Council of the European Union

Brussels, 25 June 2018
(OR. en)

10453/18

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

COSI 162	**VISA 161**
FRONT 195	**FAUXDOC 56**
ASIM 82	**COPEN 229**
DAPIX 203	**CSCI 92**
ENFOPOL 347	**SAP 15**
ENFOCUSTOM 135	**JAI 691**
SIRIS 72	**CT 121**
SCHENGEN 31	**COMIX 346**
DATAPROTECT 138	**CODEC 1157**

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	9670/18
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226 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) - Mandate for negotiations with the European Parliament

At its meeting on 14 June 2018, the Permanent Representatives Committee agreed on the mandate for negotiations with the European Parliament, as set out in the Annexes.

Changes to the Commission proposals are marked in ***bold/italics*** for additions and in ~~strikethrough~~ for deletions.

ANNEX I

2017/0351 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

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,[2]

Having regard to the opinion of the Committee of the Regions,[3]

Acting in accordance with the ordinary legislative procedure,

---

1 Parliamentary reservation: **FR**.

2 OJ C , , p. .

3

Whereas:

(1) In its Communication of 6 April 2016 entitled *Stronger and Smarter Information Systems for Borders and Security*[4], 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[5], 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[6], 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[7] called for continued delivery on the interoperability of EU information systems and databases.

(5) In its final report of 11 May 2017[8], 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.

(6) In its Communication of 16 May 2017 entitled *Seventh progress report towards an effective and genuine Security Union*[9], 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.

---

4 COM(2016)205, 6.4.2016.

5 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.

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

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

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

9 COM(2017) 261 final, 16.5.2017.

(7) In its Conclusions of 9 June 2017[10] 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[11] 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*** ~~management of~~ the external borders, to contribute to preventing and combating ~~irregular~~ ***illegal im***migration 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 lodged in a Member State,*** 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. To achieve this, a European search portal (ESP), a shared biometric matching service (shared BMS), a common identity repository (CIR) and a multiple-identity detector (MID) should be established as interoperability components.

(10) 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 existing and future EU information systems, strengthen and simplify the data security and data protection safeguards that govern the respective EU information systems, streamline the ~~law enforcement~~ 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 to the extent of enabling it 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 ~~third-country nationals~~ ***persons*** whose personal data ~~is~~ ***are*** processed in the EU information systems and by Europol, ~~and to~~ ***including*** EU citizens whose personal data ~~is~~ ***are*** processed in the SIS and by Europol.

---

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

11 European Council conclusions, 22-23 June 2017.

(13) The European search portal (ESP) should be established to facilitate technically the ability of Member State authorities and EU ~~bodies~~ ***agencies*** to have fast, seamless, efficient, systematic and controlled access to the EU information systems, the Europol data and the Interpol databases 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 result of the query should not be shared in an automated manner with the owner of the Interpol data and a positive result should only be shared following the assessment of the competent authoritities including the Interpol National Central Bureau of the Member State querying the Interpol databases.

(14) The International Criminal Police Organisation (Interpol) database of Stolen and Lost Travel Documents (SLTD) enables authorised ~~law enforcement~~ 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[12], or the national provisions transposing Chapter V of Directive (EU) 2016/680 of the European Parliament and of the Council[13] should apply. This should be without prejudice to the specific rules laid down in Council Common Position 2005/69/JHA[14] and Council Decision 2007/533/JHA[15].

---

12 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).

13 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).

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

15 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).

(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 fast and systematic use of all 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 bodies 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.

(16a) To help fighting identity fraud when consulting national copies of SIS, new biographic identity data from CIR records could be added to an alert in SIS using the existing alias procedures of the Sirene Manual, in case of a red link between data in SIS and the CIR. After adding the new identity data as an alias in the SIS, a new multiple identity detection process should be launched in order to change the existing red link into a white link in an automated manner.

(17) Biometric data, such as ~~fingerprints~~ ***dactyloscopic data*** 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 ~~by relying on one unique technological component instead of different ones in each of the underlying systems~~. 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 in one single location, facilitating cross-system comparisons using biometric data and enabling economies of scale in developing and maintaining the EU central systems.

(18) Biometric data constitute sensitive personal data. This ***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[16], Regulation (EC) No 767/2008 of the European Parliament and of the Council[17], [the ETIAS Regulation] for the management of the borders of the Union, the system established by [the Eurodac Regulation] to identify the applicants for international protection and combat ~~irregular~~ ***illegal im***migration, and the system established by [the ECRIS-TCN system Regulation] require in order to be effective to rely on the accurate identification of the ~~third-country nationals~~ ***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].

(21) Personal data stored in these EU information systems may relate to the same persons but under different or incomplete identities. Member States dispose of efficient ways to identify their citizens or registered permanent residents in their territory, but the same is not true for ***other categories of persons*** ~~third-country nationals~~. The interoperability between EU information systems should contribute to the correct identification of ***those persons*** ~~third-country nationals~~. The common identity repository (CIR) should store the personal data concerning ~~third-country nationals~~ ***those 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. ***However, for the purpose of fighting identity fraud, where a red link is stored in the MID, the linked identity and travel document data should be stored in the CIR for as long as the corresponding data are stored in at least one of the EU information systems from which the linked data originates.***

(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 ~~the~~ identity, ***travel document*** and biometric data ~~of third-country nationals~~ ~~is~~ ***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 system Regulations, as the CIR should be a new shared component of those underlying systems.

---

16 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. 20–82).

17 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).

(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 of ***each person*** ~~third-country nationals~~ 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 ~~law enforcement~~ 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 ~~or prosecution~~ of serious crime.

(25) The common identity repository (CIR) should provide for a shared container for identity, ***travel document*** and biometric data of ~~third-country nationals~~ ***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*** ~~serving~~ as the shared component between ~~these systems~~ ***them*** for storage of ~~this~~ ***the identity, travel document and biometric*** data, and to allow ~~its~~ ***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) In order to ensure the correct identification of a person, ***police authorities empowered by national law*** ~~Member State authorities competent for preventing and combating irregular migration and competent authorities within the meaning of Article 3(7) of Directive 2016/680~~ should be allowed to query the common identity repository (CIR) with the biometric data of that person taken during an identity check.

(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*** ~~legislative measures~~.

(30) This Regulation should also introduce~~s~~ 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 ~~law enforcement~~ 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, investigation and prosecution of terrorist offences or serious criminal offences in a specific case.

(31) Full access to the necessary data contained in the EU information systems necessary for the purposes of preventing, detecting ~~and~~ ***or*** investigating terrorist offences or other serious criminal offences, beyond the relevant identity data ***or travel document data*** covered under common identity repository (CIR) ~~obtained using biometric data of that person taken during an identity check~~, should continue to be governed by the provisions in the respective legal instruments. The designated ~~law enforcement~~ 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*** ~~hit~~ in the system (a so-called ~~hit~~***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 ~~third country national~~, but may 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 2016/680 or Regulation (EC) No 45/2001.

(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 ~~and~~ ***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 ~~hit~~***match***-flag type of response indicating the data ***are*** ~~is~~ recorded in the EES, the VIS, [the ETIAS] or Eurodac requires automated processing of personal data. A ~~hit~~***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 ~~hit~~***match***-flag. Access by the end-user ***to*** ~~of~~ a ~~hit~~***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*** ~~for~~ personal data more effectively directly to the system that was flagged as containing it.

(34) The two-step data consultation approach is particularly valuable in cases where the suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence is unknown. In those cases the common identity repository (CIR) should enable identifying the information system that knows the person in one single search. By creating the obligation to use this new ~~law-enforcement~~ access approach ***for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences*** in these cases, access to the personal data stored in the EES ~~the VIS, [the ETIAS]~~ and Eurodac should take place without the requirements of a prior search in national databases and the launch of a prior search in the automated fingerprint identification system of other Member States under Decision 2008/615/JHA. The principle of prior search effectively limits the possibility of Member State***s***' authorities to consult ***centralised*** systems for ***the*** justified ~~law-enforcement~~ purposes ***of preventing, detecting or investigating terrorist offences or other serious criminal offences*** and could thereby result in missed opportunities to uncover necessary information. The requirements of a prior search in national databases and the launch of a prior search in the automated fingerprint identification system of other Member States under Decision 2008/615/JHA should only cease to apply once the alternative safeguard of the two-step approach to ~~law-enforcement~~ access ***for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences*** through the CIR has become operational.

(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) The possibility to achieve the objectives of the EU information systems is undermined by the current inability for the authorities using these systems to conduct sufficiently reliable verifications of the identities of the ~~third-country nationals~~ ***persons*** whose data are stored in different systems. That inability is determined by the fact that the set of identity data ***or travel document data*** stored in a given individual system may be fraudulent, incorrect, or incomplete, and that there is currently no possibility to detect such fraudulent, incorrect or incomplete 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 ~~third-country nationals~~ ***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*** ~~lawfully~~ or ~~unlawfully~~ ***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 and the fight against ~~irregular~~ ***illegal im***migration.

(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 EU ***agency*** ~~body~~. 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 ~~third-country national~~ ***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 ~~third-country national~~ ***person***.

(40) The national authority or EU ***agency*** ~~body~~ 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) Access to the multiple-identity detector (MID) by Member State authorities and EU ***agencies*** ~~bodies~~ having access to at least one EU information system included in the common identity repository (CIR) or to the SIS should be limited to so called red links where the linked data shares the same biometric but different identity data and the authority responsible for the verification of different identities concluded it refers ~~unlawfully~~ to the same person ***in an unjustified manner***, or where the linked data has ~~similar~~ ***different*** identity data, ***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 ~~unlawfully~~ to the same person ***in an unjustified manner, or where the linked data have same or similar identity data, the same travel document data, but different biometric data and the authority responsible for the verification of different identities concluded it refers to different persons in an unjustified manner***. Where the linked identity data ***are*** ~~is~~ not similar, a yellow link should be established and a manual verification should take place in order to confirm the link or change its colour accordingly.

(42) The manual verification of multiple identities should be ensured by the authority creating or updating the data that triggered a ~~hit~~ ***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 lawful or unlawful identities. Such assessment should be performed where possible in the presence of the ~~third-country national~~ ***person*** 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.

(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, on persons for discreet checks or specific checks or on unknown wanted persons, 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) Access to the MID by Member State authorities and EU agencies is not foreseen where a white link exists between data from two or more EU information systems. However, this will not affect the users' access rights. Where it becomes evident when accessing data from two or more EU information systems that a white link was wrongly created, that Member State authority or EU agency should be able 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) UMF is not meant as a mandatory, sole or preferred standard for the whole field of Justice and Home Affairs and the diverse solutions deployed by the European Commission, the EU agencies and 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. 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 and should record such anonymous 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) ***No*** 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, when Directive (EU) ***No*** 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) No 2016/680 applies.[18]

(49) The specific provisions on data protection of ~~[the EES~~ Regulation ***(EU) 2017/2226***~~]~~, Regulation (EC) No 767/2008, [the ETIAS Regulation] and [the Regulation on SIS in the field of border checks] should apply to the processing of personal data in those respective systems.

(50) Regulation (EC) No 45/2001 of the European Parliament and of the Council**[19]** 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) ***No*** 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 (EC) No 45/2001 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.

(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*** ~~... "~~

(53) Insofar as confidentiality is concerned, the relevant provisions of the Staff Regulations of officials and the Conditions of Employment of other servants of the European Union should apply to officials or other servants employed and working in connection with SIS.

(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.

---

18 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) No 2016/680 applies."

