different identities.

Article 48

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

Without prejudice to Article 65 of Regulation (EU) 2018/1240, Article 41 of Regulation (EU) 2017/2226, Article 31 of Regulation (EC) No 767/2008, and the querying of Interpol databases through the ESP in accordance with Article 9(5) of this Regulation which comply with the provisions of Chapter V of Regulation (EU) 2018/1725 and Chapter V of Regulation (EU) 2016/679, personal data stored in, processed or accessed by the interoperability components shall not be transferred or made available to any third country, to any international organisation or to any private party.

Article 49

Supervision by the supervisory authorities

-1. Each Member State shall ensure that the supervisory authority established in accordance with Article 51(1) of Regulation (EU) 2016/679 and Article 41(1) of Directive (EU) 2016/680 independently monitors the lawfulness of the processing of personal data referred to in this Regulation by the Member State concerned, including their transmission to and from the components of interoperability.

-1a. 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.

1. 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 referred to in Article 51(1) of Regulation (EU) 2016/679 and Article 41(1) of Directive (EU) 2016/680 shall publish annually the number of requests for rectification, erasure, or restriction of processing of data, the action subsequently taken and the number of rectifications, erasures and restrictions of processing made in response to requests by the persons concerned.

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

2a. 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 as laid down in this Regulation. Member States shall grant the supervisory authorities referred to in Article 51(1) of Regulation (EU) 2016/679 access to their logs as referred to in Articles 10, 16, 24 and 36, to their justification referred to in Article 22(3) and allow them to access all their premises used for interoperability purposes at all times.

Article 50

Audit 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, the Council, eu-LISA, the Commission, the Member States and 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 and the ETIAS Central Unit shall supply information requested by the European Data Protection Supervisor to it, give the European Data Protection Supervisor access to all the documents and to its logs as referred to in Articles 10, 16, 24 and 36 and allow the European Data Protection Supervisor access to all its premises at any time.

Article 51

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 national 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, 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 activities to the European Parliament, the Council, the Commission, Europol, the European Border and Coast Guard Agency and eu-LISA two years after entry into force of this Regulation and every two years thereafter. That report shall include a chapter on each Member State prepared by the supervisory authority of that Member State.

CHAPTER VIII
Responsibilities

Article 52

Responsibilities of eu-LISA during the design and development phase

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

2. The interoperability components shall be hosted by eu-LISA in its technical sites and shall provide the functionalities laid down in this Regulation in accordance with the conditions of security, availability, quality and performance referred to in Article 53(1).

3. eu-LISA shall be responsible for the development of the interoperability components, for any adaptations required for establishing interoperability between the central systems of the EES, VIS, ETIAS, SIS, Eurodac and the ECRIS-TCN system, and the ESP, the shared BMS, the CIR, the MID and the CRRS.

Without prejudice to Article 56, it shall not have access to any of the personal data processed through the ESP, the shared BMS, the CIR and the MID.

eu-LISA shall define the design of the physical architecture of the interoperability components including their communication infrastructures and the technical specifications and their evolution as regards the central infrastructure and the secure communication infrastructure, which shall be adopted by the Management Board, subject to a favourable opinion of the Commission. eu-LISA shall also implement any necessary adaptations to the EES, VIS, ETIAS or SIS deriving from the establishment of interoperability and provided for by this Regulation.

eu-LISA shall develop and implement the interoperability components as soon as possible after the entry into force of this Regulation and the adoption by the Commission of the measures provided for in Articles 8(2), 9(7), 28(5) and (6), 37(4), 38(4), 39(5), 44(5) and 68(7a).

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 65, 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 legislative 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.

The Programme Management Board shall every month submit to eu-LISA's Management Board written reports on progress of the project. 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 full information to non-participating Members of the Management Board.

The chairmanship shall be held by a Member State that is fully bound under Union law by the legislative instruments governing the development, establishment, operation and use of all the EU information systems.

All travel and subsistence expenses incurred by the members of the Programme Management Board shall be paid by the Agency, 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 65 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 53

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 maintenance and technological developments. In cooperation with the Member States, it shall ensure 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 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, in particular 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, controlled access, full, uninterrupted availability of the components and the data stored in the MID, sBMS and 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 entire 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 56, it 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 54

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(2) and 20(2a) in order to access the CIR for identification purposes;

(f) the manual verification of different identities referred to in Article 29;

(g) the compliance with data quality requirements established under Union law;

(ga) fully complying with the rules of each EU information system to ensure the security and integrity of personal data;

(h) 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 55

Responsibilities of the ETIAS Central Unit

The ETIAS Central Unit shall be responsible for:

(a) the manual verification of different identities referred to in Article 29;

(b) carrying out a multiple-identity detection between the data stored in the EES, VIS, Eurodac and the SIS referred to in Article 59.

CHAPTER IX
Amendments to other Union instruments

Article 55a

Amendments to Regulation (EC) No 767/2008

1) In Article 1, the following paragraph is added:

"2. By storing identity, travel document and biometric data in the common identity repository (CIR) established by [Article 17(1) of Regulation 2018/XX on interoperability], the VIS contributes to facilitating and assisting in the correct identification of persons registered in the VIS under the conditions and for the ultimate objectives referred to in [Article 20] of that Regulation."

2) In Article 4, the following points are added:

"(12) 'VIS data' means all data stored in the VIS Central System and in the CIR in accordance with Articles 9 to14.

"(13) 'identity data' means the data referred to in Article 9(4)(a) to (aa);

(14) ‘fingerprint data’ means the data relating to the five fingerprints of the index, middle finger, ring finger, little finger and the thumb from the right hand where present, and from the left hand;

"1a). The CIR shall contain the data referred to in Article 9(4)(a) to (c), 9(5) and 9(6), the remaining VIS data shall be stored in the VIS Central System."

4) Article 6(2) is amended as follows:

"2. Access to the VIS for consulting the data shall be reserved exclusively for the duly authorised staff of the national authorities of each Member State which are competent for the purposes laid down in Article 15 to 22, and for the duly authorised staff of the national authorities of each Member State and of the Union agencies which are competent for the purposes laid down in [Article 20 and Article 21 of the Regulation 2018/XX on interoperability], limited to the extent that the data are required for the performance of their tasks in accordance with those purposes, and proportionate to the objectives pursued."

5) Article 9(4) (a) to (c) is amended as follows:

"(a) surname (family name); first name or names (given names); date of birth; sex;

(aa) surname at birth (former surname(s)); place and country of birth; current nationality and nationality at birth;

(b) the type and number of the travel document or documents and the three-letter code of the issuing country of the travel document or documents;

(c) the date of expiry of the validity of the travel document or documents;

(cc) the authority which issued the travel document and its date of issue."

Article 55b

Amendments to Regulation (EU) 2016/399

Regulation (EU) 2016/399 is amended as follows:

In Article 8 of Regulation (EU) 2016/399, the following paragraph 4a is added:

"4a. The border guard shall consult the multiple-identity detector together with the common identity repository referred to in [Article 17(1) of Regulation 2018/XX on interoperability] or the Schengen Information System or both to assess the differences in the linked identity data and travel document data, and shall carry out any additional verification necessary to take a decision on the status and colour of the link.

In accordance with [Article 59(1) of Regulation 2018/XX], this paragraph shall apply only as from the start of operations of the multiple-identity detector."

Article 55c

Amendments to Regulation (EU) 2017/2226

Regulation (EU) 2017/2226 is amended as follows:

1) In Article 1, the following paragraph is added:

"1a. By storing identity, travel document and biometric data in the common identity repository (CIR) established by [Article 17(1) of Regulation 2018/XX on interoperability], the EES contributes to facilitating and assisting in the correct identification of persons registered in the EES under the conditions and for the ultimate objectives referred to in [Article 20] of that Regulation."

2) In Article 3, the following point is added:

"'CIR' means the common identity repository as referred to in [Article 17(1) ~~4(35)~~ of Regulation 2018/XX on interoperability]."

3) Article 3(1)(22) shall be replaced by the following:

"(22) 'EES data' means all data stored in the EES Central System and in the CIR in accordance with Articles 15 to 20.

4) In Article 3, a new point (22a) is added:

"(22a) 'identity data' means the data referred to in Article 16(1)(a), as well as the relevant data referred to in Articles 17(1) and 18(1);

5) In Article 6(1), the following point is inserted:

"(j) ensure the correct identification of persons."

6) Article 7(1)(a) is replaced by the following:

"(a) the common identity repository (CIR) as referred to in [Article 17(2)(a) of Regulation 2018/XX on interoperability];

(aa) a Central System (EES Central System);"

7) In Article 7(1), point (f) is replaced by the following:

"(f) a secure communication infrastructure between the EES Central System and the central infrastructures of the European search portal established by [Article 6(1)of Regulation 2018/XX on interoperability] and the common identity repository established by [Article 17(1) of Regulation 2018/XX on interoperability] ".

8) In Article 7, the following paragraph is added:

"1a. The CIR shall contain the data referred to in Article 16(1)(a) to (d), Article 17(1)(a) to (c) and Article 18(1) and (2), the remaining EES data shall be stored in the EES Central System.

9) In Article 9, the following paragraph is added:

"4. Access to consulting the EES data stored in the CIR shall be reserved exclusively for the duly authorised staff of the national authorities of each Member State and for the duly authorised staff of the Union agencies that are competent for the purposes laid down in [Article 20 and Article 21 of Regulation 2018/XX on interoperability]. That access shall be limited to the extent necessary for the performance of the tasks of those national authorities and Union agencies in accordance with those purposes and shall be proportionate to the objectives pursued."

10) In Article 21(1), the words "EES Central System" are replaced, every time they appear, by the words "EES Central System or the CIR".

11) In Article 21(2), the words "both the EES Central System and in the NUI" are replaced by the words "both the EES Central System and the CIR on the one hand and in the NUI on the other".

12) In Article 21(2), the words "shall be entered in the EES Central System" are replaced by the words "shall be entered in the EES Central System and the CIR".

12a) A new paragraph 2a is added to Article 23:

"2a. For the purpose of the verifications set out in paragraph 1, the border authority shall launch a query by using the European Search Portal defined in [Article 6(1) of the Interoperability Regulation] to compare the data on the third-country national with the relevant data of the EES and the VIS."

12b) Article 23(4) is replaced by the following:

"4. Where the search with the alphanumeric data set out in paragraph 2 of this Article indicates that data on the third- country national are not recorded in the EES, where a verification of the third-country national pursuant to paragraph 2 of this Article fails or where there are doubts as to the identity of the third-country national, the border authorities shall have access to data for identification in accordance with Article 27 of this Regulation in order to create or update an individual file in accordance with Article 14.

In addition to the identification referred to in first subparagraph of this paragraph, the following provisions shall apply:

(a) for third-country nationals who are subject to a visa requirement, if the search in the VIS with the data referred to in Article 18(1) of Regulation (EC) No 767/2008 indicates that data on the third-country national are recorded in the VIS, a verification of fingerprints against the VIS shall be carried out in accordance with Article 18(5) of Regulation (EC) No 767/2008. For this purpose, the border authority may launch a search from the EES to the VIS as provided for in Article 18(6) of Regulation (EC) No 767/2008. Where a verification of a third-country national pursuant to paragraph 2 of this Article failed, the border authorities shall access the VIS data for identification in accordance with Article 20 of Regulation (EC) No 767/2008.

(b) for third-country nationals who are not subject to a visa requirement and for whom no data are found in the EES further to the identification run in accordance with Article 27 of this Regulation, the VIS shall be consulted in accordance with Article 19a of Regulation (EC) No 767/2008. The border authority may launch a search from the EES to the VIS as provided for in Article 19a of Regulation (EC) No 767/2008."

13) A new paragraph (1a) is added to Article 32:

"1a. In cases where the designated authorities launched a query to the CIR in accordance with [Article 22 of Regulation 2018/XX on interoperability], they may access EES for consultation where the conditions laid down in this Article are met and where the reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on interoperability] reveals that data are stored in the EES."

14) (…)

15) (…)

16) A new paragraph is added to Article 33:

"1a. In cases where Europol launched a query to the CIR in accordance with [Article 22 of Regulation 2018/XX on interoperability], they may access EES for consultation where the conditions laid down in this Article are met and where the reply received as referred to in paragraph 3 of[Article 22 of Regulation 2018/XX on interoperability] reveals that data are stored in the EES."

17) (…)

18) In Article 34(1) and (2), the words "in the EES Central System" shall be replaced by the words "in the CIR and in the EES Central System respectively".

19) In Article 34(5), the words "of the EES Central System" shall be replaced by the words "from the EES Central System and from the CIR".

20) In Article 35, paragraph 7 is replaced by the following:

"The EES Central System and the CIR shall immediately inform all Member States of the erasure of EES or CIR data and where applicable remove them from the list of identified persons referred to in Article 12(3)."

21) In Article 36, the words "of the EES Central System" shall be replaced by the words "of the EES Central System and the CIR".

22) In Article 37(1), the words "development of the EES Central System", shall be replaced by the words "development of the EES Central System and the CIR".

23) In the first subparagraph of Article 37(3), the words "the EES Central System" shall be replaced, the first and the third time they appear, by the words "the EES Central System and the CIR".

24) In Article 46(1) the following point (f) is added:

"(f) a reference to the use of the European search portal to query the EES as referred to in [Article 7(2) of the Regulation 2018/XX on interoperability]."

25) Article 63(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 paragraph 1 in the central repository for reporting and statistics referred to in [Article 39 of the Regulation 2018/XX on interoperability]."

26) In Article 63(4) a new subparagraph is added:

"The daily statistics shall be stored in the central repository for reporting and statistics."

Article 55d

Amendments to Regulation (EU) 2018/1240

Regulation (EU) 2018/1240 is amended as follows:

1. In Article 1, the following paragraph is inserted:

"1a. By storing identity and travel document data in the common identity repository (CIR) established by [Article 17 of Regulation 2018/XX on interoperability], the ETIAS contributes to facilitating and assisting in the correct identification of persons registered in the ETIAS under the conditions and for the ultimate objectives referred to in Article 20 of that Regulation."

2. In Article 3(1), the following points are added:

"(23) 'CIR' means the common identity repository established by Article 17(1) of Regulation 2018/XX on interoperability];

(24) 'ETIAS Central System' means the Central System referred to in Article 6(2)(ab) together with the CIR to the extent that the CIR contains the data referred to in Article 6(2a);

(25) 'identity data' means the data referred to in points (a), (b) and (c) of Article 17(2);

(26) ‘travel document data’ means the data referred to in points (d) and (e) of Article 17(2) and the three letter code of the country issuing the travel document as referred to in point (c) of Article 19(3);".

3. In Article 4, the following point is added:

"(g) contribute to the correct identification of persons;".

4. In Article 6(2), point (a) is replaced by the following:

"(a) the CIR established by [Article 17 of Regulation 2018/XX on interoperability];".

5. In Article 6(2), the following point is inserted:

"(ab) a Central System, including the ETIAS watchlist referred to in Article 34;".

6. In Article 6(2), point (d) is replaced by the following:

"(d) a secure communication infrastructure between the Central System and the central infrastructures of the European search portal established by [Article 6(1) of Regulation 2018/XX on interoperability~~,~~ and the CIR established by [Article 17(1) of Regulation 2018/XX on interoperability];".

7. In Article 6, the following paragraph is inserted:

"2a. The CIR shall contain the identity and travel document data referred to in points (25) and (26) of Article 3(1) remaining data shall be stored in the Central System.".

8. Article 13 is amended as follows:

(a) the following paragraph is inserted:

"4a. Access to consulting the ETIAS identity and travel document data stored in the CIR shall also be reserved exclusively for the duly authorised staff of the national authorities of each Member State and for the duly authorised staff of the Union agencies that are competent for the purposes laid down in [Article 20 and Article 21 of Regulation 2018/XX on interoperability]. That access shall be limited to the extent necessary for the performance of the tasks of those national authorities and Union agencies in accordance with those purposes and shall be proportionate to the objectives pursued.";

(b) paragraph 5 is replaced by the following:

"5. Each Member State shall designate the competent national authorities referred to in paragraphs 1, 2, 4 and 4a and shall communicate a list of these authorities to eu-LISA without delay, in accordance with Article 87(2). That list shall specify for which purpose the duly authorised staff of each authority shall have access to the data in ETIAS Information System in accordance with paragraphs 1, 2, 4 and 4a.".

9. Article 17(2) is amended as follows:

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

"(a) surname (family name), first name(s) (given name(s)), surname at birth; date of birth, place of birth, sex, current nationality;";

(b) the following point is inserted:

"(ab) country of birth, first name(s) of the parents of the applicant;".

10. In Article 19(4) the words "point (a) of Article 17(2)" are replaced by the words "points (a) and (ab) of Article 17(2)".

11. Article 20 is amended as follows:

(a) in paragraph 2, the first subparagraph is replaced by the following:

"2. The ETIAS Central System shall launch a query by using the European Search Portal established by [Article 6(1) of the Interoperability Regulation] to compare the relevant data referred to in points (a), (ab), (b), (c), (d), (f), (g), (j), (k) and (m) of Article 17(2) and in Article 17(8) to the data present in a record, file or alert registered in an application file stored in the ETIAS Central System, SIS, the EES, VIS, Eurodac, Europol data and Interpol databases SLTD and TDAWN."

(b) In paragraph 4, the words "points (a), (b), (c), (d), (f), (g), (j), (k) and (m) of Article 17(2) and Article 17(8)" are replaced by the words "points (a), (ab), (b), (c), (d), (f), (g), (j), (k), (m) of Article 17(2) and Article 17(8)".

(c) In paragraph 5, the words "points (a), (c), (f), (h) and (i) of Article 17(2)" are replaced by the words "points (a), (ab), (c), (f), (h) and (i) of Article 17(2)".

12. In Article 23, paragraph 1 is replaced by the following:

"1. The ETIAS Central System shall launch a query by using the European Search Portal established by [Article 6(1) of the Interoperability Regulation] to compare the relevant data referred to in points (a), (ab), (b) and (d) of Article 17(2) to the data present in SIS in order to determine whether the applicant is the subject of one of the following alerts:

(a) an alert on missing persons;

(b) an alert on persons sought to assist with a judicial procedure;

(c) an alert on persons for discreet checks or specific checks.".

13. In Article 49(1), the words "points (a), (b), (c), (d) and (e) of Article 17(2) are replaced by the words "points (a), (ab), (b), (c), (d) and (e) of Article 17(2)".

14. In Article 52, the following paragraph is inserted:

"1a. In cases where the designated authorities launched a query to the CIR in accordance with [Article 22 of Regulation 2018/XX on interoperability], they may access the application files stored in the ETIAS Central System in accordance with this Article for consultation where the reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on interoperability] reveals that data is stored in the application files stored in the ETIAS Central System."

15. In Article 53, the following paragraph is inserted:

"1a. In cases where Europol launched a query to the CIR in accordance with [Article 22 of Regulation 2018/XX on interoperability], they may access the application files stored in the ETIAS Central System in accordance with this Article for consultation where the reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on interoperability] reveals that data is stored in the application files stored in the ETIAS Central System.".

16. In the fifth subparagraph of Article 65(3), the words "points (a), (b), (d), (e) and (f) of Article 17(2)" are replaced by the words "points (a), (ab), (b), (d), (e) and (f) of Article 17(2)".

17. In Article 69(1), the following point is inserted:

"(ca) where relevant, a reference to the use of the European search portal to query the ETIAS Central System as referred to in [Article 7(2) of the Regulation 2018/XX on interoperability,".

18. In Article 73(2), the words "the central repository of data" are replaced by the words "the central repository for reporting and statistics referred to in [Article 39 of the Regulation 2018/XX on interoperability] to the extent that it contains data obtained from the ETIAS Central System in accordance with Article 84".

19. In Article 74(1), the words "and the central repository of data, as referred to in Article 6" are deleted.

20. In Article 84(2), the first subparagraph is replaced by the following:

"2. For the purpose of paragraph 1, eu-LISA shall store the data referred to in paragraph 1 in the central repository for reporting and statistics referred to in [Article 39 of the Regulation 2018/XX on interoperability]. In accordance with [Article 39(1) of the Regulation 2018/XX on interoperability], cross-system statistical data and analytical reporting shall allow the authorities listed in paragraph 1 to obtain customisable reports and statistics, to support the implementation of the ETIAS screening rules referred to in Article 33, to improve the assessment of the security, illegal immigration and high epidemic risks, to enhance the efficiency of border checks and to help the ETIAS Central Unit and the ETIAS National Units process the travel authorisation applications.".

21. In Article 84(4), a second subparagraph is added:

"The daily statistics shall be stored in the central repository for reporting and statistics.".

Article 55e

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 eu-LISA's operational responsibility, eu-LISA, closely involving its Advisory Groups, shall establish for all systems under the Agency's operational responsibility automated data quality control mechanisms and procedures and common data quality indicators and the minimum quality standards to store data, in accordance with the relevant provisions of the systems' instruments and of [Article 37 of Regulation 2018/XX on interoperability].

2. eu-LISA shall establish a central repository containing only anonymised data for reporting and statistics subject to specific provisions in the legislative instruments governing the development, establishment, operation and use of large-scale IT systems managed by eu-LISA in accordance with [Article 39 of Regulation 2018/XX on interoperability]."

3. Article 19(1) is amended as follows:

(a) the following point is inserted:

"(eea) adopt the reports on the state of play of the development of the interoperability components pursuant to [Article 68(2) of Regulation 2018/XX on interoperability].";

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

"(ff) adopt the reports on the technical functioning of SIS II pursuant to Article 54(7) of Regulation 2018/1861 and Article 71(7) of Regulation 2018/1862, of 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 Regulation (EU) 2018/XX on the ECRIS-TCN system and the ECRIS reference implementation pursuant to Article 34(4) of Regulation (EU) 2018/XX] and of the interoperability components pursuant to [Article 68(4) of Regulation 2018/XX on interoperability];"

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

"(hh) adopt formal comments on the European Data Protection Supervisor's reports on the audits pursuant to Article 56(2) of Regulation (EU) 2018/1861, Article 42(2) of Regulation (EC) No 767/2008 and Article 31(2) of Regulation (EU) No 603/2013, Article 56(2) of Regulation (EU) 2017/2226, and Article 67 of Regulation (EU) 2018/1240 and to Article 27(2) of Regulation (EU) 2018/XX (establishing the ECRIS-TCN system) and to [Article 50 of Regulation 2018/XX on interoperability] 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 II 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 II (N.SIS II) and SIRENE Bureaux pursuant to Article 7(3) of Regulation (EU) 2018/1862 ~~06~~ and Article 7(3) of Regulation (EU) 2018/1861 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/…[+], [the list of competent authorities pursuant to Article 32 of Regulation (EU) 2018/… (ECRIS-TCN)] and the list of authorities pursuant to Article 61(1) of [Regulation (EU) 2018/… on interoperability]."

[+] OJ: Please insert serial number of the Regulation in 2016/0357A(COD).

4. 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 observers when a question concerning SIS in relation to the application of Regulation (EU) 2016/1624 is on the agenda. Europol may also attend the meetings of the Management Board as 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 also 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 also attend the meetings of the Management Board as observer when a question concerning ETIAS in relation with the application of Regulation (EU) 2018/1240 is on the agenda. EASO may also attend the meetings of the Management Board as an observer when a question concerning the automated system for registration, monitoring and the allocation mechanism for applications for international protection referred to in Article 44 of Regulation (EU) 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 (recast), is on the agenda.Eurojust, Europol, the European Public Prosecutor's Office may also attend the meetings of the Management Board as observers when a question concerning Regulation 2018/XX (establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS), and amending Regulation (EU) No 1077/2011 (ECRIS-TCN system) is on the agenda.] Europol, Eurojust and the European Border and Coast Guard Agency may also attend the meetings of the Management Board as observers when a question concerning [Regulation 2018/XX on interoperability] 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.".

5. In Article 24(3), point (p) is replaced by the following

"(p) without prejudice to Article 17 of the Staff Regulations, 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 2018/1240, Article 11(16) of Regulation 2018/XX (establishing the ECRIS-TCN system) and [Article 53(2) of Regulation 2018/XX on interoperability];".

6. In Article 23, paragraph 3 is replaced by the following:

(a) in paragraph 1, the following point is inserted:

"(e) Interoperability Advisory Group;";

(b) paragraph 3 is replaced by the following:

"3. Europol and 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 also appoint a representative to the ECRIS-TCN system Advisory Group. Europol, Eurojust and the European Border and Coast Guard Agency may each appoint a representative to the Interoperability Advisory Group.".

Article 55f

Amendments to Regulation (EU) 2018/1861

Regulation (EU) 2018/1861 is amended as follows:

1. In Article 3, the following points are added:

“(23) ‘ESP’ means the European search portal established by [Article 6(1) of Regulation 2018/XX on interoperability].

(24) ‘shared BMS' means the shared biometric matching service established by [Article 12(1) of Regulation 2018/XX on interoperability].

(25) 'CIR' means the common identity repository established by [Article 17(1) of Regulation 2018/XX on interoperability];

(26) ‘MID’ means the multiple-identity detector established by [Article 25(1) of Regulation 2018/XX on interoperability]."

2. Article 4 is amended as follows:

(a) in paragraph 1, the following point is added:

"(e) a secure communication infrastructure between CS-SIS and the central infrastructures of the ESP established by [Article 6(1) of Regulation 2018/XX on interoperability], the shared BMS established by [Article 12(1) of Regulation 2018/XX on interoperability] and the MID established by [Article 25(1) of Regulation 2018/XX on interoperability] ".

(b) the following paragraphs are added:

“8. Without prejudice to paragraphs 1 to 5, SIS data may also be searched via the ESP.

9. Without prejudice to paragraphs 1 to 5, SIS data may also be transmitted via the secure communication infrastructure defined in point (e) of paragraph 1. These transmissions shall be limited to the extent that the data are required for the functionalities referred to in [Regulation 2018/XX on interoperability]."

3. In Article 7, the following paragraph is inserted:

"2a. The SIRENE Bureaux shall also ensure the verification of different identities in accordance with [Article 29 Regulation 2018/XX on interoperability]. To the extent necessary to carry out this task, the SIRENE Bureaux shall have access to consulting the data stored in the CIR and the MID for the purposes laid down in [Articles 21 and 26 of Regulation 2018/XX on interoperability].".

4. In Article 12, paragraph 1 is replaced by the following:

“1. Member States shall ensure that every access to and all exchanges of personal data within CS-SIS are logged in their N.SIS for the purposes of checking whether or not the search is lawful, monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of N.SIS, data integrity and security. This does not apply to the automatic processes referred to in points (a), (b) and (c) of Article 4(4). Member States shall ensure that every access to personal data via the ESP are also logged for the purposes of checking whether or not the search is lawful, monitoring the lawfulness of data processing, self-monitoring, data integrity and security.”

5. In Article 34(1), the following point (g) is added:

“(g) verifying different identities and combating identity fraud in accordance with [Chapter V of Regulation 2018/XX on interoperability].”

6. In Article 60, paragraph 6 is replaced by the following:

"6. For the purpose of paragraphs 3, 4 and 5 and of Article 15(5), the Agency shall store data referred to in paragraph 3 and in Article 15(5) which shall not allow for the identification of individuals in the central repository for reporting and statistics referred to in [Article 39 of the Regulation 2018/XX on interoperability].

The Agency shall allow the Commission and the bodies referred to in paragraph 5 to obtain bespoke reports and statistics. Upon request, the Agency shall give access to Member States, the Commission, Europol, and the European Border and Coast Guard Agency to the central repository in accordance with [Article 39 of the Regulation 2018/XX on interoperability]."

Article 55g

Amendments to Council Decision 2004/512/EC

Council Decision 2004/512/EC establishing the Visa Information System (VIS) is amended as follows:

Article 1(2) is amended as follows:

"2. The Visa Information System shall be based on a centralised architecture and consist of:

a) the common identity repository as referred to in [Article 17(2)(a) of Regulation 2018/XX on interoperability],

b) a central information system, hereinafter referred to as 'the Central Visa Information System' (CS-VIS),

c) an interface in each Member State, hereinafter referred to as 'the National Interface' (NI-VIS) which shall provide the connection to the relevant central national authority of the respective Member State;

d) a communication infrastructure between the Central Visa Information System and the National Interfaces;

e) a Secure Communication Channel between the EES Central System and the CS-VIS;

f) a secure communication infrastructure between the VIS Central System and the central infrastructures of the European search portal established by [Article 6**(1)** of Regulation 2018/XX on interoperability], and the common identity repository established by [Article 17(1) of Regulation 2018/XX on interoperability]".

Article 55h

Amendments to Council Decision 2008/633/JHA

1) A new paragraph is added to Article 5:

"1a. In cases where the designated authorities launched a query to the CIR in accordance with [Article 22 of Regulation 2018/XX on interoperability], and where the conditions for access laid down in this Article are met, they may access VIS for consultation where the reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on interoperability] reveals that data is stored in the VIS."

2) A new point is added to Article 7:

"1a. In cases where Europol launched a query to the CIR in accordance with [Article 22 of Regulation 2018/XX on interoperability], and where the conditions for access laid down in this Article are met, Europol may access VIS for consultation where the reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on interoperability] reveals that data is stored in the VIS.".

CHAPTER X
Final provisions

Article 56

Reporting and statistics

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

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

(b) number of queries to each of the Interpol databases.

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 without enabling individual identification:

(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.

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 without enabling individual identification:

(a) (…)

(b) (…)

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

(d) the number of each type of link and the EU information systems between which each link was established;

(db) the period of time for which a yellow and red link remained in the system.