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

(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 the Regulation (EU) ***No*** 2016/399 of the European Parliament and of the Council[20] 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 ~~third-country nationals~~ ***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) However, an amendment of Regulation (EU) 2016/399 would be required in order to add the obligation for the border guard to refer a third-country national to second-line check in case the consultation of the multiple-identity detector (MID) through the European search portal (ESP) would indicate the existence of a yellow link or a red link, in view of not prolonging the waiting time in the first-line checks.~~

(59) Should the query of the multiple-identity detector (MID) through the European search portal (ESP) result in a yellow link or detect a red link, the border guard ~~on second line~~ 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*** ~~bodies~~ 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 EU ***agencies*** ~~bodies~~ 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.

---

20 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.

(62) The costs for the development of the interoperability components projected under the current Multiannual Financial Framework are lower than the remaining amount on the budget earmarked for Smart Borders in Regulation (EU) No 515/2014 of the European Parliament and the Council[21]. Accordingly, this Regulation, pursuant to Article 5(5)(b) of Regulation (EU) No 515/2014, should reallocate the amount currently attributed for developing IT systems supporting the management of migration flows across the external borders.

(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)*** ~~profiles for the users of the European search portal (ESP) and the content and format of the ESP replies~~. 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[22]. 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); format of the ESP replies; performance requirements and performance monitoring of the shared BMS;*** automated data quality control mechanisms, procedures and indicators; development of the UMF standard; procedures for determining cases of similarity of identities; ~~the~~ operation of the central repository for reporting and statistics; ~~and~~ cooperation procedure in case of security incidents***; and specifications of the technical solution to facilitate the querying of EU information systems and the CIR***. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[23].

(65) Regulation ***(EU)*** 2016/794 shall apply for any processing of Europol data for the purposes of this Regulation.

---

21 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).

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

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

(65a) 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) No 2016/679, Directive (EU) No 2016/680 and Regulation (EC) No 45/2001. 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[24]; the United Kingdom is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(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[25]; 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[26] which fall within the area referred to in Article 1, points A, B and G of Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of that Agreement[27].

---

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

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

26 OJ L 176, 10.7.1999, p. 36

27 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[28] which fall within the area referred to in Article 1, points A, B and G of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/146/EC[29].

(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*[30] which fall within the area referred to in Article 1, points A, B and G of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU[31].

(74) As regards Cyprus, the provisions related to the SIS and the VIS constitute provisions building upon, or otherwise related to, the Schengen acquis within the meaning of Article 3(2) of the 2003 Act of Accession.

(75) As regards Bulgaria and Romania, the provisions related to the SIS and the VIS constitute provisions building upon, or otherwise related to, the Schengen acquis within the meaning of Article 4(2) of the 2005 Act of Accession read in conjunction with Council Decision 2010/365/EU[32] and Council Decision (EU) 2017/1908[33].

(76) As regards Croatia, the provisions related to the SIS and the VIS constitute provisions building upon, or otherwise related to, the Schengen acquis within the meaning of Article 4(2) of the 2011 Act of Accession read in conjunction with Council Decision (EU) 2017/733[34].

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

---

28 OJ L 53, 27.2.2008, p. 52.

29 OJ L 53, 27.2.2008, p. 1.

30 OJ L 160, 18.6.2011, p. 21.

31 OJ L 160, 18.6.2011, p. 19.

32 Council Decision 2010/365/EU of 29 June 2010 on the application of the provisions of the Schengen acquis relating to the Schengen information System in the Republic of Bulgaria and Romania, OJ L 166, 1.7.2010, p. 17.

33 Council Decision (EU) 2017/1908 of 12 October 2017 on the putting into effect of certain provisions of the Schengen acquis relating to the Visa Information System in the Republic of Bulgaria and Romania, OJ M 269, 19.10.2017, p. 39.

34 Council Decision (EU) 2017/733 of 25 April 2017 on the application of the provisions of the Schengen acquis relating to the Schengen information System in the Republic of Croatia, OJ L 108, 26.4.2017, p. 31.

(78) In order to have this Regulation fit into the existing legal framework, ~~the~~ 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:

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)] 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 and operation of the interoperability components.

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

Article 2
Objectives ~~of interoperability~~

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

   (a) ***to improve the effectiveness and efficiency of checks at the external borders***; ~~to improve the management of the external borders~~;

   (b) to contribute to preventing and combating ~~irregular~~ ***illegal im***migration;

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

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

   (e) to assist in examining application***s*** for international protection ***lodged in a Member State***;

   (f) in the event of a natural disaster or an accident, for humanitarian reasons, to assist in the identification of unknown persons who are not able to identify themselves or unidentified human remains.

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

   (a) ensuring the correct identification of persons;

   (b) contributing to fighting identity fraud;

   (c) improving and harmonising data quality requirements of the respective EU information systems ***while respecting the data processing requirements of the legal bases of the individual systems, data protection standards and ~~the data owner~~ principles***;

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

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

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

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

Article 3
Scope

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

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

Article 4
Definitions

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

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

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

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

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

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

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

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

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

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

(10) ***‘dactyloscopic data’ means fingerprints images, images of fingerprint latents, palm prints, and palm prints latents[35] which due to their unique character and the reference points contained therein enable accurate and conclusive comparisons on a person's identity***; ~~‘fingerprint data’ means the data relating to the fingerprints of an individual~~;

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

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

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

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

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

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

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

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

(19) ‘Europol data’ means personal data ***processed by*** ~~provided to~~ 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);

---

35 *NB: Same definition as in Council Decision 2008/616/JHA.*

(21) ‘match’ means the existence of a correspondence ***as a result of an automated comparison between*** ~~established by comparing two or more occurrences of~~ personal data recorded or being recorded in an information system or database;

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

(23) 'police authority' means 'competent authority' as defined in Article 3(7) of Directive ***No*** 2016/680;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Article 5
Non-discrimination

Processing of personal data for the purposes of this Regulation shall not result in discrimination against persons on any grounds such as ***gender*** ~~sex~~, racial or ethnic origin, religion or belief, disability, age or sexual orientation. It shall fully respect human dignity and integrity. ~~Particular attention shall be paid to children, the elderly and persons with a disability~~.

CHAPTER II
European Search Portal

Article 6
European search portal

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

2. The ESP shall be composed of:

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

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

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

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

Article 7

Use of the European search portal

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

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

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

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

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

Article 8
Profiles for the users of the European search portal

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

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

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

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

2. The Commission shall adopt ***implementing*** ~~delegated~~ acts ~~in accordance with Article 63~~ to specify the technical details of the profiles referred to in paragraph 1 for the users of the ESP referred to in Article 7(1) in accordance with their access rights. ***Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).***

Article 9
Queries

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

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

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

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

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

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

7. The Commission shall adopt an ***implementing*** ~~delegated~~ act ~~in accordance with Article 63~~ to specify ***the process for querying the EU information systems, Europol data and Interpol databases by the ESP and*** the ~~content and~~ 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 the ~~EES~~ Regulation ***(EU) 2017/2226***~~]~~, Article 34 of Regulation (EC) No 767/2008, [Article 59 of the ETIAS proposal] and Articles 12 and 18 of the Regulation on SIS in the field of border checks, eu-LISA shall keep logs of all data processing operations within the ESP. Those logs shall include~~, in particular,~~ the following:

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

   (b) the date and time of the query;

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

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

1a. Each Member State shall keep logs of queries of the authority and the staff duly authorised to use the ESP including the transaction identification number referred to in point (d) of paragraph 1.

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 pursuant to Article 42. Those logs shall be ***made available to the competent supervisory authority on request. They shall be*** protected by appropriate measures against unauthorised access ***and modifications*** and erased one year after their creation, unless they are required for monitoring procedures that have already begun ***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 ***automatically*** by eu-LISA.

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

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

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

CHAPTER III
Shared Biometric Matching Service

Article 12
Shared biometric matching service

1. A shared biometric matching service (shared BMS) storing biometric templates ***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 ***Common Identity Repository (***CIR***)*** and the multiple-identity detector ***(MID)*** and the objectives of the EES, the VIS, Eurodac, the SIS and [the ECRIS-TCN system].

2. The shared BMS shall be composed of:

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

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

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

Article 13
Data stored in the shared biometric matching service

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

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

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

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

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

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

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

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

The shared BMS shall store the biometric templates - logically separated - according to the EU information system from which the data originated.

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.

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

3. Biometric templates ~~shall only~~ ***may*** be entered ***only*** 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) ***and (4)***.

5. The Commission shall lay down the performance requirements and performance monitoring of the shared BMS, including the minimum requirements regarding the biometric performance of the shared BMS, in particular in terms of the required False Positive Identification Rate, False Negative Identification Rate and Failure To Enrol Rate, as well as the procedures and tools for notifying False Positive Identifications and False Negative verifications to eu-LISA in implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

For the specific purpose of monitoring the performance of the shared BMS, Member States shall be allowed to use the biometric templates stored in the shared BMS.

Article 14

Searching biometric data with the shared biometric matching service

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

Article 15

Data retention in the shared biometric matching service

The data referred to in Article 13***(1) and (2)*** shall be stored in the shared BMS for as long as the corresponding biometric data ***are*** ~~is~~ 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 ~~the EES~~ Regulation~~]~~ ***(EU) 2017/2226***, Article 34 of Regulation (EC) No 767/2008 and [Article 12 and 18 of the Regulation on SIS in the field of ~~law enforcement~~ ***border checks***], eu-LISA shall keep logs of all data processing operations within the shared BMS. Those logs shall include~~, in particular,~~ the following:

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

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

   (c) the date and time of the query;

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

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

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

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

1a. Each Member State 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 pursuant to Article 42. Those logs shall be ***made available to the competent supervisory authority on request. They shall*** protected by appropriate measures against unauthorised access ***and modifications*** and erased one year after their creation, unless they are required for monitoring procedures that have already begun, ***in which case they shall be erased once the monitoring procedures no longer require these logs***. The logs referred to in paragraph 1(a) shall be erased once the data ***are*** ~~is~~ erased.

CHAPTER IV
Common Identity Repository

Article 17
Common identity repository

1. A common identity repository (CIR), creating an individual file for each person that is recorded in the EES, the VIS, [the ETIAS], Eurodac or [the ECRIS-TCN system] containing the data referred to in Article 18, is established for the purpose of facilitating and assisting the correct identification of persons registered in the EES, the VIS, [the ETIAS], the Eurodac and [the ECRIS-TCN system] ***in accordance with Article 20***, of supporting the functioning of the multiple-identity detector ***in accordance with Article 21*** and of facilitating and streamlining access by ~~law enforcement~~ ***designated*** authorities ***and Europol*** to non-law enforcement ***EU*** information systems ~~at EU level~~, where necessary for the prevention, ~~investigation,~~ detection ***or investigation*** ~~or prosecution~~ ***of terrorist offences or other*** ~~of~~ serious ~~crime~~ ***criminal offences 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 EU ***agencies*** ~~bodies~~ that are entitled to use the ~~European search portal (ESP)~~ ***CIR*** in accordance with Union law ***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 ~~multiple-identity detector~~ ***MID***.

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

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

Article 18
The common identity repository data

1. The CIR shall store the following data – logically separated – according to the ***EU*** information system from which the data was originated:

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

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

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

   ~~(d) (not applicable)~~

   ~~(e) (not applicable)~~

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

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

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

Article 19
Adding, amending and deleting data in the common identity repository

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

2. Where ~~the multiple-identity detector creates~~ a white or red link ***is created in the MID*** in accordance with Articles 32 ~~and~~ ***or*** 33 between the data of two or more of the EU information systems constituting the CIR, instead of creating a new individual file, the CIR shall add the new data to the individual file of the linked data.

Article 20

Access to the common identity repository for identification

1. Where a ~~Member State~~ police authority has been so empowered by national legislative measures as referred to in paragraph 2, it may, solely for the purpose of identifying a person, query the CIR with the biometric data of that person taken during an identity check.

1a. ***Where a police authority has been so empowered by national legislative measures as referred to in paragraph 2a, it may, for the purpose of identifying unknown persons who are not able to identify themselves or unidentified human remains, in the event of a ~~natural~~ disaster or an accident, query the CIR with the biometric data of those persons.***

1b. Where the query indicates that data on that person is stored in the CIR, the ~~Member States~~ ***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.

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

2a. Member States wishing to avail themselves of the possibility provided for in paragraph 1a 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 ~~identity~~ 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 ~~identity~~ 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 ~~law enforcement~~ purposes ***of preventing, detecting or investigating terrorist offences or other serious criminal offences***

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

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

3. Where, in reply to a query, the CIR indicates data on that person is present in the EES, the VIS and [the ETIAS], the CIR shall provide to ~~Member States'~~ designated authorities and Europol a reply in the form of a reference indicating which of the ***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 those systems may be used only for the purpose of submitting an access request subject to the conditions and procedures laid down in the respective legislative instruments governing such access.***

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

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

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

Article 24
Keeping of logs

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

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

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

   (b) the date and time of the query;

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

   (d) the results of the query;

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

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

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

(b) the date and time of the query;

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

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

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

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

~~(a) the national file reference;~~

(b) the date and time of the query;

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

(d) the results of the query;

(e) the ~~name of the authority~~ ***Member State or EU agency querying*** ~~consulting~~ the CIR;

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

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

5. Each Member State shall keep logs of queries of ***the 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;

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

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

CHAPTER V
Multiple-identity Detector

Article 25
Multiple-identity detector

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

2. The MID shall be composed of:

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

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

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

Article 26
Access to the multiple-identity detector

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

   (a) ~~border~~ ***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*** ~~as provided for in~~ Article 14 of ***that*** ~~the [EES~~ Regulation~~]~~;

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

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

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

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

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

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

Article 27
Multiple-identity detection

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

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

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

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

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

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

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

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

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

(a) surname (family name); first name(s) (given name(s)); date of birth, sex and nationality(ies) as referred to in Article 16(1)(a) ***as well as the relevant data referred to in Articles 17(1) and 18(1)*** of ~~the [EES~~ Regulation ***(EU) 2017/2226***~~]~~;

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

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

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

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

~~(f) (not applicable);~~

~~(g) (not applicable);~~

~~(h) (not applicable).~~

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

4. The multiple-identity detection ***may*** ~~shall only~~ be launched ***only*** 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 (3***a***) do not report any ***match*** ~~hit~~, 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 (3***a***) reports one or several ***match(es)*** ~~hit(s)~~, the common identity repository and, where relevant, the SIS shall create a link between the data used to launch the query and the data triggering the ***match*** ~~hit~~.

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

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

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

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

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

7. The Commission shall lay down the technical rules for ~~linking data~~ ***creating links between data*** from different ***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 m*anual verification of different identities*

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

   (a) the ~~border~~ ***competent*** authority ***referred to in Article 9(2) of Regulation (EU) 2017/2226*** for ~~hits~~ ***matches*** that occurred when creating or updating an individual ***file*** in ~~[~~the EES in accordance with ~~Article 14 of~~ ***that*** ~~the EES~~ Regulation~~]~~;

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

   (c) [the ETIAS Central Unit and the ETIAS National Units for ~~hits~~ ***matches*** that occurred ***when creating or updating an application file*** in accordance with ~~Articles 18, 20 and 22 of~~ the ETIAS Regulation;]

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

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

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

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

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

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

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

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

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

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

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

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

4. Where the authority responsible for the verification of different identities in the identity confirmation file is the ~~border~~ ***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 ~~the EES~~ Regulation ***(EU) 2017/2226***, and where a yellow link is ***created*** ~~obtained~~, ***that*** ~~the~~ ~~border~~ authority shall carry out additional verifications ~~as part of a second-line check. During this second-line check, t~~ ~~***T***~~he ***That*** ~~border~~ authorit**y~~ies~~ shall have access to the related data contained in the relevant identity confirmation file and shall assess the different identities and shall update the link in accordance with Articles 31 to 33 and add it to the identity confirmation file without delay.

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

6. Where data reporting a ~~hit~~ ***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 different identity data and no manual verification of different identity has taken place;

   (b) the linked data has ~~different~~ ***some differences in the*** identity data ***or in travel document data***, ~~and~~ 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***;

   (c) the linked data has same or similar 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 the linked data do not share the same biometric ***data*** but have ***same or*** similar identity data and the authority responsible for the verification of different identities concluded it refers to two different persons.

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

Article 32
Red link

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

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

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

   (c) the linked data has different identity data, 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;

   (d) the linked data has same or similar identity data, the same travel document data, but different biometric data and the authority responsible for the verification of different identities concluded it refers to different persons 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 ***EU*** information systems constituting the CIR or with the SIS, the multiple-identity detector shall reply indicating the data referred to in Article 34. Follow-up to a red link shall take place in accordance with Union and national law, ***basing any legal consequence for the person only on the relevant data on that person and not on the red link itself.***

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

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

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 authority responsible for verification of different identities shall provide a reference to the authorities responsible for the data linked.~~

6. If a Member State authority has evidence to suggest that a red link recorded in the MID is factually inacurate or not up-to-date or that data were processed in the MID, the CIR or the SIS in breach of this Regulation, it shall check the relevant data stored in the CIR and SIS and shall, if necessary, rectify or erase the link from the MID without delay. That Member State authority shall inform the Member State responsible for the manual verification without delay.

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, ~~and~~ ***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 or similar identity 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 the same person ~~legally~~ having different identity data in a justified manner;

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

2. Where the CIR or the SIS are queried and where a white link exists between ~~one~~ ***two*** or more of the ***EU*** information systems constituting the CIR or with the SIS, the ~~multiple-identity detector~~ ***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 ~~hit~~ ***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~~(1)~~***(2)***.

4. ~~Without prejudice to the provisions related to the handling of alerts in the SIS referred to in the [Regulations on SIS in the field of border checks, on SIS in the field of law enforcement and on SIS in the field of illegal return],~~ ~~w~~***W***here a white link is created following a manual verification of multiple identities ***between data from the EES, the VIS, [the ETIAS] or Eurodac***, the authority responsible for ***the*** verification of different identities shall inform the person of the presence of discrepancies between his or her personal data between systems and shall provide a reference to the authorities responsible for the data linked.

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

Article 34
Identity confirmation file

The identity confirmation file shall contain the following data:

(a) the links~~, including their description in form of colours,~~ as referred to in Articles 30 to 33;

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

(c) a single identification number allowing to retrieve the data from the ***EU*** information systems of corresponding linked files ***in accordance with respective access rights under Union and national law***;

(d) ~~where relevant,~~ the authority responsible for the verification of different identities;

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

Article 35
Data retention in the multiple-identity detector

1. ***Without prejudice to paragraphs 2 and 3,*** the identity confirmation files and ~~its~~ ***their*** data, including the links, shall be stored in the ~~multiple-identity detector (~~MID~~)~~ only for as long as the linked data ***are*** ~~is~~ stored in two or more EU information systems ***and be deleted thereafter in an automated manner***.

2. ***Where a red link is created between data in the CIR, the identity confirmation files and their data, including the red link, shall be stored in the MID only for as long as the corresponding data are stored in at least one of the EU information systems from which the linked data originates and be deleted thereafter in an automated manner***.

3. ***Where a red link is created between data in the CIR and the SIS, the identity confirmation files and their data, including the red link, shall be stored in the MID only for as long as the corresponding data are stored in the SIS 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~~, in particular,~~ the following:

   ~~(a) the purpose of access of the user and his or her access rights;~~

   (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;

   (f) the ~~identifying mark of the person who carried out the query~~ ***Member State or EU agency querying the MID***.

2. Each Member State shall keep logs of the ***authority, the purpose of access 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 request and the lawfulness of data processing, and for ensuring data security pursuant to Article 42. Those logs shall be ***made available to the competent supervisory authority on request. They shall*** be protected by appropriate measures against unauthorised access ***and modification.*** ~~and~~ ***They shall be*** erased ***in an automated manner*** 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 those logs***. The logs related to the history of the identity confirmation file shall be erased once the data in the identity confirmation file is erased.

CHAPTER VI
Measures supporting interoperability

Article 37
Data quality

1. ***Without prejudice to Member States' responsibilities with regard to the quality of data entered into the systems,*** eu-LISA shall establish automated data quality control mechanisms and procedures on the data stored in the EES, ***the VIS,*** the [ETIAS], ~~the VIS,~~ the SIS, the shared biometric matching service (shared BMS)~~,~~ ***and*** the common identity repository (CIR) ~~and the multiple-identity detector (MID)~~.

2. eu-LISA shall ~~establish~~ ***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 VIS,~~ the SIS, the shared BMS~~,~~ ***and*** the CIR ~~and the MID~~.

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

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

5. One year after the establishment of the automated data quality control mechanisms and procedures, ~~and~~ common data quality indicators ***and 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 shall ***regularly*** report on any progress against this action plan until it is fully implemented.

   The Commission shall transmit the evaluation report to the European Parliament, to the Council, to the European Data Protection Supervisor and to the European Union Agency for Fundamental Rights established by Council Regulation (EC) No 168/2007.[36]

[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).

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 **A**~~a~~ffairs.

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

3. The implementation of the UMF standard may be considered in the 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 ~~or associated countries~~.

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

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***, as well as the Schengen Evaluation Mechanism provided for in Regulation (EU) No 1053/2013,*** and to generate***, in accordance with the respective legal instruments,*** cross-system statistical data and analytical reporting for policy, operational and data quality purposes.

2. eu-LISA shall establish, implement and host the CRRS in its technical sites containing the data referred to in [Article 63 of the EES Regulation], Article 17 of Regulation (EC) No 767/2008, [Article 73 of the ETIAS Regulation] and [Article 54 of the Regulation on SIS in the field of border checks], logically separated. The data contained in the CRRS shall not enable the identification of individuals. Access to the ~~repository~~ ***CRRS*** shall be granted by means of secured access ~~through the Trans- European Services for Telematics between Administrations (TESTA) network service~~ with control of access and specific user profiles, solely for the purpose of reporting and statistics, to the authorities referred to in [Article 63 of the EES Regulation], Article 17 of Regulation (EC) No 767/2008, [Article 73 of the ETIAS Regulation] and [Article 54 of the Regulation on SIS in the field of border checks]~~,~~.

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

4. The CRRS shall be composed of:

(-a) the tools necessary for anonymising data;

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

(b) a secure communication infrastructure to connect the CRRS to the EES, ***the VIS,*** [the ETIAS], ~~the VIS~~ 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***s*** 2 and 3 and security rules applicable to the repository by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

CHAPTER VII
Data protection

Article 40
Data controller

1. In relation to the processing of data in the shared biometric matching service (shared BMS), the Member State authorities that are controllers for the ~~VIS,~~ EES, ***the VIS*** and SIS respectively, shall ~~also~~ be ~~considered as~~ 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 ~~VIS,~~ EES***, the VIS*** and [ETIAS], respectively, shall ~~also~~ be ~~considered as~~ controllers in accordance with Article 4(7) of Regulation (EU) 2016/679 in relation to data referred to in Article 18 that they enter into respective systems and shall have responsibility for the processing of that personal data in the CIR.