4. The duly authorised staff of the European Border and Coast Guard Agency established by Regulation (EU) 2016/1624 of the European Parliament and of the Council[37] shall have access to consult the data referred to in paragraphs 1, 2 and 3 for the purpose of carrying out risk analyses and vulnerability assessments as referred to in Articles 11 and 13 of that Regulation.

4a. The duly authorised staff of Europol shall have access to consult the data referred to in paragraphs 2 and 3 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.

5. For the purpose of paragraphs 1, 2 and 3 of this Article, eu-LISA shall store the data referred to in paragraph 1, 2 and 3 of this Article in the central repository for reporting and statistics referred to in Chapter VII of this Regulation. The data included in the repository shall not enable the identification of individuals, but it shall allow the authorities listed in paragraph 1, 2 and 3 of this Article to obtain customisable reports and statistics to enhance the efficiency of border checks, to help authorities processing visa applications and to support evidence-based policymaking on migration and security in the Union.

---

[37] 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).

5a. Upon request, relevant information shall be made available by the Commission to the Agency for Fundamental Rights in order to evaluate the impact on fundamental rights of this Regulation.

Article 57

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 a adopt a delegated act in accordance with Article 63 to once extend the period referred to in paragraph 1 by no longer than 1 year when an assessment of the practical implementation of the ESP showed that it is necessary to extend this period especially because of the impact of the introduction of the ESP on the organisation and duration of border checks.

Article 58

Transitional period applicable to the provisions on access to the common identity repository for purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences

Article 22, points 13, 14, 15, 16 and 16a of Article 55c, Article 55h and points 14 and 15 of Article 15f shall apply from the date of the start of operations referred to in Article 62(1).

Article 59

Transitional period for the multiple-identity detection

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

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

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

Where several matches are reported, a link shall be created to 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 information systems to the ETIAS Central Unit.

4. Where a link is created to an alert in the SIS, other than a refusal of entry or return alert or an alert on a travel document reported lost, stolen or invalidated in accordance with Article 3 of Regulation (EU) 2018/1860, Articles 24 and 25 of Regulation (EU) 2018/1861 and Article 38 of Regulation (EU) 2018/1862 respectively, the MID shall grant access to the identity data present in the different information systems to the SIRENE Bureau of the Member State that created the alert.

5. The ETIAS Central Unit or the SIRENE Bureau of the Member State that created the alert shall have access to the data contained in the identity confirmation file and shall assess the different identities and shall update the link in accordance with Articles 31 to 33 and add it to the identity confirmation file.

5a. The ETIAS Central Unit shall only notify the Commission in accordance with Article 61(3) once all yellow links have been verified and updated either into green, white or red links.

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

The Commission is empowered to adopt a delegated act in accordance with Article 63 to extend the period referred to in paragraph 1 by six months, renewable twice by six months each time. Such extension shall only be granted where an assessment of the estimated completion time for the multiple-identity detection referred to in this Article, carried out no later than three months before the expiry of either the deadline referred to in paragraph 1 or the deadline of the first two extensions, demonstrates that such deadline cannot be met for reasons independent of the ETIAS Central Unit and that no corrective measures can be applied.

Article 60

Costs

1. The costs incurred in connection with the establishment and operation of the ESP, the 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.

2a. 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 will be mobilised from the envelope of EUR 791 million foreseen under Article 5(5) point (b) of the ISF Borders and Visa Regulation[38] to cover the costs of implementation of this Regulation, as foreseen under paragraphs 1 and 2.

2b. From the envelope referred to in the preceding paragraph, EUR 22.861.000 will be allocated to eu-LISA, EUR 9.072.000 will be allocated to Europol, and EUR 144.000 will be allocated to CEPOL, to support these agencies in performing their respective tasks in line with the requirements of this Regulation. Such funding shall be implemented under indirect management.

3. The costs incurred by the designated authorities referred to in Article 4(24) shall be borne, respectively, by each Member State and Europol. The costs for the connection of the designated authorities to the CIR shall be borne by each Member State and Europol, respectively.

Article 61

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 62. 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 test referred to in Article 62(1)(b).

3. The ETIAS Central Unit shall notify the Commission of the successful completion of the transitional measure laid down in Article 59.

[38] 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 (OJ L 150, 20.5.2014, p. 143).

4. The Commission shall make available to the Member States and the public, by a constantly updated public website, the information notified pursuant to paragraph 1.

Article 62

Start of operations[39]

1. The Commission shall determine the date from which the ESP is to start operations by means of an implementing act when the following conditions are met:

(a) the measures referred to in Articles 8(2), 9(7) and 44(5) have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the ESP, which is to be conducted by eu-LISA in cooperation with the Member States 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 Articles 8(1) and has notified them to the Commission;

The ESP shall only query the Interpol databases where the technical arrangements allow to fulfil the requirements referred to in Article 9(5). The impossibility to fulfil this requirement shall result in the ESP not querying the Interpol databases but shall not delay the start of operations of the ESP.

The date referred to in the first subparagraph shall be set for within 30 days from the decision of the Commission.

1a. The Commission shall determine the date from which the sBMS is to start operations by means of an implementing act when the following conditions are met:

(a) the measures referred to in Articles 13(5) and 44(5) have been adopted;

[39] With regards to the Commission decision by implementing act, a corresponding recital needs to be added during the lawyers-linguist revision.

(b) eu-LISA has declared the successful completion of a comprehensive test of the sBMS, which is to be conducted by eu-LISA in cooperation with the Member States;

(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 1d(b).

The date referred to in the first subparagraph shall be set for within 30 days from the decision of the Commission.

1b. The Commission shall determine the date from which the CIR is to start operations by means of an implementing act when the following conditions are met:

(a) the measures referred to in Articles 44(5) and 68(7a) have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the CIR, which is to be conducted by eu-LISA in cooperation with the Member States;

(c) eu-LISA has validated the technical and legal arrangements to collect and transmit the data referred to in Article 18 has notified them to the Commission;

(d) eu-LISA has declared the successful completion of the test referred to in paragraph 1d(b).

The date referred to in the first subparagraph shall be set for within 30 days from the decision of the Commission.

1c. The Commission shall determine the date from which the MID is to start operations by means of an implementing act when the following conditions are met:

(a) the measures referred to in Articles 28(5), 28(7), 32(4a), 33(4a), 44(5) and 47a(6) have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the MID, which is to be conducted by eu-LISA in cooperation with the Member States 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 as referred to in Article 61(3);

(e) eu-LISA has declared the successful completion of the tests referred to in paragraphs 1(b), 1a(b), 1b(b) and 1d(b).

The date referred to in the first subparagraph shall be set for within 30 days from the decision of the Commission.

1d. The Commission shall decide the date from which the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum quality standards are to be used by means of implementing acts when the following conditions are 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 quality standards, which is to be conducted by eu-LISA in cooperation with the Member States.

The date referred to in the first subparagraph shall be set for within 30 days from the decision of the Commission.

1e. (…)

1f. The Commission shall decide the date from which the CRRS is to start operations by means of an implementing act when the following conditions are met:

(a) the measures referred to in Articles 39(5) and 44(5) have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the CRRS, which is to be conducted by eu-LISA in cooperation with the Member States;

(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 date referred to in the first subparagraph shall be set for within 30 days from the decision of the Commission.

2. The Commission shall inform the European Parliament and the Council of the results of the test carried out pursuant to paragraphs 1(b), 1a(b), 1b(b), 1c(b) 1d(b), 1e(b) and 1f(b).

3. The Commission decisions referred to in paragraphs 1, 1a, 1b, 1c, 1d, 1e and 1f shall be published in the Official Journal of the European Union.

4. The Member States, the ETIAS Central Unit and Europol shall start using the each of interoperability components from the date determined by the Commission in accordance with respectively paragraphs 1,1a, 1b and 1c.

Article 63

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), 47a(6), 57(2) and 59(10) shall be conferred on the Commission for a period of five years from [*the date of entry into force of this Regulation*]. 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.

The delegation of power referred to in Articles 28(5), 39(5), 47a(6), 57(2) and 59(10) 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 on Better Law-Making of 13 April 2016.

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

A delegated act adopted pursuant to Articles 28(5), 39(5), 47a (6), 57(2) and 59(10) 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 64

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 65

Advisory group

An Advisory Group shall be established by eu-LISA. During the design and development phase of the interoperability instruments, Article 52(4) to (6) shall apply.

Article 66
Training

1. eu-LISA shall perform tasks related to the provision of training on the technical use of the interoperability components in accordance with Regulation (EU) No 1077/2011.

Member States and Union agencies shall provide their staff authorised to process data from the interoperability components, with appropriate training programme about data security, data quality, data protection rules, the procedures of the data processing and obligations to inform in accordance with Article 32, 33 and 46.

Where appropriate, common training courses on these topics shall be organised at Union level to enhance cooperation and exchange of best practices between staff of Member States and Union agencies which are authorised to process data from the interoperability components. Particular attention shall be paid to the process of multiple-identity detection, including the verification of links and the accompanying need to ensure the safeguards in relation to fundamental rights.

Article 67

Practical handbook

The Commission shall, in close cooperation with the Member States, eu-LISA and other relevant 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 68

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 [*Six months after the entry into force of this Regulation — OPOCE, please replace with the actual date*] and every six months thereafter during the development phase of the interoperability components, eu-LISA shall submit a report to the European Parliament and the Council on the state of play of the development of the interoperability components, 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 the Council explaining in detail how the objectives, in particular relating to planning and costs, were achieved as well as justifying any divergences.

3. (…)

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

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

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

(b) an examination of the results achieved against objectives and the impact on fundamental rights, including in particular an assessment of the impact of the interoperability components on the right to non-discrimination;

(ba) an assessment of the functioning of the web portal, including figures regarding the use of the web portal and the number requests that were resolved;

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

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

(da) an assessment of the use of the CIR for identification;

(db) an assessment of the use of the CIR for preventing, detecting or investigating terrorist offences or other serious criminal offences;

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

(ea) 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.

By one year after the entry into force of this Regulation and every year thereafter until the decisions of the Commission referred to in Article 62 have been taken, the Commission shall submit a report to the European Parliament and 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.

The Commission shall produce an examination of the impact of the MID on the right to non-discrimination two years after the start of operations of the MID. 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 point (b) of paragraph 5.

The evaluations shall include any necessary recommendations. The Commission shall transmit the evaluation report to the European Parliament, to the Council, to the European Data Protection Supervisor and to the European Union Agency for Fundamental Rights established by Council Regulation (EC) No 168/2007.[40]

6. The Member States and Europol shall provide eu-LISA and the Commission with the information necessary to draft the reports referred to in paragraphs 4 and 5. This information shall not jeopardise working methods or include information that reveals sources, staff members or investigations of the designated authorities.

7. eu-LISA shall provide the Commission with the information necessary to produce the evaluations referred to in paragraph 5.

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

8. While respecting the provisions of national law on the publication of sensitive information, and without prejudice to limitations necessary to protect security and public order, prevent crime and guarantee that any national investigation will not be jeopardised, each Member State and Europol shall prepare annual reports on the effectiveness of access to data stored in the CIR for purposes of preventing, detecting or investigation terrorist offences or other serious criminal offences, containing information and statistics on:

(a) the exact purpose of the consultation including the type of terrorist or serious criminal offence;

(b) reasonable grounds given for the substantiated suspicion that the suspect, perpetrator or victim is covered by Regulation (EU) 2017/2226, Regulation (EC) No 767/2008 or Regulation (EU) 2018/1240;

(c) the number of requests for access to the CIR for purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences;

(d) the number and type of cases that have ended in successful identifications;

(e) the need and use made of the exceptional case of urgency including those cases where that urgency was not accepted by the ex post verification carried out by the central access point.

7a. A technical solution shall be made available to Member States in order to manage users access requests referred to in Article 22 and to facilitate the collection of the data listed in this paragraph for the purpose of generating statistics referred to in this paragraph. The Commission shall adopt implementing acts concerning the specifications of the technical solution. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

Member State and Europol annual reports shall be transmitted to the Commission by 30 June of the subsequent year.

Article 69

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, the sBMS, the CIR, the MID, the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum quality standards and the CRRS shall apply from the date determined by the Commission respectively in Article 62(1), 62(1a), 62(1b), 62(1c), 62(1d), 62(1e) and 62(1f) with the exception of Articles 6, 12, 17, 25, 38, 42, 52, 54, 55, 60, 61, 63, 64, 65, 67 and 68(1), which shall apply from [*the data of entry into force of this Regulation*].

The provisions relating to the Eurodac shall apply from the date the recast of Regulation (EU) No 603/2013 of the European Parliament and of the Council becomes applicable.

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

Done at Strasbourg,

For the European Parliament

The President

For the Council

The President

ANNEX II

2017/0352 (COD)

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulation (EU) 2018/1726, Regulation (EU) 2018/1862 and Regulation (EU) 2018/XX [the ECRIS-TCN Regulation]

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,

After consulting the European Data Protection Supervisor,

Having regard to the opinion of the European Economic and Social Committee,[41]

Acting in accordance with the ordinary legislative procedure,

[41] OJ C , , p. .

Whereas:

(1) In its Communication of 6 April 2016 entitled Stronger and Smarter Information Systems for Borders and Security[42], 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 the interoperability between EU information systems for security, border and migration management, with the aim to address the structural shortcomings related to these 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[43], 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[44], 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) The European Council of 15 December 2016[45] called for continued delivery on the interoperability of EU information systems and databases.

(5) In its final report of 11 May 2017[46], the high-level expert group on information systems and interoperability concluded that it is necessary and technically feasible to work towards practical solutions for interoperability and that they can, in principle, both deliver operational gains and be established in compliance with data protection requirements.

---

42 COM(2016)205, 6.4.2016.

43 Roadmap of 6 June 2016 to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area — 9368/1/16 REV 1.

44 European Parliament resolution of 6 July 2016 on the strategic priorities for the Commission Work Programme 2017 (2016/2773(RSP)).

45 http://www.consilium.europa.eu/en/press/press-releases/2016/12/15/euco-conclusions-final/.

46 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

(6) In its Communication of 16 May 2017 entitled Seventh progress report towards an effective and genuine Security Union[47], the Commission set out, in line with its Communication of 6 April 2016 and confirmed by 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 where all EU information systems for security, border and migration management are interoperable in full respect of fundamental rights.

(7) In its Conclusions of 9 June 2017[48] 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 as proposed by the high-level expert group.

(8) The European Council of 23 June 2017[49] underlined the need to improve the interoperability between databases and invited the Commission to prepare, as soon as possible, draft legislation enacting the proposals made by the high-level expert group on information systems and interoperability.