3. In relation to the processing of data in the multiple-identity detector ***(MID)***:

   (a) the European Border and Coast Guard Agency shall be ~~considered~~ a data controller in accordance with Article 2~~(b)~~***(d)*** of Regulation No 45/2001 ***[or Article 3(2)(b) of Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC]*** 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 ~~are also to be considered as~~ ***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 ~~multiple-identity detector~~ ***MID;.***

Article 41
Data processor

In relation to the processing of personal data in ***the shared BMS,*** the CIR ***and the MID***, eu-LISA **shall** ~~is to~~ be ~~considered~~ the data processor in accordance with Article 2(e) of Regulation (EC) No 45/2001 ***[or Article 3(1)(a) of Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC]***.

Article 42
Security of processing

1. ~~Both~~ 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 22 of Regulation (EC) No 45/2001 ***[or Article 33 of Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC]***, 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 ***security*** measures, including a security plan, a business continuity plan and a disaster recovery plan, in order to:

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

   (b) 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;

(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 has 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;

(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.

4. Member States***, [the ETIAS Central Unit] and Europol*** 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
Confidentiality of SIS data

1. Each Member State shall apply its rules of professional secrecy or other equivalent duties of confidentiality to all persons and bodies required to work with SIS data accessed through any of the interoperability components in accordance with its national law. That obligation shall also apply after those persons leave office or employment or after the termination of the activities of those bodies.

2. Without prejudice to Article 17 of the Staff Regulations of officials and the Conditions of Employment of other servants of the European Union, eu-LISA shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality of comparable standards to those laid down in paragraph 1 to all its staff required to work with SIS data. This obligation shall also apply after those persons leave office or employment or after the termination of their activities.

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 and the European Data Protection Supervisor of ***any*** security incident~~s~~.

   Without prejudice to Article 35 of Regulation (EC) 45/2001 [or Article 37 of Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC] 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.

   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*** 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 EU ***agencies*** ~~bodies~~ 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 logs, and cooperate, where necessary, with the supervisory authorities referred to in Article~~s~~ 49 and ***with the European Data Protection Supervisor as referred to in Article*** 50.

Article 46
Right of information

1. Without prejudice to the right of information referred to in Articles 11 and 12 of Regulation (EC) 45/2001 ***[or Articles 15 and 16 of Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC], Articles 13 and 14 of Directive (EU) 2016/680*** and Articles 13 and 14 of Regulation (EU) 2016/679, persons whose data are stored in the shared ~~biometric matching service~~ ***BMS***, the ~~common identity repository~~ ***CIR*** or the ~~multiple-identity detector~~ ***MID*** shall be informed by the ~~authority collecting their data~~ ***data controller***, at the time their data are collected ***in accordance with paragraph 2***, about the processing of personal data for the purposes of this Regulation, including about identity and contact details of the respective data controllers, ***about the period for which the personal data will be stored or about the criteria used to determine that period,*** ~~and~~ about the procedures for exercising their rights of access, rectification and erasure, as well as about the contact details of the European Data Protection Supervisor and of the national supervisory authority of the Member State responsible for the collection of the data.

2. Persons whose data ***are*** ~~is~~ 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 the EES Regulation];

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

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

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

~~(e) (not applicable).~~

Article 47

Right of access, ~~correction~~ ***rectification*** *and erasure* ***of data stored in the MID***

1. In order to exercise their rights under Articles 13, 14, 15 and 16 of Regulation (EC) 45/2001 ***[or Articles 17, 18, 19 and 20 of Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC], Article 16 of Directive (EU) 2016/680*** and Articles 15, 16, 17 and 18 of Regulation (EU) 2016/679, any person shall have the right to address him or herself to the ~~Member State responsible for the manual verification of different identities or~~ ***competent authority*** of any Member State, who shall examine and reply to the request.

2. ~~The Member State responsible for the manual verification of different identities as referred to in Article 29 or the Member State to which the request has been made~~ ***The Member State which examined such request*** shall reply ~~to such requests~~ within ~~45~~ ***60*** days of receipt of the request. ***Member States may decide that these replies are given by central offices.***

3. If a request for ~~correction~~ ***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***.*** ~~and t~~***T***he Member State responsible ***for the manual verification of different identities*** shall check the accuracy of the data and the lawfulness of the data processing within ~~30~~ ***45*** days of such contact.

3a. ***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 within 45 days of such contact.***

4. Where, following an examination, it is found that the data stored in the ~~multiple-identity detector (~~MID~~)~~ are ~~factually~~ 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*** ~~applicable,~~ the Member State to which the request has been made shall correct or delete these data.

5. Where data ***stored*** in the MID is amended by ***a*** ~~the responsible~~ Member State during its validity period, ~~the responsible~~ ***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 ~~hit~~ ***match***, ~~the responsible~~ ***that*** Member State ~~or, where applicable, the Member State to which the request has been made~~ shall delete the data from the identity confirmation file. Where the automated processing reports one or several ***match(es)*** ~~hit(s)~~, ~~the responsible~~ ***that*** Member State shall create or update the relevant link in accordance with the relevant provisions of this Regulation.

6. Where the ~~responsible~~ 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 ~~factually~~ 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 rectification or erasure of personal data*** ~~referred in paragraph 3~~ 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 ~~competent~~ national supervisory authorities.

8. Any request ***for rectification or erasure of personal data*** ~~made pursuant to paragraph 3~~ 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 ~~paragraph 3~~ ***this Article*** and shall be erased immediately afterwards.

9. The ~~responsible~~ 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 rectification or erasure of personal data*** ~~referred to in paragraph 3~~ was made and how it was addressed, and shall make that document available to ~~competent data protection~~ national supervisory authorities without delay.

Article 47a[37]
Penalties

Member States shall lay down the rules on penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.

Article 47b
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 (EC) 45/2001:

(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 eu-LISA incompatible with this Regulation shall be entitled to receive compensation from that agency. eu-LISA shall be liable for unlawful personal data processing operations in accordance with its role as processor or, where applicable, controller.

That Member State 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 held liable for such damage, unless and insofar as eu-LISA or another Member State participating in the interoperability components 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.

[37] Articles 47a and 47b are copied from the text agreed with the EP on the ETIAS Regulation.

Article 48

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

Without prejudice to [Article 55 of the ETIAS Regulation], Article 41 of Regulation (EU) 2017/2226, and Article 31 of Regulation (EC) 767/2008, ~~P~~***p***ersonal data stored in or accessed by the interoperability components shall not be transferred or made available to any third country, to any international organisation or to any private party, with the exception of transfers to Interpol for the purpose of carrying out the automated processing referred to in [Article 18(2)(b) and (m) of the ETIAS Regulation] or for the purposes of Article 8(2) of Regulation (EU) 2016/399. Such transfers of personal data to Interpol shall be compliant with the provisions of Article 9 of Regulation (EC) No 45/2001 ***[or Chapter V of Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC]*** and Chapter V of Regulation (EU) 2016/679.

Article 49

Supervision by the ~~*national*~~ *supervisory* ~~*authority*~~ ***authorities***

1. The supervisory ~~authority or~~ authorities ~~designated pursuant to Article 49 of Regulation (EU) 2016/679~~ 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.

2. Member States shall ensure that their supervisory ~~authority has~~ ***authorities have*** sufficient resources to fulfil the tasks entrusted to ~~it~~ ***them*** under this Regulation.

3. 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.

Article 50
*~~Supervision~~ **Audit** by the European Data Protection Supervisor*

The European Data Protection Supervisor shall ensure that an audit of ~~eu-LISA's~~ personal data processing ~~activities~~ ***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***,*** ~~and~~ the Member States ***and the EU agency concerned***. eu-LISA***, [the ETIAS Central Unit] and Europol*** shall be given an opportunity to make comments before the reports are adopted.

Article 51
Cooperation between ~~national~~ supervisory authorities and the European Data Protection Supervisor

1. The European Data Protection Supervisor shall act in close cooperation with national supervisory authorities with respect to specific issues requiring national involvement, 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, or in the context of questions raised by one or more ~~national~~ supervisory authorities on the implementation and interpretation of this Regulation.

2. In the cases referred to in paragraph 1, coordinated supervision shall be ensured in accordance with ***[***Article 62 of Regulation (EU) XXXX/2018 ~~[revised Regulation 45/2001]~~ ***of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC]***.

CHAPTER VIII
Responsibilities

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

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

2. The interoperability components shall be hosted by eu-LISA in its technical sites and shall provide the functionalities laid down in this Regulation in accordance with the conditions of security, availability, quality and ~~speed~~ ***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, and Eurodac, and [the ECRIS-TCN system], and the European search portal ***(ESP)***, the shared biometric matching service ***(BMS)***, the common identity repository ***(CIR),*** ~~and~~ the multiple-identity detector ***(MID) and the central repository for reporting and statistics (CRRS)***.

   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 ~~or VIS~~ deriving from the establishment of interoperability and provided for by this Regulation.

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

   The development shall consist of the elaboration and implementation of the technical specifications, testing and overall project 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 ~~large-scale IT~~ ***EU information*** systems ~~managed by eu-LISA~~ 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 ~~the~~ ***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*** ~~large-scale IT systems managed by eu-LISA~~.

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 ~~and the national uniform interfaces~~. In cooperation with the Member States, it shall ensure ~~at all times~~ the best available technology, 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 necessary to keep the interoperability components functioning ***providing uninterrupted services to the Member States*** 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.

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.

3. eu-LISA shall develop and maintain a mechanism and procedures for carrying out quality checks on the data stored in the shared biometric matching service and the common identity repository 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 ~~European search portal (~~ESP~~)~~ and the ~~common identity repository (~~CIR~~)~~;

(b) the integration of the existing national systems and infrastructures with the ESP, ~~shared biometric matching service,~~ the CIR and the ~~multiple-identity detector~~ ***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 ~~and by the duly empowered staff~~ of the competent national authorities to the ESP, the CIR and the ~~multiple-identity detector~~ ***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~~(3)~~***(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 ~~implementation~~ ***compliance with*** data quality requirements ~~in the EU information systems and in the interoperability components~~ ***established under Union law***;

(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 ~~referred to in Article 4(24)~~ 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***(1)(c)***;

(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) 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 ~~at second line~~ shall consult the multiple-identity detector together with the common identity repository referred to in [Article 4(35) of Regulation 2018/XX on interoperability] or the Schengen Information System or both to assess the differences in the linked identity~~ies~~ ***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 ~~as well as to take a decision on the entry or refusal of entry of the person concerned~~.

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 55b
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 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 (21a) is added:

"'CIR' means the common identity repository as defined in [Article 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 ~~Article 14 and~~ Articles 15 ~~16~~ 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 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 of Regulation 2018/XX on interoperability], the shared biometric matching service established by [Article 12 of Regulation 2018/XX on interoperability], the common identity repository established by [Article 17 of Regulation 2018/XX on interoperability] and the multiple-identity detector established by [Article 25 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), ~~and~~ 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:

"~~3.~~ ***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 EU ***agencies*** ~~bodies~~ 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 EU ***agencies*** ~~bodies~~ 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, ~~both times~~ ***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 reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on interoperability] reveals that data ***are*** ~~is~~ stored in the EES."

14) Article 32(2) is replaced by the following:

"2. Access to the EES as a tool for the purpose of identifying an unknown suspect, perpetrator or suspected victim of a terrorist ~~office~~ ***offence*** or other~~wise~~ serious criminal offence shall only be allowed when a query to the CIR was launched in accordance with [Article 22 of Regulation 2018/XX on interoperability] and all the conditions listed in paragraph 1 and paragraph 1a are met.

However, this additional condition shall not apply in a case of urgency where there is a need to prevent an imminent danger to the life of a person associated with a terrorist offence or another serious criminal offence. Those reasonable grounds shall be included in the electronic or written request sent by the operating unit of the designated authority to the central access point."

15) Article 32(4) is deleted.

16) A new paragraph (1a) 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 reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on interoperability] reveals that data ***are*** ~~is~~ stored in the EES."

16a) Article 33(2), subparagraph 2 is deleted.

17) In Article 33, paragraph 3 is replaced by the following:

"The conditions laid down in Article 32(3) and (5) shall apply accordingly"

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".

18a) In Article 34, a new paragraph 3a is added:

"3a. Where a red link is stored in the multiple identity detector (MID) established by [Article 25 of Regulation 2018/XX on interoperability] in accordance with [Article 32 of Regulation 2018/XX on interoperability], the linked EES data referred to in Article 16(1)(a) to (d) and Article 17(1)(a) to (c) and Article 18(1) and (2)shall be stored in the CIR in accordance with [Article 23(3) of Regulation 2018/XX on interoperability]."

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) ~~where relevant,~~ 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 55c
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 of Regulation 2018/XX on interoperability], shared biometric matching service established by [Article 12 of Regulation 2018/XX on interoperability], the common identity repository and the multiple-identity detector (MID) established by [Article 25 of Regulation 2018/XX on interoperability]".

Article 55d
Amendments to Regulation (EC) 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 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 ~~laid down in paragraph 1 of this Article~~ ***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;

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

(16) ‘biometric data’ means fingerprint data and facial image;"

3) In Article 5, the following paragraph is added:

"1a). The CIR shall contain the data referred to in Article 9(4)(a) to (c~~e~~), 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 EU ***agencies*** ~~bodies~~ 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; ~~nationality or nationalities;~~ 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;

6) Article 9(5) is replaced by the following:

"facial image ~~as defined in Article 4(15)~~".

6a) A second sentence is added in Article 23(1), as follows:

"Where a red link is stored in the multiple identity detector (MID) established by [Article 25 of Regulation 2018/XX on interoperability] in accordance with [Article 32 of Regulation 2018/XX on interoperability], the linked VIS data referred to in Article 9(4)(a) to (cc), 9(5) and 9(6) shall be stored in the CIR in accordance with [Article 23(3) of Regulation 2018/XX on interoperability]".

~~7) In Article 29(2)(a) the word "VIS" is replaced by the words "VIS or the CIR" in both instances where it appears.~~

Article 55e
Amendments to Council Decision 2008/633/JHA

1) A new paragraph (1a) 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], 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 ***are*** ~~is~~ stored in the VIS."

2) A new point (1a) 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], 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 ***are*** ~~is~~ stored in the VIS."

CHAPTER X
Final provisions

Article 55f
Business Continuity

Interoperability of central EU information systems supported by this Regulation shall be accompanied by business continuity solutions, determined and implemented in accordance with [Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011], that ensure uninterrupted availability ~~for CIR and sufficient availability~~ of ~~the other~~ all interoperability components and the data stored therein. In order to ensure operational needs, the Commission, in close cooperation with the Member States and eu-LISA, shall adopt the implementing acts necessary for the development and technical implementation of such solutions ~~facilitating continuous availability of the data stored in the CIR and shared BMS, supported by the MID, and accessed by the ESP. The ESP, the shared BMS, the CIR, the MID and the possible backup solution shall be located in the technical sites of eu-LISA~~.

Article 56
Reporting and statistics

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

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

   (b) 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 common identity repository ***(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, ~~sex~~ ***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 multiple-identity detector ***(MID)***, solely for the purposes of reporting and statistics without enabling individual identification:

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

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

(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;*** ~~.~~

(e) the period of time a yellow link or a red link remained.

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[38] 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 1, 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 paragraph 1 of this Article, eu-LISA shall store the data referred to in paragraph***s*** 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 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.

---

38 Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC (OJ L 251, 16.9.2016, p. 1).

Article 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. ***Following the period referred to in paragraph 1, the Commission, in close cooperation with Member States and eu-LISA, shall assess the impact of the ESP on border checks. On the basis of this assessment, and after consultation with the Member States, the Commission may adopt a delegated act in accordance with Article 63 to extend the period referred to in paragraph 1 until any potential technical issue linked to the ESP has been solved ~~for a maximum of additional two years~~.***

Article 58
Transitional period applicable to the provisions on access to the common identity repository for ~~law enforcement~~ purposes ***of preventing, detecting or investigating terrorist offences or other serious criminal offences***

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

Article 59
Transitional period for the multiple-identity detection

1. For a period of one year following the notification by eu-LISA of the completion of the test referred to in Article 62(1)(b) regarding the ~~multiple-identity detector (~~MID~~)~~ and before the start of operations of the MID, the ETIAS Central Unit as referred to in [Article 33(a) of Regulation (EU) 2016/1624] shall be responsible for carrying out a multiple-identity detection between the data stored in the ***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)*** ~~hit(s)~~ and the identity data of the linked files is identical or similar, a white link shall be created in accordance with Article 33.

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

   Where several ~~hits~~ ***matches*** are reported, a link shall be created to each piece of data triggering the ~~hit~~ ***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 alert or an alert on a travel document reported lost, stolen or invalidated in accordance with Article 24 of the Regulation on SIS in the field of border checks and Article 38 of the Regulation on SIS in the field of law enforcement respectively, the MID shall grant access to the identity data present in the different information systems to the SIRENE Bureau of the Member State that created the alert.

5. The ETIAS Central Unit or the SIRENE Bureau of the Member State that created the alert shall have access to the data contained in the identity confirmation file and shall assess the different identities and shall update the link in accordance with Articles 31, 32 and 33 and add it to the identity confirmation file.

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

7. Where a red link is created between data in the CIR, the identity confirmation file including the red link shall be stored in the MID at least for three years or for as long as the corresponding data are stored in at least one of the EU information systems.

8. Where a red link is created between data in the CIR, the linked data referred to in Article 18(1), (2) and (2a) shall be stored in the CIR at least for three years or for as long as the corresponding data are stored in at least one of the EU information systems.

9. Where a red link is created between data in the CIR and the SIS, the linked data referred to in Article 18(1), (2) and (2a) shall be stored in the CIR for as long as the corresponding data are stored in the SIS.

10. Following the period referred to in paragraph 1, the Commission, in close cooperation with Member States and the ETIAS Central Unit, shall assess the need to extend the transitional period in which the ETIAS Central Unit performs the tasks referred to in this Article. On the basis of this assessment, and after consultation with the Member States, the Commission may adopt a delegated act in accordance with Article 63 to extend the period referred to in paragraph 1.

Article 60
Costs

1. The costs incurred in connection with the establishment and operation of the ESP, the shared biometric matching service ***(BMS)***, the ~~common identity repository (~~CIR~~)~~ and the MID shall be borne by the general budget of the Union.

2. Costs incurred in connection with the integration of the existing national infrastructures and their connection to the national uniform interfaces ~~as well as in connection with hosting the national uniform interfaces~~ shall be borne by the general budget of the Union.

   The following costs shall be excluded:

   (a) Member States' project management office (meetings, missions, offices);

   (b) hosting of national IT systems (space, implementation, electricity, cooling);

   (c) operation of national IT systems (operators and support contracts);

   (d) design, development, implementation, operation and maintenance of national communication networks.

3. 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.

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

1. The Commission shall decide the date from which each interoperability component is to start operations, after the following conditions are met:

   (a) the measures referred to in Articles 8(2), 9(7), ***13(5),*** 28(5)***, (5a)*** and (~~7~~***6***), ***32(4a), 33(4a),*** 37(4), 38(4), 39(5), ~~and~~ 44(5)***, 57(2) and 59(10), 68(7a)*** have been adopted;

   (b) eu-LISA has declared the successful completion of a comprehensive test of the relevant interoperability component, which is to be conducted by eu-LISA in cooperation with the Member States, ***the ETIAS Central Unit and Europol***;

   (c) eu-LISA has validated the technical and legal arrangements to collect and transmit the data referred to in Articles 8(1), 13, ~~19~~ ***18***, 34 and 39 and ~~have~~ ***has*** notified them to the Commission;

   (d) the Member States have notified the Commission as referred to in Article 61(1);

   (e) for the multiple-identity detector, the ETIAS Central Unit has notified the Commission as referred to in Article 61(3).

2. The Commission shall inform the European Parliament and the Council of the results of the test carried out pursuant to paragraph 1(b).

3. The Commission decision referred to in paragraph 1 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 interoperability components from the date determined by the Commission in accordance with paragraph 1.

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 Article~~s 8(2),~~ ~~and 9(7)~~ ***57(2) and 59(10)*** shall be conferred on the Commission for ~~an indeterminate~~ ***a*** period of ***five years*** ~~time~~ 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.***

3. The delegation of power referred to in Article~~s 8(2), and 9(7)~~ ***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.

6. A delegated act adopted pursuant to Article~~s 8(2), and 9(7)~~ ***57(2)*** shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of [two months] of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by [two months] at the initiative of the European Parliament or of the Council.

Article 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 in order to provide it with the expertise related to interoperability, in particular in the context of the preparation of its annual work programme and its annual activity report. 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.

2. ***The staff of Member State authorities, [the ETIAS Central Unit] and Europol, authorised to process data from the interoperability components, shall receive appropriate training about data security, data protection rules and the procedures of data processing, in which particular attention is 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 in light of objectives relating to planning and costs and to monitor the functioning of the interoperability components in light of objectives relating to the technical output, cost-effectiveness, security and quality of service.

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

3. For the purposes of technical maintenance, eu-LISA shall have access to the necessary information relating to the data processing operations performed in the interoperability components.

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

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

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

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

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

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

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

The evaluations shall include any necessary recommendations***, including the possibility, if appropriate, to conduct parallel searches in different EU information systems***. 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.[39]

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.

7a. A technical solution shall be made available to Member States in order to facilitate the querying of EU information systems and the CIR pursuant to Article 22 for the purpose of managing users request and generating statistics referred to in this Article. 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).

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

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 common identity repository for ~~law enforcement~~ 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 ~~the [EES Regulation]~~ ***Regulation (EU) 2017/2226***, ~~the VIS~~ Regulation ***(EC) No 767/2008*** or the [ETIAS Regulation];

(c) the number of requests for access to the ***CIR*** ~~common identity repository~~ for ~~law enforcement~~ 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.

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.*

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	*For the Council*
The President	The President

ANNEX II

2017/0352 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)[40]

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]

Having regard to the opinion of the Committee of the Regions,[42]

Acting in accordance with the ordinary legislative procedure,

[40] Parliamentary reservation: **FR**.

[41] OJ C , , p. .

[42]

Whereas:

(1) In its Communication of 6 April 2016 entitled *Stronger and Smarter Information Systems for Borders and Security*[43], 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[44], 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[45], 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[46] called for continued delivery on the interoperability of EU information systems and databases.

(5) In its final report of 11 May 2017[47], 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.

(6) In its Communication of 16 May 2017 entitled *Seventh progress report towards an effective and genuine Security Union*[48], 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.

---

43 COM(2016)205, 6.4.2016.

44 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.

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

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

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

48 COM(2017) 261 final, 16.5.2017.

(7) In its Conclusions of 9 June 2017[49] 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[50] 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*** ~~management of~~ the external borders, to contribute to preventing and combating ~~irregular~~ ***illegal im***migration 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 lodged in a Member State,*** 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. To achieve this, a European search portal (ESP), a shared biometric matching service (shared BMS), a common identity repository (CIR) and a multiple-identity detector (MID) should be established as interoperability components.

(10) 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 existing and future EU information systems, strengthen and simplify the data security and data protection safeguards that govern the respective EU information systems, streamline the ~~law enforcement~~ 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 to the extent of enabling it 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 ~~third-country nationals~~ ***persons*** whose personal data ~~is~~ ***are*** processed in the EU information systems and by Europol, ~~and to~~ ***including*** EU citizens whose personal data ~~is~~ ***are*** processed in the SIS and by Europol.