(9) With a view to improve the effectiveness and efficiency of checks at the external borders, to contribute to preventing and combating illegal immigration and to contribute to a high level of security within the area of freedom, security and justice of the Union, including the maintenance of public security and public policy and safeguarding the security in the territories of the Member States, to improve the implementation of the common visa policy, to assist in examining applications for international protection, to contribute in the prevention, detection and investigation of terrorist offences or other serious criminal offences, to aid in the identificaton of unknown persons who are unable to identify themselves or unidentified human remains in cases of natural disasters, accidents or terrorist attacks, 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 the individual, 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.

---

47 COM(2017) 261 final, 16.5.2017.

48 http://www.consilium.europa.eu/media/22186/st10136en17-vf.pdf.

49 European Council conclusions, 22-23 June 2017.

(10) The interoperability between the EU information systems should allow said systems to supplement each other in order to facilitate the correct identification of persons, including unknown persons who are not able to identify themselves or unidentified remains, contribute to fighting identity fraud, improve and harmonise 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 the access for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences to the EES, the VIS, the ETIAS and Eurodac, and support the purposes of the EES, the VIS, the ETIAS, Eurodac, the SIS and the ECRIS-TCN system.

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

(12) The interoperability components should concern persons in respect of whom personal data may be processed in the EU information systems and by Europol, namely persons whose personal data are processed in the EU information systems and by Europol.

(13) The European search portal (ESP) should be established to facilitate technically the ability of Member State authorities and Union agencies to have fast, seamless, efficient, systematic and controlled access to the EU information systems, the Europol data and the Interpol databases insofar as this is needed to perform their tasks, in accordance with their access rights, and to support the objectives of the EES, the VIS, the ETIAS, Eurodac, the SIS, the ECRIS-TCN system and the Europol data. Enabling the simultaneous querying of all relevant EU information systems in parallel, as well as of the Europol data and the Interpol databases, the ESP should act as a single window or 'message broker' to search 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.

(13a) When querying the Interpol databases, the design of the ESP should ensure that the data used by the user of the ESP to launch a query is not shared with the owners of Interpol data. The design of the ESP shall also ensure that the Interpol databases are only queried in accordance with applicable Union and national law.

(14) Those European search portal (ESP) end-users that have the right to access Europol data under Regulation (EU) 2016/794 of the European Parliament and of the Council[50] should be able to query the 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.

(15) The European search portal (ESP) should be developed and configured in such a way that it does not allow the use of fields of data for the query that are not related to persons or travel documents or that are not present in an EU information system, in the Europol data or in the Interpol database.

(16) To ensure the systematic use of the relevant EU information systems, the European search portal (ESP) should be used to query the common identity repository, the EES, the VIS, the ETIAS, Eurodac and the ECRIS-TCN system. However, the 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 the Central SIS in accordance with their access rights and in order to perform their tasks. The ESP should be an additional means to query the Central SIS, the Europol data and the Interpol systems, complementing the existing dedicated interfaces.

(17) Biometric data, such as fingerprints and facial images, are unique and therefore much more reliable than alphanumeric data for identifying a person. The shared biometric matching service (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 may be registered in different databases, by matching their biometric data across different systems and by relying on one unique technological component instead of five different ones in each of the underlying systems. 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, the VIS and the 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, facilitating cross-system comparisons using biometric templates and enabling economies of scale in developing and maintaining the EU central systems.

---

[50] 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).

(17a) The biometric templates stored in the shared BMS which are comprised of data derived from a feature extraction of actual biometric samples should be obtained in such a way that reverting the 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 the SIS, are only used for SIS purposes and cannot be used to be cross-checked with data present in other information systems, in line with the principles of necessity and proportionality, the shared BMS should not store DNA profiles or biometric templates obtained from palm print data.

(18) Biometric data constitute sensitive personal data. This R~~r~~egulation should lay down the basis for and the safeguards for processing of such data for the purpose of uniquely identifying the persons concerned.

(19) The systems established by Regulation (EU) 2017/2226 of the European Parliament and of the Council[51], Regulation (EC) No 767/2008 of the European Parliament and of the Council[52], Regulation (EU) 2018/1240, the system established by the Eurodac Regulation and the system established by the ECRIS-TCN Regulation require the accurate identification of the persons whose personal data are stored therein.

(20) The common identity repository (CIR) should therefore facilitate and assist in the correct identification of persons registered in the EES, the VIS, the ETIAS, Eurodac and the ECRIS-TCN system.

---

51 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).

52 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).

(21) Personal data stored in these EU information systems may relate to the same person 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. The common identity repository (CIR) should store the personal data concerning persons present in the systems that are necessary to enable the more accurate identification of those individuals, therefore including their identity, travel document and biometric data, regardless of the system in which the data was 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 ~~is~~ deleted in the underlying systems in accordance with their logical separation.

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

(23) In that connection, creating an individual file in the common identity repository (CIR) for each person that is recorded in the EES, the VIS, the ETIAS, Eurodac or the ECRIS-TCN system, is necessary to achieve the purpose of correct identification within the Schengen area, and to support the multiple-identity detector for the dual purpose of facilitating identity checks for bona fide travellers and combating identity fraud. The individual file should store in one single place and make accessible to the duly authorised end-users all the possible identities linked to a person.

(24) The common identity repository (CIR) should thus support the functioning of the multiple-identity detector and to 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, investigation or detection of serious crime.

(25) The common identity repository (CIR) should provide for a shared container for identity, travel document and biometric data of persons registered in the EES, the VIS, the ETIAS, Eurodac and the ECRIS-TCN system. It should be part of the technical architecture of these systems and serve as the shared component between them for storage of the identity, travel document and biometric data, and to allow their querying.

(26) All records in the common identity repository (CIR) should be logically separated by automatically tagging each record with the underlying system owning that record. The access control of the CIR should use these tags to allow the record to be accessible or not.

(27) 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 and provide 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 interest of the child.

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

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

(30) This Regulation should also introduce a new possibility for streamlined access to data beyond identity data or travel document data present in the EES, the VIS, the ETIAS or Eurodac by Member State designated authorities responsible for preventing, detecting or investigating terrorist offences or other serious criminal offences and Europol. Data, including data other than identity data or travel document data contained in those systems, 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 consultation will contribute to the prevention, detection or investigation of the criminal offences or other serious criminal offences in question, 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.

(31) Full access to the necessary data contained in the EU information systems necessary for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences, beyond the relevant identity data or travel document data covered under common identity repository (CIR), should continue to be governed by the provisions in the respective 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 in the conduct of their tasks. The end-user authorised by the designated authority should therefore be allowed to see in which of the EU information systems the data corresponding to the query introduced are recorded. The concerned system would thus be flagged following the automated verification of the presence of a match in the system (a so-called match-flag functionality).

(31a) The reply will not be interpreted and used as a ground or reason to draw conclusions on or undertake measures towards 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 legislative instruments governing such access. Any such act will be subject to measures set out in Chapter VII and measures in Regulation (EU) 2016/679, Directive (EU) 2016/680 or Regulation (EU) 2018/1725.

(31b) As a general rule, where a match-flag indicates that the data are recorded in the 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.

(32) The logs of the queries of the common identity repository should indicate the purpose of the query. 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, therefore indicating that such query was launched for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences.

(33) The query of the common identity repository (CIR) by Member State designated authorities and Europol in order to obtain a match-flag type of response indicating the data are recorded in the EES, the VIS, the ETIAS or Eurodac requires automated processing of personal data. A match-flag would 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 concerned individual 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 would therefore realise a very limited interference with the right to protection of personal data of the concerned individual, while it would be necessary to allow the designated authority and Europol to address its request for access to personal data more effectively directly to the system that was flagged as containing it.

(34) (…)

(35) The multiple-identity detector (MID) should be established to support the functioning of the common identity repository and to support the objectives of the EES, the VIS, the ETIAS, Eurodac, the SIS and the ECRIS-TCN system. 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 therein.

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

(37) The multiple-identity detector (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 the links between individuals present in more than one EU information system, strictly limited to the data necessary to verify that a person is recorded in a justified or unjustified manner under different biographical identities in different systems, or to clarify that two persons having similar biographical data may not be the same person. Data processing through the European search portal (ESP) and the shared biometric matching service (shared BMS) in order to link individual files across individual systems should be kept to an absolute minimum and therefore is limited to a multiple-identity detection at the time new data are ~~is~~ added to one of the information systems included in the common identity repository and in the SIS. The MID should include safeguards against potential discrimination or unfavourable decisions for persons with multiple lawful identities.

(38) 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. 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, the effective implementation of the Union's asylum and visa policies.

(39) The European search portal (ESP) and shared biometric matching service (shared BMS) should compare data in common identity repository (CIR) and SIS on persons when new records are created or uploaded by a national authority or an Union agency. Such comparison should be automated. The CIR and the SIS should use the shared BMS to detect possible links on the basis of biometric data. The CIR and the SIS should use the ESP to detect possible links on the basis of alphanumeric data. The CIR and the SIS should be able to identify identical or similar data on the 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 the 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 concerned person.

(40) The national authority or Union agency that recorded the data in the respective EU information system should confirm or change these links. This authority should have access to the data stored in the common identity repository (CIR) or the SIS and in the multiple-identity detector (MID) for the purpose of the manual identity verification.

(41) (…)

(42) The manual verification of multiple identities should be ensured by the authority creating or updating the data that triggered a match resulting in a link with data already stored in another EU information system. The authority responsible for the verification of multiple identities should assess whether there are multiple identities referring to the same person in a justified or unjustified manner. Such assessment should be performed where possible in the presence of the persons and where necessary by requesting additional clarifications or information. Such assessment should be performed without delay, in line with legal requirements for the accuracy of information under Union and national law. ~~Especially at borders,~~ The persons involved would be restricted in their movement for the duration of the verification which should not last indefinitely. The existence of a yellow link in the MID should not constitute in itself a ground for refusal of entry and any decision on authorising or refusing entry should exclusively be taken on the basis of the applicable provisions of the Schengen Borders Code or national law as appropriate.

(43) For the links obtained in relation to the Schengen Information System (SIS) related to the alerts in respect of persons wanted for arrest or 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 verification of multiple identities should be the SIRENE Bureau of the Member State that created the alert. Indeed those categories of SIS alerts are sensitive and should not necessarily be shared with the authorities creating or updating the data 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 the SIS Regulations.

(43a) The creation of those links requires transparency towards the individuals affected. In order to facilitate the implementation of the necessary safeguards in accordance with Union data protection rules, individuals who are subject to a red link or a white link following manual verification should be informed in writing without prejudice to limitations to protect security and public order, prevent crime and guarantee that any national investigation will not be 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.

(43b) In addition to the access to the MID foreseen for the authority responsible for the verification of multiple identities where a yellow link is created, access to the MID by Member State authorities and Union agencies having access to at least one EU information system included in the CIR or to the SIS is foreseen where a red link exists. The red links indicates that a person is using different identities in an unjustified manner or that a person is using somebody else's identity.

(43c) Access to the MID by Member State authorities and Union agencies is also foreseen where a white or green link exists between data from two EU information systems where such authority has access to both information systems. Such access is granted for the sole purpose of allowing that Member State authority or Union agency to detect potential cases where the link was incorrect or that the data processed in the MID, CIR and SIS were processed in breach of this Regulation and take necessary actions to correct the situation and replace the link.

(44) eu-LISA should establish automated data quality control mechanisms and common data quality indicators. eu-LISA should be responsible to develop a central monitoring capacity for data quality and to produce regular data analysis reports to improve the control of implementation and application by Member States of EU information systems. The common quality indicators should include the minimum quality standards to store data in the EU information systems or the interoperability components. The goal of such a data quality standards should be for the EU information systems and interoperability components to automatically identify apparently incorrect or inconsistent data submissions so that the originating Member State is able to verify the data and carry out any necessary remedial actions.

(45) The Commission should evaluate eu-LISA 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.

(46) The Universal Message Format (UMF) should establish a standard for structured, cross-border information exchange between information systems, authorities and/or organisations in the field of Justice and Home affairs. 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 the exchange in a consistent and semantically equivalent manner.

(46a) The implementation of the UMF standard may be considered in the VIS, the SIS and in any existing or new cross-border information exchange models and information systems in the area of Justice and Home Affairs, developed by Member States.

(47) 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 respective legal instruments. eu-LISA should establish, implement and host the CRRS in its technical sites containing anonymous statistical data from the above-mentioned systems, the common identity repository, the multiple-identity detector and the shared biometric matching service. 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.

(48) Regulation (EU) 2016/679 should apply to the processing of personal data 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, in which case Directive (EU) 2016/680 of the European Parliament and of the Council should apply.

(48a) Where the processing of personal data by the Member States for the purpose of interoperability 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.[53]

[53] The following recital has been included as part of the political agreement in the ETIAS file: "Where the processing of personal data by the Member States for the purpose of assessing applications 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."

(48b) Regulation (EU) 2016/679 or, where relevant, Directive (EU) 2016/680 should also apply to the transfers of personal data to third countries or international organisations carried out in accordance with 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.

(49) The specific provisions on data protection of Regulation (EU) 2017/2226, Regulation (EC) No 767/2008, Regulation (EU) 2018/1240, and Regulation (EU) 2018/1861 should apply to the processing of personal data in those respective systems.

(50) Regulation (EU) 2018/1725 should apply 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 should apply to the processing of personal data by Europol.

(51) The national supervisory authorities established in accordance with Regulation (EU) 2016/679 or Directive (EU) 2016/680 should monitor the lawfulness of the processing of personal data by the Member States, whilst the European Data Protection Supervisor as established by Regulation (EU) 2018/1725 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 him under this Regulation, sufficient resources, including both human and financial resources, are required.

(52) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 16 April 2018.

(52a) The Article 29 Data Protection Working Party provided an opinion on the Commission proposal on 11 April 2018.

(53) (…)

(54) 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 regarding the development, design and management of the interoperability components. eu-LISA obligations in this respect should include adopting the measures necessary to prevent access by unauthorised persons, such as staff of external service providers, to personal data processed through the interoperability components. When awarding contracts for the provision of services, the Member States and eu-LISA should consider any measures necessary to secure compliance with laws or regulations relating to the protection of personal data and the privacy of individuals or to safeguard essential security interests, in line with the Financial regulation and applicable international conventions. eu-LISA should apply the principles of privacy by design and by default during the development of the interoperability components.

(55) The implementation of the interoperability components provided for in this Regulation will have an impact on the way checks are carried out at border crossing points. These impacts will result from a combined application of the existing rules of Regulation (EU) 2016/399 of the European Parliament and of the Council[54] and the rules on interoperability provided for in this Regulation.

(56) As a consequence of this combined application of the rules, the European search portal (ESP) should constitute the main access point for the compulsory systematic consultation of databases for persons at border crossing points provided for by the Schengen Borders Code. In addition, the identity data or travel document data that led to the classification of a link in the multiple-identity detector (MID) as a red link should be taken into account by the border guards for assessing whether or not the person fulfils the conditions of entry defined in the Schengen Borders Code. However the presence of a red link should not in itself constitute a ground for refusal of entry and the existing grounds for refusal of entry listed in the Schengen Borders Code should therefore not be amended.