---

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

50 European Council conclusions, 22-23 June 2017.

(13) The European search portal (ESP) should be established to facilitate technically the ability of Member State authorities and EU ~~bodies~~ ***agencies*** to have fast, seamless, efficient, systematic and controlled access to the EU information systems, the Europol data and the Interpol databases 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 result of the query should not be shared in an automated manner with the owner of the Interpol data and a positive result should only be shared following the assessment of the competent authoritities including the Interpol National Central Bureau of the Member State querying the Interpol databases.

(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[51] 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 fast and systematic use of all 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 bodies 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.

(16a) To help fighting identity fraud when consulting national copies of SIS, new biographic identity data from CIR records could be added to an alert in SIS using the existing alias procedures of the Sirene Manual, in case of a red link between data in SIS and the CIR. After adding the new identity data as an alias in the SIS, a new multiple identity detection process should be launched in order to change the existing red link into a white link in an automated manner.

---

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

(17) Biometric data, such as ~~fingerprints~~ ***dactyloscopic data*** 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 ~~by relying on one unique technological component instead of different ones in each of the underlying systems~~. 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 in one single location, facilitating cross-system comparisons using biometric data and enabling economies of scale in developing and maintaining the EU central systems.

(18) Biometric data constitute sensitive personal data. This ***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[52], Regulation (EC) No 767/2008 of the European Parliament and of the Council[53], [the ETIAS Regulation] for the management of the borders of the Union, the system established by [the Eurodac Regulation] to identify the applicants for international protection and combat ~~irregular~~ ***illegal im***migration, and the system established by [the ECRIS-TCN system Regulation] require in order to be effective to rely on the accurate identification of the ~~third-country nationals~~ ***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].

---

52 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. 20–82).

53 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 persons but under different or incomplete identities. Member States dispose of efficient ways to identify their citizens or registered permanent residents in their territory, but the same is not true for ***other categories of persons*** ~~third-country nationals~~. The interoperability between EU information systems should contribute to the correct identification of ***those persons*** ~~third-country nationals~~. The common identity repository (CIR) should store the personal data concerning ~~third-country nationals~~ ***those 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. ***However, for the purpose of fighting identity fraud, where a red link is stored in the MID, the linked identity and travel document data should be stored in the CIR for as long as the corresponding data are stored in at least one of the EU information systems from which the linked data originates.***

(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 ~~the~~ identity, ***travel document*** and biometric data ~~of third-country nationals~~ ~~is~~ ***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 system 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 of ***each person*** ~~third-country nationals~~ 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 ~~law enforcement~~ 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 ~~or prosecution~~ of serious crime.

(25) The common identity repository (CIR) should provide for a shared container for identity, ***travel document*** and biometric data of ~~third-country nationals~~ ***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*** ~~serving~~ as the shared component between ~~these systems~~ ***them*** for storage of ~~this~~ ***the identity, travel document and biometric*** data, and to allow ~~its~~ ***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) In order to ensure the correct identification of a person, ***police authorities empowered by national law*** ~~Member State authorities competent for preventing and combating irregular migration and competent authorities within the meaning of Article 3(7) of Directive 2016/680~~ should be allowed to query the common identity repository (CIR) with the biometric data of that person taken during an identity check.

(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*** ~~legislative measures~~.

(30) This Regulation should also introduce~~s~~ 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 ~~law enforcement~~ 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, investigation and prosecution of terrorist offences or serious criminal offences in a specific case.

(31) Full access to the necessary data contained in the EU information systems necessary for the purposes of preventing, detecting ~~and~~ ***or*** investigating terrorist offences or other serious criminal offences, beyond the relevant identity data ***or travel document data*** covered under common identity repository (CIR) ~~obtained using biometric data of that person taken during an identity check~~, should continue to be governed by the provisions in the respective legal instruments. The designated ~~law enforcement~~ 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*** ~~hit~~ in the system (a so-called ~~hit~~***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 ~~third country national~~, but may 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 2016/680 or Regulation (EC) No 45/2001.

(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 ~~and~~ ***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 ~~hit~~***match***-flag type of response indicating the data ***are*** ~~is~~ recorded in the EES, the VIS, [the ETIAS] or Eurodac requires automated processing of personal data. A ~~hit~~***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 ~~hit~~***match***-flag. Access by the end-user ***to*** ~~of~~ a ~~hit~~***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*** ~~for~~ personal data more effectively directly to the system that was flagged as containing it.

(34) The two-step data consultation approach is particularly valuable in cases where the suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence is unknown. In those cases the common identity repository (CIR) should enable identifying the information system that knows the person in one single search. By creating the obligation to use this new ~~law enforcement~~ access approach ***for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences*** in these cases, access to the personal data stored in the EES ~~the VIS, [the ETIAS]~~ and Eurodac should take place without the requirements of a prior search in national databases and the launch of a prior search in the automated fingerprint identification system of other Member States under Decision 2008/615/JHA. The principle of prior search effectively limits the possibility of Member State***s***' authorities to consult ***centralised*** systems for ***the*** justified ~~law enforcement~~ purposes ***of preventing, detecting or investigating terrorist offences or other serious criminal offences*** and could thereby result in missed opportunities to uncover necessary information. The requirements of a prior search in national databases and the launch of a prior search in the automated fingerprint identification system of other Member States under Decision 2008/615/JHA should only cease to apply once the alternative safeguard of the two-step approach to ~~law enforcement~~ access ***for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences*** through the CIR has become operational.

(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) The possibility to achieve the objectives of the EU information systems is undermined by the current inability for the authorities using these systems to conduct sufficiently reliable verifications of the identities of the ~~third-country nationals~~ ***persons*** whose data are stored in different systems. That inability is determined by the fact that the set of identity data ***or travel document data*** stored in a given individual system may be fraudulent, incorrect, or incomplete, and that there is currently no possibility to detect such fraudulent, incorrect or incomplete 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 ~~third-country nationals~~ ***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*** ~~lawfully~~ or ~~unlawfully~~ ***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 and the fight against ~~irregular~~ ***illegal im***migration.

(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 EU ***agency*** ~~body~~. 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 ~~third-country national~~ ***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 ~~third-country national~~ ***person***.

(40) The national authority or EU ***agency*** ~~body~~ 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) Access to the multiple-identity detector (MID) by Member State authorities and EU ***agencies*** ~~bodies~~ having access to at least one EU information system included in the common identity repository (CIR) or to the SIS should be limited to so called red links where the linked data shares the same biometric but different identity data and the authority responsible for the verification of different identities concluded it refers ~~unlawfully~~ to the same person ***in an unjustified manner***, or where the linked data has ~~similar~~ ***different*** identity data, ***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 ~~unlawfully~~ to the same person ***in an unjustified manner, or where the linked data have same or similar identity data, the same travel document data, but different biometric data and the authority responsible for the verification of different identities concluded it refers to different persons in an unjustified manner***. Where the linked identity data ***are*** ~~is~~ not similar, a yellow link should be established and a manual verification should take place in order to confirm the link or change its colour accordingly.

(42) The manual verification of multiple identities should be ensured by the authority creating or updating the data that triggered a ~~hit~~ ***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 lawful or unlawful identities. Such assessment should be performed where possible in the presence of the ~~third-country national~~ ***person*** 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.

(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, on persons for discreet checks or specific checks or on unknown wanted persons, 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) Access to the MID by Member State authorities and EU agencies is not foreseen where a white link exists between data from two or more EU information systems. However, this will not affect the users' access rights. Where it becomes evident when accessing data from two or more EU information systems that a white link was wrongly created, that Member State authority or EU agency should be able 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) UMF is not meant as a mandatory, sole or preferred standard for the whole field of Justice and Home Affairs and the diverse solutions deployed by the European Commission, the EU agencies and 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. 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 and should record such anonymous 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) ***No*** 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, when Directive (EU) ***No*** 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) No 2016/680 applies.[54]

(49) The specific provisions on data protection of ~~[the EES~~ Regulation ***(EU) 2017/2226***~~]~~, Regulation (EC) No 767/2008, [the ETIAS Regulation] and [the Regulation on SIS in the field of border checks] should apply to the processing of personal data in those respective systems.

(50) Regulation (EC) No 45/2001 of the European Parliament and of the Council[55] 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.

---

54 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) No 2016/680 applies."

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

(51) The national supervisory authorities established in accordance with ~~[~~Regulation (EU) ***No*** 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 (EC) No 45/2001 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.

(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*** ~~...~~ "

(53) Insofar as confidentiality is concerned, the relevant provisions of the Staff Regulations of officials and the Conditions of Employment of other servants of the European Union should apply to officials or other servants employed and working in connection with SIS.

(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.

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

(56) In order to allow competent authorities and the EU ***agencies*** ~~bodies~~ 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.

(57) The costs for the development of the interoperability components projected under the current Multiannual Financial Framework are lower than the remaining amount on the budget earmarked for Smart Borders in Regulation (EU) No 515/2014 of the European Parliament and the Council[56]. Accordingly, this Regulation, pursuant to Article 5(5)(b) of Regulation (EU) No 515/2014, should reallocate the amount currently attributed for developing IT systems supporting the management of migration flows across the external borders.

---

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).

(58) 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)*** ~~profiles for the users of the European search portal (ESP) and the content and format of the ESP replies~~. 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.

(59) 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); format of the ESP replies; performance requirements and performance monitoring of the shared BMS;*** automated data quality control mechanisms, procedures and indicators; development of the UMF standard; procedures for determining cases of similarity of identities; ~~the~~ operation of the central repository for reporting and statistics; ~~and~~ cooperation procedure in case of security incidents***; and specifications of the technical solution to facilitate the querying of EU information systems and the CIR***. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[58].

(60) Regulation ***(EU)*** 2016/794 shall apply for any processing of Europol data for the purposes of this Regulation.

(60a) 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) No 2016/679, Directive (EU) No 2016/680 and Regulation (EC) No 45/2001. 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.

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

---

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

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

(62) ***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 Decision 2007/533/JHA, 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. Moreover,*** in accordance with Article 3 of the Agreement between the European Community and the Kingdom of Denmark on the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in Denmark or any other Member State of the European Union and 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention[1], Denmark is to notify the Commission whether it will implement the contents of this Regulation, insofar as it relates to Eurodac [and the automated system for registration, monitoring and the allocation mechanism for applications for international protection referred to in Article 44 of Regulation (EU) XX/XX 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)].

[1]

(63) Insofar as its provisions relate to SIS as governed by Decision 2007/533/JHA, 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*[59]. Furthermore, insofar as its provisions relate to Eurodac [and the automated system for registration, monitoring and the allocation mechanism for applications for international protection referred to in Article 44 of Regulation (EU) XX/XX 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)] the United Kingdom may notify to the President of the Council its wish to take part in the adoption and application of this Regulation, 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). ~~Insofar as its provisions relate to [the ECRIS-TCN system], in accordance with Articles 1 and 2 and Article 4a(1) 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, the United Kingdom is not taking part in the adoption of this Regulation and is not bound or subject to its application. In accordance with Article 3 and Article 4a(1) of Protocol 21, the United Kingdom may notify its wish to take part in the adoption of this Regulation.~~ Insofar as its provisions relate to [the ECRIS-TCN system], in accordance with Article 3 and Article 4a(1) 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, the United Kingdom has notified its wish to part in the adoption of this Regulation. In accordance with Article 3 and Article 4a(1) of Protocol 21, the United Kingdom has notified its wish to take part in the adoption of this Regulation.