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

(58) (…)

---

54 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, OJ L 77, 23.3.2016, p.1.

(59) Should the query of the multiple-identity detector (MID)[55] through the European search portal (ESP) result in a yellow link or detect a red link, the border guard should consult the common identity repository or the Schengen Information System or both in order to assess the information on the person being checked, to manually verify his/her different identity and to adapt the colour of the link if required.

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

(61) In order to allow competent authorities and the Union agencies to adapt to the new requirements on the use of the European search portal (ESP), it is necessary to provide for a transitional period. Similarly, in order to allow for the coherent and optimal functioning of the multiple-identity detector (MID), transitional measures should be established for the start of its operations.

(61a) Since the objectives 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. 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 those objectives.

(62) The remaining amount on the budget earmarked for Smart Borders in Regulation (EU) No 515/2014 of the European Parliament and the Council[56] should be reallocated to this Regulation, pursuant to Article 5(5)(b) of Regulation (EU) No 515/2014 to cover the costs for the development of the interoperability components.

---

55 How the components are mentioned (in full or acronyms) will be cross-checked by the lawyer-linguists.

56 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).

(63) 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 should be delegated to the Commission in respect of the extension of the transitional period for the use of the European Search Portal (ESP), as well as for the ETIAS Central Unit and extension of the transitional period for the use of multiple-identity detection (MID). In particular, power should be delegated to the Commission in respect of the procedures to determine the cases where identity data can be considered as identical or similar, ~~t~~the rules on the operation of the CRRS, including specific safeguards for processing of personal data and 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 on Better Law-Making of 13 April 2016[57]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council should receive all documents at the same time as Member State experts, and their experts should systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(64) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to adopt detailed rules on: technical details of profiles for the users of the European search portal (ESP); specifications of the technical solution to facilitate the querying of EU information systems, Europol data and Interpol databases by the ESP and format of the ESP replies; technical rules for creating links in MID between data from different EU information systems; the content of the form and the modalities for informing the data subject where a red link is created; performance requirements and performance monitoring of the shared BMS; automated data quality control mechanisms, procedures and indicators; development of the UMF standard; cooperation procedure in case of security incidents; determining the dates from which the ESP, sBMS, CIR, MID, CRRS are to start operations; and the specifications of the technical solution for Member States in order 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.

(65) (…)

(65a) As interoperability components will involve the processing of significant amounts of sensitive personal data, it is important that persons whose data is processed through those components can effectively exercise their rights as data subjects as laid down in Regulation (EU) 2016/679, Directive (EU) 2016/680 and Regulation (EU) 2018/1725. The data subjects should be provided with web portal that facilitates them in exercising their rights to access to and rectification, erasure and restriction of their personal data. eu-LISA should establish and manage such a web portal.

[57] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.123.01.0001.01.ENG.

(65b) One of the core principles of data protection is data minimisation as highlighted in Article 5(1)(c) of Regulation (EU) 2016/679 in accordance with which 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 do 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 purpose of this Regulation.

(65c) This Regulation should contain clear provisions on liability and right to compensation for unlawful processing of personal data or from any other act incompatible with it, 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. With regard to the role of eu-LISA as a data processor, this latter should be responsible for the damage it provoked where it has not complied with the specific obligations of this Regulation directed to it, or where it has acted outside or contrary to lawful instructions of the Member State which is the data controller.

(66) This Regulation is without prejudice to the application of Directive 2004/38/EC.

(67) In accordance with Articles 1 and 2 of Protocol No 22 on the Position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of European Union, 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 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 adoption of this Regulation whether it will implement it in its national law.

(68) Insofar as its provisions relate to SIS as governed by Regulation 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 Treaty on European Union and to the Treaty on the Functioning of the European Union (Protocol on the Schengen *acquis*) and Article 8(2) of 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*[58]. Furthermore, insofar as its provisions relate to Eurodac and to [ECRIS-TCN system], 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 (Protocol on the position of the United Kingdom and Ireland), the United Kingdom has notified, by letter of 18 May 2018, its wish to take part in the adoption and application of this Regulation.

[58] 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).

(69) Insofar as its provisions relate to SIS as governed by Regulation 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 Treaty on European Union and to the Treaty on the Functioning of the European Union (Protocol on the Schengen *acquis*), and Article 6(2) of 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*[59]. Furthermore, insofar as its provisions relate to Eurodac and to [ECRIS-TCN system], in accordance with Articles 1 and 2 of Protocol 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, Ireland is not taking part in the adoption of this Regulation and is not bound 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 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.

(70) As regards Iceland and Norway, this Regulation constitutes, insofar as it relates to SIS as governed by Regulation 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 association of those two States with the implementation, application and development of the Schengen acquis[60] which fall within the area referred to in Article 1, point G of Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of that Agreement[61].

(71) As regards Switzerland, this Regulation constitutes insofar as it relates to SIS as governed by Regulation 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 concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis[62] 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[63].

59

60 OJ L 176, 10.7.1999, p. 36.
61 OJ L 176, 10.7.1999, p. 31.
62 OJ L 53, 27.2.2008, p. 52.
63 OJ L 53, 27.2.2008, p. 1.

(72) As regards Liechtenstein, this Regulation constitutes insofar as it relates to SIS as governed by Regulation 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[64] 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 2011/349/EU.

(73) 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.

(74) In order to have this Regulation fit into the existing legal framework, Regulation (EU) 2016/399, Regulation (EU) 2017/2226, Council Decision 2008/633/JHA, Regulation (EC) No 767/2008 and Council Decision 2004/512/EC should be amended accordingly,

HAVE ADOPTED THIS REGULATION:

64 OJ L 160, 18.6.2011, p. 21.

CHAPTER I
General provisions

Article 1

Subject matter

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

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 lays down the responsibilities of the Member States and of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), with respect to the design, development and operation of the interoperability components.

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

4a. This Regulation also lays down a framework for verifying identities and for identifying persons.

Article 2

Objectives

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

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

(b) to contribute to preventing and combating 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 the security in the territories of the Member States;

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

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

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

(eb) to aid in the identification of unknown persons who are unable to identify themselves or unidentified human remains in cases of natural disasters, accidents or terrorist attacks.

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

(a) ensuring the correct identification of persons;

(b) contributing to combating identity fraud;

(c) improving the 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 bases of the individual systems, data protection standards and principles;

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

(e) strengthening and simplifying and making more uniform the data security and data protection conditions that govern the respective EU information systems, without prejudice to 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 the necessary and proportionate conditions for that;

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

Article 3

Scope

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

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

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

Article 4

Definitions

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

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

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

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

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

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

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

(7) (…)

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

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

(10) ’fingerprint data' means fingerprints 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;

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

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

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

(14) ‘travel document’ means a passport or other equivalent document entitling the holder to cross the external borders and to which a visa may be affixed;

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

(16) (…)

(17) (…)

(18) 'EU information systems' means the EES, VIS, ETIAS, Eurodac, SIS and ECRIS-TCN operationally managed by eu-LISA;

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

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

(21) '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;

(22) (..)

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

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

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

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

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

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

(29) 'the European Travel Information and Authorisation System' ('ETIAS') means the European Travel Information and Authorisation System as referred to in Regulation (EU) 2018/1240;

(30) 'Eurodac' means Eurodac as referred to in Regulation (EU) No 603/2013;

(31) 'Schengen Information System' ('SIS') means the Schengen Information System as referred to in Regulation (EU) 2018/1860, Regulation (EU) 2018/1861 and Regulation (EU) 2018/1862;

(32) 'ECRIS-TCN System' means the centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons as referred to in the ECRIS-TCN Regulation[65].

[65] OJ: please include the reference number of this Regulation when it is published.

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 and 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 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 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, the VIS, the ETIAS, Eurodac, the SIS, the ECRIS-TCN system as well as of the Europol data and the Interpol databases;

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

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

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

2. The authorities referred to in paragraph 1 shall use the ESP to search data related to persons or their travel documents in the central systems of Eurodac and the ECRIS-TCN system in accordance with their access rights as referred to in the legal instruments governing the 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 Regulation (EU) 2018/1860 and Regulation (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 authorities referred to in paragraph 1 may use the ESP to search data related to persons or their travel documents in the Europol data in accordance with their access rights under Union and national law.

Article 8

Profiles for the users of the European search portal

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

(a) the fields of data used for querying;

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

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

(c) the fields 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 for the users of the ESP referred to in Article 7(1) in accordance with their access rights as laid down in the legal instruments governing EU information systems and in accordance with national law. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

2a. 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 users of the ESP shall launch a query by submitting alphanumeric and/or biometric data to the ESP. Where a query has been launched, the ESP shall query simultaneously, with the data submitted by the user of the ESP and in accordance with the user profile, the EES*, the ETIAS, the VIS, the SIS, Eurodac, the ECRIS-TCN system and the CIR as well as the Europol data and the Interpol databases*.

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

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

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

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

The ESP shall provide no information regarding data in information systems to which the user has no access in accordance with 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 is available from one of the EU information systems, Europol data and 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 querying the EU information systems, Europol data and Interpol databases by the ESP and the format of the ESP replies. This implementing act shall be adopted in accordance with the examination procedure referred to in Article 64(2).

Article 10

Keeping of logs

1. Without prejudice to Article 40 of Regulation (EU) 2016/794, Articles 12 and 18 of (EU) 2018/1862 and Article 29 of the ECRIS-TCN Regulation, eu-LISA shall keep logs of all data processing operations within the ESP. Those logs shall include, in particular, the following:

(a) the Member State or Union agency launching the query and the ESP profile used as referred to in Article 8;

(b) the date and time of the query;

(c) the EU information systems and the Europol data queried.

1a. Each Member State and Union Agency shall keep logs of queries of the authority and the staff duly authorised to use the ESP.

2. The logs referred to in paragraphs 1 and 1a 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, unless they are required for monitoring procedures that have already begun in which case they shall be erased once the monitoring procedures no longer require these 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 referred to in Article 9(1) or the CIR, because of a failure of the ESP, the users of the ESP 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, 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 referred to in Article 9(1) or the CIR where they are required to do so according to 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 BMS storing biometric templates obtained from the biometric data referred to in Article 13, that are stored in the CIR and the SIS, and enabling querying with biometric data across several EU information systems is established for the purposes of supporting the CIR and MID and the objectives of the EES, the VIS, Eurodac, the SIS and the ECRIS-TCN system.

2. The shared BMS shall be composed of:

(a) a central infrastructure, that shall replace the central systems of respectively the EES, VIS, SIS, Eurodac and ECRIS-TCN to the extent that it shall store biometric templates and allow to search 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 – logically separated – according to the information system from which the data originates, that it shall obtain from the following biometric data:

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

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

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

(e) the data referred to in Article 4(t) and (u) of Regulation (EU) 2018/1860;

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 and a reference to the actual record in the EU information systems in which the corresponding biometric data are is stored.

3. Biometric templates shall only be entered in the shared BMS following an automated quality check of the biometric data added to one of the 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, 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. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

Article 14

Searching biometric data with the shared biometric matching service

In order to search the biometric data stored within the CIR and the SIS, the CIR and the SIS shall use the biometric templates stored in the shared BMS. Queries with biometric data shall take place in accordance with the purposes provided for in this Regulation and in Regulation (EC) No 767/2008, Regulation (EU) 2017/2226, Regulations (EU) 2018/1860, 2018/1861 and 2018/1862 and the ECRIS-TCN Regulation.

Article 15

Data retention in the shared biometric matching service

The data referred to in Article 13(1) and (2) shall be stored in the shared BMS for as long as the corresponding biometric data are stored in the CIR or the SIS and shall be erased in an automated manner.

Article 16

Keeping of logs

1. Without prejudice to Article 12 and 18 of Regulation (EU) 2018/1862 and Article 29 of the ECRIS-TCN Regulation, eu-LISA shall keep logs of all data processing operations within the shared BMS. Those logs shall include the following:

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

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

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

(c) the date and time of the query;

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

(e) (…);

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

1a. Each Member State and Union Agency shall keep logs of queries of the authority and the staff duly authorised to use the shared BMS.

2. The logs referred to in paragraphs 1 and 1a 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, unless they are required for monitoring procedures that have already begun in which case they shall be erased once the monitoring procedures no longer require these logs.

CHAPTER IV
Common Identity Repository

Article 17

Common identity repository

1. A CIR, creating an individual file for each person that is recorded in the EES, the VIS, the ETIAS, Eurodac or the ECRIS-TCN system containing the data referred to in Article 18, is established for the purpose of facilitating and assisting the correct identification of persons registered in the EES, the VIS, the ETIAS, the Eurodac and the ECRIS-TCN system 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 non-law enforcement EU information systems, 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, the VIS, the ETIAS, Eurodac and the ECRIS-TCN system to the extent that it shall store the data referred to in Article 18;

(b) a secure communication channel between the CIR, Member States and 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, the ETIAS, the VIS, Eurodac and the ECRIS-TCN system as well as with the central infrastructures of the ESP, the shared BMS and the MID.

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

3a. Where it is technically impossible to query the CIR for the purpose of identifying a person pursuant Article 20, for the detection of multiple identities pursuant Article 21 or for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences pursuant Article 22, because of a failure of the CIR, the users of the CIR shall be notified by eu-LISA in an automated manner.

4. 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 was originated:

(a) (…)

(b) (…)

(c) (…)

(d) (…)

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

2a. The authorities accessing the CIR shall do so in accordance with their access rights as referred to in the legal instruments governing the EU information systems and in national law and in accordance with their access rights under this Regulation for the purposes referred to in Articles 20, 21 and 22.

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

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

Article 19

Adding, amending and deleting data in the common identity repository

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

2. Where a white or red link is created in the MID in accordance with Articles 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 The query of the CIR shall be carried out by a police authority in accordance with paragraphs 1 and 2 only in the following circumstances:

- 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,

- where there are doubts about the identity data provided by that person,

- where there are doubts as to the authenticity of the travel document or another credible document provided by that person,

- where there are doubts as to the identity of the holder of the travel document or another credible document, or

- where the person is unable or refuses to cooperate.

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

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

1a. Where the query indicates that data on that person is 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.

1b. Where a police authority has been so empowered by national legislative measures as referred to in paragraph 2a, 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 not able to identify themselves or unidentified human remains, query the CIR with the biometric data of those persons.

2. Member States wishing to avail themselves of the possibility provided for in paragraph 1 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 police authorities competent and lay down the procedures, conditions and criteria of such checks.

2a. Member States wishing to avail themselves of the possibility provided for in paragraph 1b 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 verification of different identities determined 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 belonging to the various EU information systems connected to a yellow link.

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

Article 22

Querying the common identity repository for 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 offence 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 is present in Eurodac.

2. (…)

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

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

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

Where exceptionally, such full access is not requested, the designated authorities shall record the justification therefor traceable to the national file and Europol shall record the justification in the relevant file.