59

(64) Insofar as its provisions relate to SIS as governed by Decision 2007/533/JHA, Ireland 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 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*[60]. Furthermore, insofar as its provisions relate to Eurodac [and the automated system for registration, monitoring and the allocation mechanism for applications for international protection referred to in Article 44 of Regulation (EU) XX/XX 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)], Ireland may notify to the President of the Council its wish to take part in the adoption and application of this Regulation, 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 Treaty on European Union and to the Treaty on the Functioning of the European Union (Protocol on the position of the United Kingdom and Ireland). Insofar as its provisions relate to [the ECRIS-TCN system], in accordance with Articles 1 and 2 and Article 4a(1) 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. In accordance with Article 3 and Article 4a(1) of Protocol 21, Ireland may notify its wish to take part in the adoption of this Regulation.

(65) As regards Iceland and Norway, as regards Eurodac [and the automated system for registration, monitoring and the allocation mechanism for applications for international protection referred to in Article 44 of Regulation (EU) XX/XX 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)], this Regulation constitutes a new measure within the meaning of the Agreement between the European Community and the Republic of Iceland and the Kingdom of Norway concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Iceland or Norway.

60

(66) As regards Switzerland, as regards Eurodac [and the automated system for registration, monitoring and the allocation mechanism for applications for international protection referred to in Article 44 of Regulation (EU) XX/XX 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)], this Regulation constitutes a new measure related to Eurodac within the meaning of the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland.

(67) As regards Liechtenstein, as regards Eurodac, [and the automated system for registration, monitoring and the allocation mechanism for applications for international protection referred to in Article 44 of Regulation (EU) XX/XX 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)] this Regulation constitutes a new measure within the meaning of the Protocol between 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 Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland.

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

HAVE ADOPTED THIS REGULATION:

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 and operation of the interoperability components.

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

Article 2
Objectives ~~of interoperability~~

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

   (a) ***to improve the effectiveness and efficiency of checks at the external borders***; ~~to improve the management of the external borders~~;

   (b) to contribute to preventing and combating ~~irregular~~ ***illegal im***migration;

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

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

   (e) to assist in examining application***s*** for international protection ***lodged in a Member State***;

   (f) in the event of a natural disaster or an accident, for humanitarian reasons, to assist in the identification of unknown persons who are not able to identify themselves or unidentified human remains.

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

   (a) ensuring the correct identification of persons;

   (b) contributing to fighting identity fraud;

   (c) improving and harmonising data quality requirements of the respective EU information systems ***while respecting the data processing requirements of the legal bases of the individual systems, data protection standards and ~~the data owner~~ principles***;

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

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

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

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

Article 3
Scope

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

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

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

(10) ***‘dactyloscopic data’ means fingerprints images, images of fingerprint latents, palm prints, and palm prints latents[61] which due to their unique character and the reference points contained therein enable accurate and conclusive comparisons on a person's identity***; ~~‘fingerprint data’ means the data relating to the fingerprints of an individual~~;

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

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

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

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

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

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

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

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

(19) ‘Europol data’ means personal data ***processed by*** ~~provided to~~ 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);

---

61 *NB: Same definition as in Council Decision 2008/616/JHA.*

(21) ‘match’ means the existence of a correspondence ***as a result of an automated comparison between*** ~~established by comparing two or more occurrences of~~ personal data recorded or being recorded in an information system or database;

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

(23) 'police authority' means 'competent authority' as defined in Article 3(7) of Directive ***No*** 2016/680;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Article 5
Non-discrimination

Processing of personal data for the purposes of this Regulation shall not result in discrimination against persons on any grounds such as ***gender*** ~~sex~~, racial or ethnic origin, religion or belief, disability, age or sexual orientation. It shall fully respect human dignity and integrity. ~~Particular attention shall be paid to children, the elderly and persons with a disability~~.

CHAPTER II
European Search Portal

Article 6
European search portal

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

2. The ESP shall be composed of:

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

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

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

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

Article 7
Use of the European search portal

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

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

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

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

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

Article 8
Profiles for the users of the European search portal

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

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

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

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

2. The Commission shall adopt ***implementing*** ~~delegated~~ acts ~~in accordance with Article 63~~ to specify the technical details of the profiles referred to in paragraph 1 for the users of the ESP referred to in Article 7(1) in accordance with their access rights. ***Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).***

Article 9
Queries

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

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

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

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

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

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

7. The Commission shall adopt an ***implementing*** ~~delegated~~ act ~~in accordance with Article 63~~ to specify ***the process for querying the EU information systems, Europol data and Interpol databases by the ESP and*** the ~~content and~~ 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 39 of the Eurodac Regulation], [Articles 12 and 18 of the Regulation on SIS in the field of law enforcement], ***[Article 13 of the Regulation on SIS in the field of illegal return]***, [Article 29 of the ECRIS-TCN Regulation] and Article 40 of Regulation (EU) 2016/794, eu-LISA shall keep logs of all data processing operations within the ESP. Those logs shall include, in particular, the following:

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

   (b) the date and time of the query;

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

   (d) ***the unique transaction identification number*** ~~in accordance with national rules or with Regulation (EU) 2016/794 or, when applicable, Regulation (EU) 45/2001, the identifying mark of the person who carried out the query~~.

1a. Each Member State shall keep logs of queries of the authority and the staff duly authorised to use the ESP including the transaction identification number referred to in point (d) of paragraph 1.

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 pursuant to Article 42. Those logs shall be ***made available to the competent supervisory authority on request. They shall be*** protected by appropriate measures against unauthorised access ***and modifications*** and erased one year after their creation, unless they are required for monitoring procedures that have already begun ***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 ***automatically*** by eu-LISA.

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

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

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

CHAPTER III

Shared Biometric Matching Service

Article 12
Shared biometric matching service

1. A shared biometric matching service (shared BMS) storing biometric templates ***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 ***Common Identity Repository (***CIR***)*** and the multiple-identity detector ***(MID)*** and the objectives of the EES, the VIS, Eurodac, the SIS and [the ECRIS-TCN system].

2. The shared BMS shall be composed of:

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

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

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

Article 13
Data stored in the shared biometric matching service

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

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

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

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

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

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

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

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

The shared BMS shall store the biometric templates - logically separated - according to the EU information system from which the data originated.

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~~ ***may*** be entered ***only*** 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) ***and (4)***.

5. The Commission shall lay down the performance requirements and performance monitoring of the shared BMS, including the minimum requirements regarding the biometric performance of the shared BMS, in particular in terms of the required False Positive Identification Rate, False Negative Identification Rate and Failure To Enrol Rate, as well as the procedures and tools for notifying False Positive Identifications and False Negative verifications to eu-LISA in implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).

For the specific purpose of monitoring the performance of the shared BMS, Member States shall be allowed to use the biometric templates stored in the shared BMS.

Article 14
Searching biometric data with the shared biometric matching service

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

Article 15

Data retention in the shared biometric matching service

The data referred to in Article 13***(1) and (2)*** shall be stored in the shared BMS for as long as the corresponding biometric data ***are*** ~~is~~ 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 39 of the Eurodac Regulation], [Article 12 and 18 of the Regulation on SIS in the field of law enforcement***, to Article 13 of the Regulation on SIS in the field of illegal return***] and to [Article 29 of the ECRIS-TCN Regulation], eu-LISA shall keep logs of all data processing operations within the shared BMS. Those logs shall include~~, in particular,~~ the following:

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

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

   (c) the date and time of the query;

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

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

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

   (g) ~~in accordance with national rules or with Regulation (EU) 2016/794 or, when applicable, Regulation (EU) 45/2001, the identifying mark of the person who carried out the query~~ ***the Member State or EU agency searching biometric data***.

1a. Each Member State 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 pursuant to Article 42. Those logs shall be ***made available to the competent supervisory authority on request. They shall*** protected by appropriate measures against unauthorised access ***and modifications*** and erased one year after their creation, unless they are required for monitoring procedures that have already begun, ***in which case they shall be erased once the monitoring procedures no longer require these logs***. The logs referred to in paragraph 1(a) shall be erased once the data ***are*** ~~is~~ erased.

CHAPTER IV
Common Identity Repository

Article 17
Common identity repository

1. A common identity repository (CIR), creating an individual file for each person that is recorded in the EES, the VIS, [the ETIAS], Eurodac or [the ECRIS-TCN system] containing the data referred to in Article 18, is established for the purpose of facilitating and assisting the correct identification of persons registered in the EES, the VIS, [the ETIAS], the Eurodac and [the ECRIS-TCN system] ***in accordance with Article 20***, of supporting the functioning of the multiple-identity detector ***in accordance with Article 21*** and of facilitating and streamlining access by ~~law enforcement~~ ***designated*** authorities ***and Europol*** to non-law enforcement ***EU*** information systems ~~at EU level~~, where necessary for the prevention, ~~investigation,~~ detection ***or investigation*** ~~or prosecution~~ ***of terrorist offences or other*** ~~of~~ serious ~~crime~~ ***criminal offences 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 EU ***agencies*** ~~bodies~~ that are entitled to use the ~~European search portal (ESP)~~ ***CIR*** in accordance with Union law ***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 ~~multiple-identity detector~~ ***MID***.

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

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

Article 18
The common identity repository data

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

~~(a) (not applicable);~~

~~(b) (not applicable);~~

~~(c) (not applicable);~~

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

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

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

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

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

Article 19
Adding, amending and deleting data in the common identity repository

1. Where data ***are*** ~~is~~ added, amended or deleted in Eurodac or [the ECRIS-TCN system], the data referred to in Article 18 stored in the individual file of the CIR shall be added, amended or deleted accordingly in an automated manner.

2. Where ~~the multiple-identity detector creates~~ a white or red link ***is created in the MID*** in accordance with Articles 32 ~~and~~ ***or*** 33 between the data of two or more of the EU information systems constituting the CIR, instead of creating a new individual file, the CIR shall add the new data to the individual file of the linked data.

Article 20

Access to the common identity repository for identification

1. Where a ~~Member State~~ police authority has been so empowered by national legislative measures as referred to in paragraph 2, it may, solely for the purpose of identifying a person, query the CIR with the biometric data of that person taken during an identity check.

1a. ***Where a police authority has been so empowered by national legislative measures as referred to in paragraph 2a, it may, for the purpose of identifying unknown persons who are not able to identify themselves or unidentified human remains, in the event of a ~~natural~~ disaster or an accident, query the CIR with the biometric data of those persons.***

1b. Where the query indicates that data on that person is stored in the CIR, the ~~Member States~~ ***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.

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

2a. Member States wishing to avail themselves of the possibility provided for in paragraph 1a 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 ~~identity~~ 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 ~~identity~~ 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 ~~law enforcement~~ purposes ***of preventing, detecting or investigating terrorist offences or other serious criminal offences***

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

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

3. Where, in reply to a query the CIR indicates data on that person is present in Eurodac the CIR shall provide to ~~Member States'~~ designated authorities and Europol a reply in the form of a reference indicating which of the information systems contains matching data referred to in Article 18(2). The CIR shall reply in such a way that the security of the data is not compromised. ***The reply indicating that data on that person is present in any of those systems may be used only for the purpose of submitting an access request subject to the conditions and procedures laid down in the respective legislative instruments governing such access.***

4. Full access to the data contained in the EU information systems for the purposes of preventing, detecting ~~and~~ ***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. ***Without prejudice to paragraphs 2 and 3,*** ~~T~~***t***he data referred to in Article 18(1)***,*** ~~and~~ (2) ***and (2a)*** shall be deleted from the CIR ***in an automated manner*** in accordance with the data retention provisions of [the Eurodac Regulation] and [the ECRIS-TCN Regulation] respectively.