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

Article 23

Data retention in the common identity repository

1. The data referred to in Article 18(1)**,** (2) and (2a) shall be deleted from the CIR in an automated manner in accordance with the data retention provisions of the ECRIS-TCN Regulation respectively.

2. The individual file shall be stored in the CIR 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 the ECRIS-TCN Regulation, eu-LISA shall keep logs of all data processing operations within the CIR in accordance with paragraphs 2, 3 and 4.

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

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

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

(b) the date and time of the query;

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

(d) the results of the query.

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

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

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

(b) the date and time of the query;

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

(d) where a link is created, the results of the query indicating the EU information system from which the data was received.

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

(a) (…)

(b) the date and time of the query;

(c) the data used to launch the query;

(d) the results of the query;

(e) the Member State or Union agency querying the CIR;

(f) (…).

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) to (3) are fulfilled.

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

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

(b) the national file reference;

(ab) the purpose of access;

(b) 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.

5a. In accordance with Regulation (EU) 2016/794, for any access to the CIR pursuant to Article 22, 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.

6. The logs referred to in paragraphs 2, 3, 4, 5 and 5a 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, unless they are required for monitoring procedures that have already begun in which case they shall be erased once the monitoring procedures no longer require these logs.

7. eu-LISA shall keep the logs related to the history of the data stored in individual files, for the purposes defined in paragraph 6. eu-LISA shall erase the logs related to the history of the data stored in an automated manner, once the data are erased.

CHAPTER V
Multiple-identity Detector

Article 25

Multiple-identity detector

1. A MID creating and storing an identity confirmation file as refered to in Article 34 containing links between data in the EU information systems included in the CIR and the SIS and as a consequence detecting multiple identities, with the dual purpose of facilitating identity checks and combating identity fraud, is established for the purpose of supporting the functioning of the CIR and the objectives of the EES, the VIS, the ETIAS, Eurodac, the SIS and the ECRIS-TCN system.

2. The MID shall be composed of:

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

(b) a secure communication infrastructure to connect the MID with the 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 identity verification referred to in Article 29, access to the data referred to in Article 34 stored in the MID shall be granted to:

(a) (…)

(b) (…)

(c) (…)

(d) (…)

(e) the SIRENE Bureaux of the Member State creating or updating an alert in accordance with Regulation (EU) 2018/1862;

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

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

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 informations systems 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 informations systems between which the green link was created and a query towards those information systems revealed a match against the two sets of data linked.

Article 27

Multiple-identity detection

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

(a) (…)

(b) (…)

(c) (…)

(d) (…)

(e) an alert on a person is created or updated in the SIS in accordance with Chapters VI, VII, VIII and IX of the Regulation (EU) 2018/1862;

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

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

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

(a) (…)

(b) (…)

(c) (…)

(d) (…)

(e) (…)

(f) surname(s); forename(s); name(s) at birth, previously used names and aliases; date of birth, place of birth, nationality(ies) and sex as referred to in Article 20(3) of Regulation (EU) 2018/1862;

(g) (…)

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

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

4. 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 (3a) do not report any match, the procedures referred to in Article 27(1) shall continue in accordance with the respective Regulations governing them.

2. Where the query laid down in Article 27(2), (3) and (3a) reports one or several match(es), the CIR and, where relevant, the 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 data was already linked, the existing link shall be extended to the data used to launch the query.

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

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

5. The Commission shall lay down the procedures to determine the cases where identity data can be considered as the same, similar or presenting some differences in delegated acts. Those delegated acts shall be adopted in accordance with Article 63.

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 64(2).

Article 29

Authorities responsible and manual verification of different identities

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

(a) (…)

(b) (…)

(c) (…)

(d) (…)

(e) the SIRENE Bureaux of the Member State for matches that occurred when creating or updating a SIS alert in accordance with the Regulation (EU) 2018/1862;

(f) the central authorities of the convicting Member State for hits that occurred when recording or updating data in the ECRIS-TCN system in accordance with Article 5 or Article 9 of the ECRIS-TCN Regulation.

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

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

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

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

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

(d) (…)

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

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

4. (…)

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

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

Article 30

Yellow link

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

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

(b) the linked data has different identity data but the same travel document data, no manual verification of different identity has taken place and at least one of the EU information systems does not have biometric data on the person;

(ba) the linked data have the same identity data but different biometric data and no manual verification of different identities has taken place;

(c) the linked data has similar or different identity data, the same travel document data, but different biometric data and no manual verification of different identity has taken place.

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

Article 31

Green link

1. A link between data from two or more EU information systems shall be classified as green where:

(a) the linked data do not share the same biometric data but have the same identity data and the authority responsible for the verification of different identities concluded it refers to two different persons;

(b) the linked data do not share the same biometric data, have the similar or different identity data and have the same travel document data and the authority responsible for the verification of different identities concluded it refers to two different persons;

(c) the linked data have different identity data but have the same travel document data and at least one of the EU information systems does not have biometric data on the person and the authority responsible for the verification of different identities concluded it refers to two different persons.

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

3. If a Member State authority has evidence to suggest that a green link recorded in the MID is factually inaccurate, not up-to-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 the SIS and shall, if necessary, rectify or erase the link from the MID without delay. That Member State authority shall inform the Member State responsible for the manual verification without delay.

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 shares the same biometric but similar or different identity data and the authority responsible for the verification of different identities concluded it refers to the same person in an unjustified manner;

(b) the linked data has the same, similar or different identity data and the same travel document data but different biometric data and the authority responsible for the verification of different identities concluded it refers to two different persons using the same travel document in an unjustified manner;

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

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

2. Where the CIR or the SIS are queried and where a red link exists between two or more of the information systems constituting the CIR or with the SIS, the MID shall reply indicating the data referred to in Article 34. Follow-up to a red link shall take place in accordance with Union and national law, basing any legal consequence for the person 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 from the EES, the VIS, the ETIAS, Eurodac or the ECRIS-TCN System, the individual file stored in the CIR shall be updated in accordance with Article 19(2).

4. Without prejudice to the provisions related to the handling of alerts in the SIS referred to in Regulations (EU) 2018/1860, 2018/1861 and 2018/1862, and without prejudice to limitations necessary to protect security and public order, prevent crime and guarantee that any national investigation will not be jeopardised, where a red link is created, the authority responsible for verification of different identities shall inform the person of the presence of multiple unlawful identities and shall provide the person in writing with a single identification number as referred to in Article 34(c), a reference to the authority responsible for the verification of different identities as referred to in Article 34(d) and the website address of the web portal established in accordance with Article 47a.

4a. The information shall be given by means of a standard form by the authority responsible for verification of different identities. The Commission shall determine the content of that form and the modalities for the information by implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

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

5a. Where a Member State authority or Union agency having access to CIR or SIS obtains evidence showing that a red link recorded in MID is incorrect or the data processed in MID, CIR and SIS is processed in breach of this Regulation, that authority shall:

- where the link relates to EU information systems, either rectify or erase the link from MID immediately, or

-where the link relates to one of the SIS alerts referred to in Article 29(2), inform the relevant SIRENE Bureau of the Member State that created the SIS alert immediately. That SIRENE Bureau shall verify the evidence provided by the Member State authority and where relevant rectify or erase the link from the MID immediately.

The Member State authority obtaining the evidence shall inform the Member State responsible for the manual verification without delay indicating where relevant any 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 shares the same biometric and the same or similar identity data;

(b) the linked data shares 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;

(ba) the linked data shares the same biometric, the same travel document data but similar identity data;

(c) the linked data shares the same biometric but similar or different identity data and the authority responsible for the verification of different identities concluded it refers to the same person having different identity data in a justified manner.

2. Where the CIR or the SIS are queried and where a white link exists between two or more of the EU information systems constituting the CIR or with the SIS, 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, hence triggering a match against the data that is subject to 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 from the EES, the VIS, the ETIAS, Eurodac or the ECRIS-TCN system, the individual file stored in the CIR shall be updated in accordance with Article 19(2).

4. Without prejudice to the provisions related to the handling of alerts in the SIS referred to in Regulations (EU) 2018/1860, 2018/1861 and 2018/1862, and without prejudice to limitations necessary to protect security and public order, prevent crime and guarantee that any national investigation will not be jeopardised, where a white link is created following a manual verification of multiple identities, the authority responsible for verification of different identities shall inform the person of the presence of similar identities and shall provide the person in writing with a single identification number as referred to in Article 34(c), a reference to the authority responsible for the verification of different identities as referred to in Article 34(d) and the website address of the web portal established in accordance with Article 47a.

4a. If a Member State authority has evidence to suggest that a white link recorded in the MID is factually inaccurate, not up-to-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 the SIS and shall, if necessary, rectify or erase the link from the MID without delay. That Member State authority shall inform the Member State responsible for the manual verification without delay.

4a. The information shall be given by means of a standard form by the authority responsible for verification of different identities. The Commission shall determine the content of that form and the modalities for the information by implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

Article 34

Identity confirmation file

The identity confirmation file shall contain the following data:

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

(b) a reference to the EU information systems whose data are linked;

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

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

(e) the date of creation or update of the link.

Article 35

Data retention in the multiple-identity detector

The identity confirmation files and their data, 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 and be deleted thereafter in an automated manner.

Article 36

Keeping of logs

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

(-a) the Member State launching the query;

(a) the purpose of access of the user;

(b) the date and time of the query;

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

(d) the reference to the data linked;

(e) the history of the identity confirmation file.

2. Each Member State and Union Agency shall keep logs of queries of the authority and the staff duly authorised to use the MID.

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, unless they are required for monitoring procedures that have already begun in which case they shall be erased once the monitoring procedures no longer require these logs.

CHAPTER VI
Measures supporting interoperability

Article 37

Data quality

1. In addition 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, the ECRIS-TCN system, 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 to store data in the SIS, Eurodac, the ECRIS-TCN system, the shared BMS and the CIR.

Only data fulfilling the minimum quality standards may be entered in the SIS, Eurodac, the ECRIS-TCN system, the shared BMS, the CIR and the MID.

3. eu-LISA shall provide regular reports on the automated data quality control mechanisms and procedures and the common data quality indicators to the Member States. eu-LISA shall also provide a regular report to the Commission covering the issues encountered and the Member States concerned. eu-LISA shall also provide that report to the European Parliament and 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 to store data in the SIS, Eurodac, the ECRIS-TCN system, 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 64(2).

5. One year after the establishment of the automated data quality control mechanisms and procedures, common data quality indicators and the minimum quality standards and every year thereafter, the Commission shall evaluate Member State implementation of data quality and shall make any necessary recommendations. The Member States shall provide the Commission with an action plan to remedy any deficiencies identified in the evaluation report and, in particular, data quality issues deriving from erroneous data in existing EU information systems and 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, the European Data Protection Board and to the European Union Agency for Fundamental Rights established by Council Regulation (EC) No 168/2007.[66]

Article 38

Universal Message Format

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

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

3. (…)

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

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

Article 39

Central repository for reporting and statistics

1. A central repository for reporting and statistics (CRRS) is established for the purposes of supporting the objectives of the SIS, Eurodac and the ECRIS-TCN system, in accordance with the respective legal instruments, 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 the CRRS in its technical sites containing the data and statistics referred to in Article 71 of Regulation (EU) 2018/1862 and Article 30 of the ECRIS-TCN Regulation logically separated. The data contained in the CRRS shall not enable the identification of individuals. Access to the CRRS shall be granted by means of secured access with control of access and specific user profiles, solely for the purpose of reporting and statistics, to the authorities referred to in Article 71 of Regulation (EU) 2018/1862 and Article 30 of the ECRIS-TCN Regulation.

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;

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

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

5. The Commission shall lay down detailed rules on the operation of the CRRS, including specific safeguards for processing of personal data referred to under paragraph 2 and 3 and security rules applicable to the repository by means of a delegated act adopted in accordance with the procedure referred to in Article 63.

CHAPTER VII
Data protection

Article 40

Data controller

1. In relation to the processing of data in the shared biometric matching service (shared BMS), the Member State authorities that are controllers for SIS, the Eurodac and the ECRIS-TCN system respectively, shall be controllers in accordance with Article 4(7) of Regulation (EU) 2016/679 ***or*** Article 3(8) of Directive (EU) 2016/680 in relation to the biometric templates obtained from the data referred to in Article 13 that they enter into respective systems and shall have responsibility for the processing of the biometric templates in the shared BMS.

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

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

(a) the European Border and Coast Guard Agency shall be a data controller in accordance with Article 2(d) of Article 3(2)(b) 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 Article 4(7) of Regulation (EU) 2016/679 or Article 3(8) 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 45.

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 in accordance with Article 3(1)(a) 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 the application of 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;

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

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

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

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

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

(e) 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;

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

(g) 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;

(h) 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;

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

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

(i) 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

(…)

Article 44

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, 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 incident, 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.

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 specification 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 64(2).

Article 45

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 as referred to in Article 40 shall take the necessary measures to monitor the compliance of the data processing pursuant to this Regulation, including frequent verification of the logs referred to in Articles 10, 16, 24 and 36, and cooperate, where necessary, with the supervisory authorities referred to in Article 49 and with the European Data Protection Supervisor referred to in Article 50.

Article 45a

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 45b

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, 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 46

Right to information

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

1a. 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.

1b. The rules on the right to information contained in Regulation (EU) 2016/679 or Directive (EU) 2016/680 shall apply to the personal data recorded in the ECRIS-TCN system and processed for the purposes of this Regulation.

2. (…)

(a) (…)

(b) (…)

(c) (…)

(d) (…)

(e) (…)

Article 47

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, 16, 17 and 18 of Regulation (EU) 2016/679, Articles 17, 18, 19 and 20 of Regulation (EU) 2018/1725 and Articles 14, 15 and 16 of Directive (EU) 2016/680 and, any person shall have the right to address himself or herself to the competent authority of any Member State, who shall examine and reply to the request.

2. The Member State which examined such 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 examined such 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 these replies are 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 controller shall inform the data subject of any such extension within 30 days of receipt of the request, 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 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 and ask for its opinion to be given 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 controller shall inform the data subject of any such extension within 30 days of receipt of the request, together with the reasons for the delay.

4a. 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 or where the ETIAS Central Unit was responsible for the manual verification the Member State to which the request has been made shall correct or delete these data without any undue delay. The person concerned shall be informed in writing that his or her data has been rectified or erased.

5. Where data stored in the MID is amended by a Member State during its validity 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 shall be linked. Where the processing does not report any match, that Member State shall delete the data from the identity confirmation file. Where the automated processing reports one or several match(es), that Member State shall create or update the relevant link in accordance with the relevant provisions of this Regulation.

6. 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 correct or delete data relating to him or her.

7. This decision shall also provide the person concerned with information explaining the possibility to challenge the decision taken in respect of the request for access, rectification, restriction of processing or erasure 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 national supervisory authorities.

8. Any request for access, rectification, restriction of processing or erasure 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.

9. 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 record in the form of a written document that a request for access, rectification, restriction of processing or erasure of personal data was made and how it was addressed, and shall make that document available to national supervisory authorities without delay.

10. This article is without prejudice to the limitations and restrictions to the rights set out in this article which are provided for under Regulation 2016/679 and Directive (EU) 2016/680.

Article 47a

Web portal

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

2. The web portal shall contain information on the rights and procedures referred to in Article 46 and 47 and a user interface enabling persons whose data are processed in the MID and who were 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 verification of different identities.

3. In order to obtain the contact information of the competent authority of the Member State responsible for the verification of different identities, the person whose data are processed in the MID should enter the reference to the authority responsible for the 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 verification of different identities. The web portal shall also include a template e-mail to facilitate the communication between the user and the competent authority of the Member State responsible for the verification of different identities. Such e-mail shall include the single identification number referred to in Article 34(c) in order to allow the competent authority of the Member State responsible for the 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 as referred to in Articles 46 and 47 and shall regularly review whether these data 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 63 to adopt 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 to facilitate the communication between the user and the competent authority of the Member State responsible for the verification of different identities.

Article 48

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

Without prejudice to Article 31 of Regulation (EC) No 767/2008, Article 41 of Regulation (EU) 2017/2226, Article 65 of Regulation (EU) 2018/1240, Article 25 of Regulation (EU) 2016/794 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 49

Supervision by the supervisory authorities

-1. Each Member State shall ensure that the supervisory authority established in accordance with Article 51(1) of Regulation (EU) 2016/679 and Article 41(1) of Directive (EU) 2016/680 independently monitors the lawfulness of the processing of personal data referred to in this Regulation by the Member State concerned, including their transmission to and from the components of interoperability.

-1a. 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.

1. 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 referred to in Article 51(1) of Regulation (EU) 2016/679 and Article 41(1) of Directive (EU) 2016/680 shall publish annually the number of requests for rectification, erasure, or restriction of processing of data, the action subsequently taken and the number of rectifications, erasures and restrictions of processing made in response to requests by the persons concerned.

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

2a. 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 as laid down in this Regulation. Member States shall grant the supervisory authorities referred to in Article 51(1) of Regulation (EU) 2016/679 access to their logs as referred to in Articles 10, 16, 24 and 36, to their justification referred to in Article 22(3) and allow them to access all their premises used for interoperability purposes at all times.

Article 50

Audit 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, the Council, eu-LISA, the Commission, the Member States and 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 and the ETIAS Central Unit shall supply information requested by the European Data Protection Supervisor to it, give the European Data Protection Supervisor access to all the documents and to its logs as referred to in Articles 10, 16, 24 and 36 and allow the European Data Protection Supervisor access to all its premises at any time.

Article 51

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 national 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, 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 activities to the European Parliament, the Council, the Commission, Europol, the European Border and Coast Guard Agency and eu-LISA two years after entry into force of this Regulation and every two years thereafter. That report shall include a chapter on each Member State prepared by the supervisory authority of that Member State.

CHAPTER VIII
Responsibilities

Article 52

Responsibilities of eu-LISA during the design and development phase

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

2. The interoperability components shall be hosted by eu-LISA in its technical sites and shall provide the functionalities laid down in this Regulation in accordance with the conditions of security, availability, quality and performance referred to in Article 53(1).

3. eu-LISA shall be responsible for the development of the interoperability components, for any adaptations required for establishing interoperability between the central systems of the EES, VIS, ETIAS, SIS, Eurodac and the ECRIS-TCN system, and the ESP, the shared BMS, the CIR, the MID and the CRRS.

Without prejudice to Article 56, it shall not have access to any of the personal data processed through the ESP, the shared BMS, the CIR and the MID.

eu-LISA shall define the design of the physical architecture of the interoperability components including their communication infrastructures and the technical specifications and their evolution as regards the central infrastructure and the secure communication infrastructure, which shall be adopted by the Management Board, subject to a favourable opinion of the Commission. eu-LISA shall also implement any necessary adaptations to the SIS, Eurodac or ECRIS-TCN system deriving from the establishment of interoperability and provided for by this Regulation.

eu-LISA shall develop and implement the interoperability components as soon as possible after the entry into force of this Regulation and the adoption by the Commission of the measures provided for in Articles 8(2), 9(7), 28(5) and (6), 37(4), 38(4), 39(5), 44(5) and 68(7a).

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 65, 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 legislative 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.

The Programme Management Board shall every month submit to eu-LISA's Management Board written reports on progress of the project. 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 full information to non-participating Members of the Management Board.

The chairmanship shall be held by a Member State that is fully bound under Union law by the legislative instruments governing the development, establishment, operation and use of all the EU information systems.

All travel and subsistence expenses incurred by the members of the Programme Management Board shall be paid by the Agency, 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 65 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 53

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 maintenance and technological developments. In cooperation with the Member States, it shall ensure 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 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, in particular 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, controlled access, full, uninterrupted availability of the components and the data stored in the MID, sBMS and 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 entire 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 56, it 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 54

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(2) and 20(2a) in order to access the CIR for identification purposes;

(f) the manual verification of different identities referred to in Article 29;

(g) the compliance with data quality requirements established under Union law;

(ga) fully complying with the rules of each EU information system to ensure the security and integrity of personal data;

(h) 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 54a

Responsibilities of Europol

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

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

Article 55

Responsibilities of the ETIAS Central Unit

The ETIAS Central Unit shall be responsible for:

(a) the manual verification of different identities referred to in Article 29;

(b) carrying out a multiple-identity detection between the data stored in the EES, VIS, Eurodac and the SIS referred to in Article 59.

CHAPTER IX
Amendments to other Union instruments

Article 55a

Amendments to Regulation (EU) 2018/XX [the Eurodac Regulation]

(…)

Article 55b

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 eu-LISA's operational responsibility, eu-LISA, closely involving its Advisory Groups, shall establish for all systems under the Agency's operational responsibility automated data quality control mechanisms and procedures and common data quality indicators and the minimum quality standards to store data, in accordance with the relevant provisions of the systems' instruments and of [Article 37 of Regulation 2018/XX on interoperability].

2. eu-LISA shall establish a central repository containing only anonymised data for reporting and statistics subject to specific provisions in the legislative instruments governing the development, establishment, operation and use of large-scale IT systems managed by eu-LISA in accordance with [Article 39 of Regulation 2018/XX on interoperability]."

3. Article 19(1) is amended as follows:

(a) the following point is inserted:

"(eea) adopt the reports on the state of play of the development of the interoperability components pursuant to [Article 68(2) of Regulation 2018/XX on interoperability].";

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

"(ff) adopt the reports on the technical functioning of SIS II pursuant to Article 54(7) of Regulation 2018/1861 and Article 71(7) of Regulation 2018/1862, of 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 Regulation (EU) 2018/XX on the ECRIS-TCN system and the ECRIS reference implementation pursuant to Article 34(4) of Regulation (EU) 2018/XX] and of the interoperability components pursuant to [Article 68(4) of Regulation 2018/XX on interoperability];"

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

"(hh) adopt formal comments on the European Data Protection Supervisor's reports on the audits pursuant to Article 56(2) of Regulation (EU) 2018/1861, Article 42(2) of Regulation (EC) No 767/2008 and Article 31(2) of Regulation (EU) No 603/2013, Article 56(2) of Regulation (EU) 2017/2226, and Article 67 of Regulation (EU) 2018/1240 and to Article 27(2) of Regulation (EU) 2018/XX (establishing the ECRIS-TCN system) and to [Article 50 of Regulation 2018/XX on interoperability] 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 II 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 II (N.SIS II) and SIRENE Bureaux pursuant to Article 7(3) of Regulation (EU) 2018/1862 and Article 7(3) of Regulation (EU) 2018/1861 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/…[+], [the list of competent authorities pursuant to Article 32 of Regulation (EU) 2018/… (ECRIS-TCN)] and the list of authorities pursuant to Article 61(1) of [Regulation (EU) 2018/… on interoperability]."

4. 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 observers when a question concerning SIS in relation to the application of Regulation (EU) 2016/1624 is on the agenda. Europol may also attend the meetings of the Management Board as 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 also 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 also attend the meetings of the Management Board as observer when a question concerning ETIAS in relation with the application of Regulation (EU) 2018/1240 is on the agenda. EASO may also attend the meetings of the Management Board as an observer when a question concerning the automated system for registration, monitoring and the allocation mechanism for applications for international protection referred to in Article 44 of Regulation (EU) 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 (recast), is on the agenda.Eurojust, Europol, the European Public Prosecutor's Office may also attend the meetings of the Management Board as observers when a question concerning Regulation 2018/XX (establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS), and amending Regulation (EU) No 1077/2011 (ECRIS-TCN system) is on the agenda.] Europol, Eurojust and the European Border and Coast Guard Agency may also attend the meetings of the Management Board as observers when a question concerning [Regulation 2018/XX on interoperability] 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.".

[+] OJ: Please insert serial number of the Regulation in 2016/0357A(COD).

5. In Article 24(3), point (p) is replaced by the following

"(p) without prejudice to Article 17 of the Staff Regulations, 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 2018/1240, Article 11(16) of Regulation 2018/XX (establishing the ECRIS-TCN system) and [Article 53(2) of Regulation 2018/XX on interoperability];".

6. Article 27 is amended as follows:

(a) in paragraph 1 the following point is inserted:

"(e) Interoperability Advisory Group;";

(b) paragraph 3 is replaced by the following:

"3. Europol and 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 also appoint a representative to the ECRIS-TCN system Advisory Group. Europol, Eurojust and the European Border and Coast Guard Agency may each appoint a representative to the Interoperability Advisory Group."

Article 55c

Amendments to Regulation (EU) 2018/1862

Regulation (EU) 2018/1862 is amended as follows:

1. In Article 3, the following points are added:

“(19) ‘ESP’ means the European search portal established by [Article 6(1) of Regulation 2018/XX on interoperability].

(20) ‘shared BMS' means the shared biometric matching service established by [Article 12(1) of Regulation 2018/XX on interoperability].

(21) 'CIR' means the common identity repository established by [Article 17(1) of Regulation 2018/XX on interoperability];

(22) ‘MID’ means the multiple-identity detector established by [Article 25(1) of Regulation 2018/XX on interoperability].”.

2. Article 4 is amended as follows:

(a) in paragraph 1, the following point is added

"(d) a secure communication infrastructure between CS-SIS and the central infrastructures of the ESP established in accordance with [Article 6 of Regulation 2018/XX on interoperability], the shared BMS established in accordance with [Article 12 of Regulation 2018/XX on interoperability] and the MID established in accordance with [Article 25 of Regulation 2018/XX on interoperability]".

(b) the following paragraphs are added:

"7. Without prejudice to paragraphs 1 to 4, SIS data on persons and identity documents may also be searched via the ESP."

8. Without prejudice to paragraphs 1 to 4, SIS data on persons and identity documents may also be transmitted via the secure communication infrastructure referred to in point (e) of paragraph 1. These transmissions shall be limited to the extent that the data are required for the functionalities referred to by [Regulation 2018/XX on interoperability].".

3. In Article 7, the following paragraph is inserted:

"2a. The SIRENE Bureaux shall also ensure the verification of different identities in accordance with [Article 29 Regulation 2018/XX on interoperability]. To the extent necessary to carry out this task, the SIRENE Bureaux shall have access to consulting the data stored in the CIR and the MID for the purposes laid down in [Articles 21 and 26 of Regulation 2018/XX on interoperability]."

4. In Article 12, the following paragraph is inserted:

"1a. Member States shall ensure that every access to personal data via the ESP are also logged for the purposes of checking whether or not the search is lawful, monitoring the lawfulness of data processing, self-monitoring, 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 2018/XX on interoperability]."

6. In Article 74, paragraph 7, is replaced by the following:

"7. For the purpose of paragraphs 3, 4 and 6 and of Article 15(4), the Agency shall store data referred to in paragraph 3 and in Article 15(4) which shall not allow for the identification of individuals in the central repository for reporting and statistics referred to in [Article 39 of the Regulation 2018/XX on interoperability].

The Agency shall allow the Commission and the bodies referred to in paragraph 6 to obtain bespoke reports and statistics. Upon request, the Agency shall give access to Member States, the Commission, Europol, and the European Border and Coast Guard Agency to the central repository in accordance with [Article 39 of the Regulation 2018/XX on interoperability]."

Article 55d

Amendments to Regulation (EU) 2018/XX [the ECRIS-TCN Regulation]

Regulation (EU) 2018/XX [the ECRIS-TCN Regulation] is amended as follows:

1. In Article 1, the following point is added:

"(c) the conditions under which the ECRIS-TCN system contributes to facilitating and assisting in the correct identification of persons registered in the ECRIS-TCN system under the conditions and for the ultimate objectives referred to in [Article 20 of Regulation 2018/XX on interoperability], by storing identity, travel document and biometric data in the common identity repository (CIR) established by [Article 17(1) of Regulation 2018/XX on interoperability]."

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, as well as for contributing to facilitating and assisting in the correct identification of persons in accordance with this Regulation and with Regulation 2018/XX on interoperability."

3. Article 3 is amended as follows:

(a) the following points are added:

"(q) ‘CIR' means the common identity repository established by [Article 17(1) of Regulation 2018/XX on interoperability];

(r) 'ECRIS-TCN data' means all data stored in the ECRIS-TCN Central System and in the CIR in accordance with Article 5."

(b) in point (n), the words ‘Central System’ are replaced by the words ‘the ECRIS-TCN Central System and the CIR’.

4. Article 4(1) is amended as follows

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

"(a) the CIR-established by [Article 17(1) of Regulation 2018/XX on interoperability];"

(b) the following point is inserted:

"(ab) a Central System (ECRIS-TCN Central System);"

(c) the following point is added:

"(e) a secure communication infrastructure between the ECRIS-TCN Central System and the central infrastructures of the European search portal established by [Article 6(1) of Regulation 2018/XX on interoperability], the shared biometric matching service established by [Article 12 of Regulation 2018/XX on interoperability], and the CIR established by [Article 17(1) of Regulation 2018/XX on interoperability] and the multiple-identity detector established by [Article 25 of Regulation 2018/XX on interoperability]."

5. In Article 5, the following paragraph is inserted:

"1a. The CIR shall contain the data referred to in Article 5(1)(b) and the following data of Article 5(1)(a): surname (family name); first name(s) (given name(s)); date of birth; place of birth (town and country); nationality or nationalities; gender; and where applicable previous names, and where available pseudonyms(s) and/or alias name(s), where available, the type and number of the person's travel document(s), as well as the name of the issuing authority thereof and may contain the data referred to in Article 5(2). The remaining ECRIS-TCN data shall be stored in the ECRIS-TCN Central System."

5a. In Article 8, paragraph 1 is replaced by the following:

"1. Each data record shall be stored in the Central System and the CIR as long as the data related to the conviction(s) of the person concerned are stored in the criminal records.".

6. In Article 8, 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 fingerprints and facial images, without undue delay from the ECRIS-TCN Central System and the CIR. This shall be done automatically, where possible, and in any event no later than one month after the expiry of the retention period.".

7. In Article 9, in paragraph 1, the words ‘ECRIS-TCN System’ are replaced by the words ‘the ECRIS-TCN Central System and the CIR’.

7a. In Article 9, in paragraphs 2, 3 and 4, the words ‘Central System’ are replaced by the words ‘the ECRIS-TCN Central System and the CIR’.

8. In Article 12(2), the words ‘Central System’ are replaced by the words ‘the ECRIS-TCN Central System and the CIR’.

9. In Article 13, in paragraph 2, the words ‘Central System’ are replaced by the words ‘the ECRIS-TCN Central System and the CIR’

10. In Article 21(2), the words ‘Central System’ are replaced by the words ‘the ECRIS-TCN Central System and the CIR’

11. Article 22 is amended as follows:

(a) paragraph 1 is replaced by the following:

“1. The data included in the ECRIS-TCN Central System and the CIR shall only be processed for the purposes of the identification of the Member State(s) holding the criminal records information of third country nationals.~~,~~ The data included in the CIR shall also be processed in accordance with Regulation 2018/XX on interoperability 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 to 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 [Article 20 and Article 21 of Regulation 2018/XX on interoperability]. That access shall be limited to the extent necessary for the performance of the tasks of those national authorities and Union agencies in accordance with those purposes and shall be proportionate to the objectives pursued."

12. Article 30 is amended as follows:

(a) paragraph 2 is replaced by the following:

"2. For the purpose of paragraph 1 of this Article, eu-LISA shall store the data referred to in paragraph 1 in the central repository for reporting and statistics referred to in [Article 39 of the Regulation 2018/XX on interoperability].";

(b) paragraph 3 is deleted.

13. In Article 31(1) the words ‘Central System’ are replaced by the words ‘the ECRIS-TCN Central System’.

14. In Article 38(2) the words ‘Central System’ are replaced by the words ‘the ECRIS-TCN Central System and the CIR’.

CHAPTER X
Final provisions

Article 56

Reporting and statistics

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

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

(b) (…)

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 without enabling individual identification:

(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.

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 without enabling individual identification:

(a) (…)

(b) (…)

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

(d) the number of each type of link and the EU information systems between which each link was established;

(db) the period of time for which a yellow and red link remained in the system.

4. The duly authorised staff of the European Border and Coast Guard Agency established by Regulation (EU) 2016/1624 of the European Parliament and of the Council[67] shall have access to consult the data referred to in paragraphs 1, 2 and 3 for the purpose of carrying out risk analyses and vulnerability assessments as referred to in Articles 11 and 13 of that Regulation.

4a. The duly authorised staff of Europol shall have access to consult the data referred to in paragraphs 2 and 3 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.

[67] 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).

5. For the purpose of paragraphs 1, 2 and 3 of this Article, eu-LISA shall store the data referred to in paragraph 1, 2 and 3 of this Article in the central repository for reporting and statistics referred to in Chapter VII of this Regulation. The data included in the repository shall not enable the identification of individuals, but it shall allow the authorities listed in paragraph 1, 2 and 3 of this Article to obtain customisable reports and statistics to enhance the efficiency of border checks, to help authorities processing visa applications and to support evidence-based policymaking on migration and security in the Union.

5a. Upon request, relevant information shall be made available by the Commission to the Agency for Fundamental Rights in order to evaluate the impact on fundamental rights of this Regulation.

Article 57

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 a adopt a delegated act in accordance with Article 63 to once extend the period referred to in paragraph 1 by no longer than 1 year when an assessment of the practical implementation of the ESP showed that it is necessary to extend this period especially because of the impact of the introduction of the ESP on the organisation and duration of border checks.

Article 58

Transitional period applicable to the provisions on access to the common identity repository for 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 referred to in Article 62(1).

Article 59

Transitional period for the multiple-identity detection

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

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

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

Where several matches are reported, a link shall be created to 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 information systems to the ETIAS Central Unit.

4. Where a link is created to an alert in the SIS, other than a refusal of entry or return alert or an alert on a travel document reported lost, stolen or invalidated in accordance with Article 3 of Regulation (EU) 2018/1860, Articles 24 and 25 of Regulation (EU) 2018/1861 and Article 38 of Regulation (EU) 2018/1862 respectively, the MID shall grant access to the identity data present in the different information systems to the SIRENE Bureau of the Member State that created the alert.

5. The ETIAS Central Unit or the SIRENE Bureau of the Member State that created the alert shall have access to the data contained in the identity confirmation file and shall assess the different identities and shall update the link in accordance with Articles 31 to 33 and add it to the identity confirmation file.

5a. The ETIAS Central Unit shall only notify the Commission in accordance with Article 61(3) once all yellow links have been verified and updated either into green, white or red links.

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

The Commission is empowered to adopt a delegated act in accordance with Article 63 to extend the period referred to in paragraph 1 by six months, renewable twice by six months each time. Such extension shall only be granted where an assessment of the estimated completion time for the multiple-identity detection referred to in this Article, carried out no later than three months before the expiry of either the deadline referred to in paragraph 1 or the deadline of the first two extensions, demonstrates that such deadline cannot be met for reasons independent of the ETIAS Central Unit and that no corrective measures can be applied.

Article 60

Costs

1. The costs incurred in connection with the establishment and operation of the ESP, the 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.

2a. 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 will be mobilised from the envelope of EUR 791 million foreseen under Article 5(5) point (b) of the ISF Borders and Visa Regulation[68] to cover the costs of implementation of this Regulation, as foreseen under paragraphs 1 and 2.

2b. From the envelope referred to in the preceding paragraph, EUR 22.861.000 will be allocated to eu-LISA, EUR 9.072.000 will be allocated to Europol, and EUR 144.000 will be allocated to CEPOL, to support these agencies in performing their respective tasks in line with the requirements of this Regulation. Such funding shall be implemented under indirect management.

3. The costs incurred by the designated authorities referred to in Article 4(24) shall be borne, respectively, by each Member State and Europol. The costs for the connection of the designated authorities to the CIR shall be borne by each Member State and Europol, respectively.

Article 61

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 62. 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 test referred to in Article 62(1)(b).

---

[68] 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 (OJ L 150, 20.5.2014, p. 143).

3. The ETIAS Central Unit shall notify the Commission of the successful completion of the transitional measure laid down in Article 59.

4. The Commission shall make available to the Member States and the public, by a constantly updated public website, the information notified pursuant to paragraph 1.

Article 62

Start of operations[69]

1. The Commission shall determine the date from which the ESP is to start operations by means of an implementing act when the following conditions are met:

(a) the measures referred to in Articles 8(2), 9(7) and 44(5) have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the ESP, which is to be conducted by eu-LISA in cooperation with the Member States 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 Articles 8(1) and has notified them to the Commission;

The ESP shall only query the Interpol databases where the technical arrangements allow to fulfil the requirements referred to in Article 9(5). The impossibility to fulfil this requirement shall result in the ESP not querying the Interpol databases but shall not delay the start of operations of the ESP.

The date referred to in the first subparagraph shall be set for within 30 days from the decision of the Commission.

---

69 With regards to the Commission decision by implementing act, a corresponding recital needs to be added during the lawyers-linguist revision.

1a. The Commission shall determine the date from which the sBMS is to start operations by means of an implementing act when the following conditions are met:

(a) the measures referred to in Articles 13(5) and 44(5) have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the sBMS, which is to be conducted by eu-LISA in cooperation with the Member States;

(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 1d(b).

The date referred to in the first subparagraph shall be set for within 30 days from the decision of the Commission.

1b. The Commission shall determine the date from which the CIR is to start operations by means of an implementing act when the following conditions are met:

(a) the measures referred to in Articles 44(5) and 68(7a) have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the CIR, which is to be conducted by eu-LISA in cooperation with the Member States;

(c) eu-LISA has validated the technical and legal arrangements to collect and transmit the data referred to in Article 18 has notified them to the Commission;

(d) eu-LISA has declared the successful completion of the test referred to in paragraph 1d(b).

The date referred to in the first subparagraph shall be set for within 30 days from the decision of the Commission.

1c. The Commission shall determine the date from which the MID is to start operations by means of an implementing act when the following conditions are met:

(a) the measures referred to in Articles 28(5), 28(7), 32(4a), 33(4a), 44(5) and 47a(6) have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the MID, which is to be conducted by eu-LISA in cooperation with the Member States 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 as referred to in Article 61(3);

(e) eu-LISA has declared the successful completion of the tests referred to in paragraphs 1(b), 1a(b), 1b(b) and 1d(b).

The date referred to in the first subparagraph shall be set for within 30 days from the decision of the Commission.

1d. The Commission shall decide the date from which the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum quality standards are to be used by means of implementing acts when the following conditions are 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 quality standards, which is to be conducted by eu-LISA in cooperation with the Member States.

The date referred to in the first subparagraph shall be set for within 30 days from the decision of the Commission.

1e. (…)

1f. The Commission shall decide the date from which the CRRS is to start operations by means of an implementing act when the following conditions are met:

(a) the measures referred to in Articles 39(5) and 44(5) have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the CRRS, which is to be conducted by eu-LISA in cooperation with the Member States;

(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 date referred to in the first subparagraph shall be set for within 30 days from the decision of the Commission.

2. The Commission shall inform the European Parliament and the Council of the results of the test carried out pursuant to paragraphs 1(b), 1a(b), 1b(b), 1c(b) 1d(b), 1e(b) and 1f(b).

3. The Commission decisions referred to in paragraphs 1, 1a, 1b, 1c, 1d, 1e and 1f shall be published in the Official Journal of the European Union.

4. The Member States, the ETIAS Central Unit and Europol shall start using the each of interoperability components from the date determined by the Commission in accordance with respectively paragraphs 1,1a, 1b and 1c.

Article 63

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), 47a(6), 57(2) and 59(10) shall be conferred on the Commission for a period of five years from [*the date of entry into force of this Regulation*]. 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.

The delegation of power referred to in Articles 28(5), 39(5), 47a(6), 57(2) and 59(10) 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 on Better Law-Making of 13 April 2016.

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

A delegated act adopted pursuant to Articles 28(5), 39(5), 47a (6), 57(2) and 59(10) 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 64

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 65

Advisory group

An Advisory Group shall be established by eu-LISA. During the design and development phase of the interoperability instruments, Article 52(4) to (6) shall apply.

Article 66

Training

1. eu-LISA shall perform tasks related to the provision of training on the technical use of the interoperability components in accordance with Regulation (EU) No 1077/2011.

Member States and Union agencies shall provide their staff authorised to process data from the interoperability components, with appropriate training programme about data security, data quality, data protection rules, the procedures of the data processing and obligations to inform in accordance with Article 32, 33 and 46.

Where appropriate, common training courses on these topics shall be organised at Union level to enhance cooperation and exchange of best practices between staff of Member States and Union agencies which are authorised to process data from the interoperability components. Particular attention shall be paid to the process of multiple-identity detection, including the verification of links and the accompanying need to ensure the safeguards in relation to fundamental rights.

Article 67

Practical handbook

The Commission shall, in close cooperation with the Member States, eu-LISA and other relevant 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 68

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 [*Six months after the entry into force of this Regulation — OPOCE, please replace with the actual date*] and every six months thereafter during the development phase of the interoperability components, eu-LISA shall submit a report to the European Parliament and the Council on the state of play of the development of the interoperability components, 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 the Council explaining in detail how the objectives, in particular relating to planning and costs, were achieved as well as justifying any divergences.

3. (…)

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

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

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

(b) an examination of the results achieved against objectives and the impact on fundamental rights, including in particular an assessment of the impact of the interoperability components on the right to non-discrimination;

(ba) an assessment of the functioning of the web portal, including figures regarding the use of the web portal and the number requests that were resolved;

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

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

(da) an assessment of the use of the CIR for identification;

(db) an assessment of the use of the CIR for preventing, detecting or investigating terrorist offences or other serious criminal offences;

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

(ea) 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.

By one year after the entry into force of this Regulation and every year thereafter until the decisions of the Commission referred to in Article 62 have been taken, the Commission shall submit a report to the European Parliament and 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.

The Commission shall produce an examination of the impact of the MID on the right to non-discrimination two years after the start of operations of the MID. 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 point (b) of paragraph 5.

The evaluations shall include any necessary recommendations. The Commission shall transmit the evaluation report to the European Parliament, to the Council, to the European Data Protection Supervisor and to the European Union Agency for Fundamental Rights established by Council Regulation (EC) No 168/2007.[70]

6. The Member States and Europol shall provide eu-LISA and the Commission with the information necessary to draft the reports referred to in paragraphs 4 and 5. This information shall not jeopardise working methods or include information that reveals sources, staff members or investigations of the designated authorities.

7. eu-LISA shall provide the Commission with the information necessary to produce the evaluations referred to in paragraph 5.

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

8. While respecting the provisions of national law on the publication of sensitive information, and without prejudice to limitations necessary to protect security and public order, prevent crime and guarantee that any national investigation will not be jeopardised, each Member State and Europol shall prepare annual reports on the effectiveness of access to data stored in the CIR for purposes of preventing, detecting or investigation terrorist offences or other serious criminal offences, containing information and statistics on:

(a) the exact purpose of the consultation including the type of terrorist or serious criminal offence;

(b) reasonable grounds given for the substantiated suspicion that the suspect, perpetrator or victim's data is stored in the Eurodac;

(c) the number of requests for access to the CIR for purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences;

(d) the number and type of cases that have ended in successful identifications;

(e) the need and use made of the exceptional case of urgency including those cases where that urgency was not accepted by the ex post verification carried out by the central access point.

7a. A technical solution shall be made available to Member States in order to manage users access requests referred to in Article 22 and to facilitate the collection of the data listed in this paragraph for the purpose of generating statistics referred to in this paragraph. The Commission shall adopt implementing acts concerning the specifications of the technical solution. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

Member State and Europol annual reports shall be transmitted to the Commission by 30 June of the subsequent year.

Article 69

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, the sBMS, the CIR, the MID, the automated data quality control mechanisms and procedures, the common data quality indicators and the minimum quality standards and the CRRS shall apply from the date determined by the Commission respectively in Article 62(1), 62(1a), 62(1b), 62(1c), 62(1d), 62(1e) and 62(1f) with the exception of Articles 6, 12, 17, 25, 38, 42, 52, 54, 55, 60, 61, 63, 64, 65, 67 and 68(1), which shall apply from [*the data of entry into force of this Regulation*].

The provisions relating to the Eurodac shall apply from the date the recast of Regulation (EU) No 603/2013 of the European Parliament and of the Council becomes applicable.

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

Done at Strasbourg,

For the European Parliament

The President

For the Council

The President