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

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

Article 24
Keeping of logs

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

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

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

   (b) the date and time of the query;

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

   (d) the results of the query;

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

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

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

   (b) the date and time of the query;

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

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

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

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

   ~~(a) the national file reference;~~

   (b) the date and time of the query;

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

   (d) the results of the query;

   (e) the ~~name of the authority~~ ***Member State or EU agency querying*** ~~consulting~~ the CIR;

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

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

5. Each Member State shall keep logs of queries of ***the 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;

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

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

CHAPTER V
Multiple-identity Detector

Article 25
Multiple-identity detector

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

2. The MID shall be composed of:

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

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

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

Article 26
Access to the multiple-identity detector

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

   ~~(a) – (not applicable);~~

   ~~(b) – (not applicable);~~

   ~~(c) – (not applicable);~~

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

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

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

(dc) the authorities competent to collect the data of persons registered for the purpose of conducting an admission procedure and admitted in accordance with a national resettlement scheme provided for in Chapter IIA of the Eurodac Regulation when creating or updating data in the Eurodac;

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

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

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

Article 27
Multiple-identity detection

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

~~(a) – (not applicable);~~

~~(b) – (not applicable);~~

~~(c) – (not applicable);~~

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

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

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

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

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

~~(a) (not applicable);~~

~~(b) (not applicable);~~

~~(c) (not applicable);~~

(d) [surname(s); forename(s); name(s) at birth, previously used names and aliases; date of birth, place of birth, nationality(ies) and sex as referred to in Article 12 of the Eurodac Regulation];

~~(e) (not applicable);~~

(f) [surname(s); forename(s); name(s) at birth, previously used names and aliases; date of birth, place of birth, nationality(ies) and sex as referred to in Article 20(3) of the Regulation on SIS in the field of law enforcement;]

(g) [surname(s); forename(s); name(s) at birth, previously used names and aliases; date of birth, place of birth, nationality(ies) and sex as referred to in Article 4 of the Regulation on SIS in the field of illegal return;]

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

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

4. The multiple-identity detection ***may*** ~~shall only~~ be launched ***only*** 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 (3***a***) do not report any ***match*** ~~hit~~, 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 (3***a***) reports one or several ***match(es)*** ~~hit(s)~~, the common identity repository and, where relevant, the SIS shall create a link between the data used to launch the query and the data triggering the ***match*** ~~hit~~.

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

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

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

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

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

7. The Commission shall lay down the technical rules for ~~linking data~~ ***creating links between data*** from different ***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 m*anual verification of different identities*

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

~~(a) (not applicable);~~

~~(b) (not applicable);~~

~~(c) (not applicable);~~

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

(da) the authority competent to collect the data provided for in the Eurodac Regulation for hits that occurred when creating or updating data in the Eurodac;

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

(f) the central authorities of the convicting Member State for hits that occurred when recording or updating data in the ECRIS-TCN system in accordance with Article 5 ***or Article 9*** of the [ECRIS-TCN Regulation].

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

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

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

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

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

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

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

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

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

~~4. (not applicable).~~

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

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

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

6. Where data reporting a ~~hit~~ ***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 different identity data and no manual verification of different identity has taken place;

   (b) the linked data has ~~different~~ ***some differences in the*** identity data ***or in travel document data***, ~~and~~ 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***;

   (c) the linked data has same or similar 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 the linked data do not share the same biometric ***data*** but have ***same or*** similar identity data and the authority responsible for the verification of different identities concluded it refers to two different persons.

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

Article 32
Red link

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

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

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

   (c) the linked data has different identity data, 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;

   (d) the linked data has same or similar identity data, the same travel document data, but different biometric data and the authority responsible for the verification of different identities concluded it refers to different persons 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 ***EU*** information systems constituting the CIR or with the SIS, the multiple-identity detector shall reply indicating the data referred to in Article 34. Follow-up to a red link shall take place in accordance with Union and national law, ***basing any legal consequence for the person only on the relevant data on that person and not on the red link itself.***

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

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

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 authority responsible for verification of different identities shall provide a reference to the authorities responsible for the data linked.~~

6. If a Member State authority has evidence to suggest that a red link recorded in the MID is factually inacurate or not up-to-date or that data were processed in the MID, the CIR or the SIS in breach of this Regulation, it shall check the relevant data stored in the CIR and SIS and shall, if necessary, rectify or erase the link from the MID without delay. That Member State authority shall inform the Member State responsible for the manual verification without delay.

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, ~~and~~ ***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 or similar identity 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 the same person ~~legally~~ having different identity data in a justified manner;

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

2. Where the CIR or the SIS are queried and where a white link exists between ~~one~~ ***two*** or more of the ***EU*** information systems constituting the CIR or with the SIS, the ~~multiple-identity detector~~ ***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 ~~hit~~ ***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~~(1)~~***(2)***.

4. ~~Without prejudice to the provisions related to the handling of alerts in the SIS referred to in the [Regulations on SIS in the field of border checks, on SIS in the field of law enforcement and on SIS in the field of illegal return],~~ ~~w~~***W***here a white link is created following a manual verification of multiple identities ***between data from the EES, the VIS, [the ETIAS] or Eurodac***, the authority responsible for ***the*** verification of different identities shall inform the person of the presence of discrepancies between his or her personal data between systems and shall provide a reference to the authorities responsible for the data linked.

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

Article 34
Identity confirmation file

The identity confirmation file shall contain the following data:

(a) the links~~, including their description in form of colours,~~ as referred to in Articles 30 to 33;

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

(c) a single identification number allowing to retrieve the data from the ***EU*** information systems of corresponding linked files ***in accordance with respective access rights under Union and national law***;

(d) ~~where relevant,~~ the authority responsible for the verification of different identities;

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

Article 35
Data retention in the multiple-identity detector

1. ***Without prejudice to paragraphs 2 and 3,*** the identity confirmation files and ~~its~~ ***their*** data, including the links, shall be stored in the ~~multiple-identity detector (~~MID~~)~~ only for as long as the linked data ***are*** ~~is~~ stored in two or more EU information systems ***and be deleted thereafter in an automated manner***.

2. ***Where a red link is created between data in the CIR, the identity confirmation files and their data, including the red link, shall be stored in the MID only for as long as the corresponding data are stored in at least one of the EU information systems from which the linked data originates and be deleted thereafter in an automated manner***.

3. ***Where a red link is created between data in the CIR and the SIS, the identity confirmation files and their data, including the red link, shall be stored in the MID only for as long as the corresponding data are stored in the SIS 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~~, in particular,~~ the following:

   ~~(a) the purpose of access of the user and his or her access rights;~~

   (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;

   (f) the ~~identifying mark of the person who carried out the query~~ ***Member State or EU agency querying the MID***.

2. Each Member State shall keep logs of the ***authority, the purpose of access 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 request and the lawfulness of data processing, and for ensuring data security pursuant to Article 42. Those logs shall be ***made available to the competent supervisory authority on request. They shall*** be protected by appropriate measures against unauthorised access ***and modification.*** ~~and~~ ***They shall be*** erased ***in an automated manner*** 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 those logs***. The logs related to the history of the identity confirmation file shall be erased once the data in the identity confirmation file is erased.

CHAPTER VI
Measures supporting interoperability

Article 37
Data quality

1. ***Without prejudice to Member States' responsibilities with regard to the quality of data entered into the systems,*** eu-LISA shall establish automated data quality control mechanisms and procedures on the data stored in the SIS, Eurodac, [the ECRIS-TCN system], the shared biometric matching service (shared BMS) ***and*** the common identity repository (CIR) ~~and the multiple-identity detector (MID)~~.

2. ~~establish~~ ***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 ~~and the MID~~.

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

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

5. One year after the establishment of the automated data quality control mechanisms and procedures, ~~and~~ common data quality indicators ***and 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 shall ***regularly*** report on any progress against this action plan until it is fully implemented.

   The Commission shall transmit the evaluation report to the European Parliament, to the Council, to the European Data Protection Supervisor and to the European Union Agency for Fundamental Rights established by Council Regulation (EC) No 168/2007.[62]

[62] 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 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 ***A****~~a~~*ffairs

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

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

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

Article 39
Central repository for reporting and statistics

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

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

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

4. The CRRS shall be composed of:

(-a) the tools necessary for anonymising data;

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

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

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

CHAPTER VII
Data protection

Article 40
Data controller

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

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

   (a) the European Border and Coast Guard Agency shall be ~~considered~~ a data controller in accordance with Article 2(b) of Regulation No 45/2001 ***[or Article 3(2)(b) of Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC]*** in relation to processing of personal data by the ETIAS Central Unit;

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

Article 41
Data processor

In relation to the processing of personal data in ***the shared BMS,*** the CIR ***and the MID***, eu-LISA **shall** ~~is to~~ be ~~considered~~ the data processor in accordance with Article 2(e) of Regulation (EC) No 45/2001 ***[or Article 3(1)(a) of Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC]***.

Article 42
Security of processing

1. ~~Both~~ 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 22 of Regulation (EC) No 45/2001 ***[or Article 33 of Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC]***, 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 ***security*** measures, including a security plan, a business continuity plan and a disaster recovery plan, in order to:

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

   (b) 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;

(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 has 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;

(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.

4. Member States***, [the ETIAS Central Unit] and Europol*** 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
Confidentiality of SIS data

1. Each Member State shall apply its rules of professional secrecy or other equivalent duties of confidentiality to all persons and bodies required to work with SIS data accessed through any of the interoperability components in accordance with its national law. That obligation shall also apply after those persons leave office or employment or after the termination of the activities of those bodies.

2. Without prejudice to Article 17 of the Staff Regulations of officials and the Conditions of Employment of other servants of the European Union, eu-LISA shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality of comparable standards to those laid down in paragraph 1 to all its staff required to work with SIS data. This obligation shall also apply after those persons leave office or employment or after the termination of their activities.

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 and the European Data Protection Supervisor of ***any*** security incident~~s~~.

   Without prejudice to Article 35 of Regulation (EC) 45/2001 [or Article 37 of Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC] 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.

   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*** 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 EU ***agencies*** ~~bodies~~ 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 logs, and cooperate, where necessary, with the supervisory authorities referred to in Article~~s~~ 49 and ***with the European Data Protection Supervisor as referred to in Article*** 50.

Article 46
Right of information

1. Without prejudice to the right of information referred to in Articles 11 and 12 of Regulation (EC) 45/2001 ***[or Articles 15 and 16 of Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC], Articles 13 and 14 of Directive (EU) 2016/680*** and Articles 13 and 14 of Regulation (EU) 2016/679, persons whose data are stored in the shared ~~biometric matching service~~ ***BMS***, the ~~common identity repository~~ ***CIR*** or the ~~multiple-identity detector~~ ***MID*** shall be informed by the ~~authority collecting their data~~ ***data controller***, at the time their data are collected ***in accordance with paragraph 2***, about the processing of personal data for the purposes of this Regulation, including about identity and contact details of the respective data controllers, ***about the period for which the personal data will be stored or about the criteria used to determine that period,*** ~~and~~ about the procedures for exercising their rights of access, rectification and erasure, as well as about the contact details of the European Data Protection Supervisor and of the national supervisory authority of the Member State responsible for the collection of the data.

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

~~(a) (not applicable);~~

~~(b) (not applicable);~~

~~(c) (not applicable);~~

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

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

Article 47

*Right of access, ~~correction~~ **rectification** and erasure **of data stored in the MID***

1. In order to exercise their rights under Articles 13, 14, 15 and 16 of Regulation (EC) 45/2001 ***[or Articles 17, 18, 19 and 20 of Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC], Article 16 of Directive (EU) 2016/680*** and Articles 15, 16, 17 and 18 of Regulation (EU) 2016/679, any person shall have the right to address him or herself to the ~~Member State responsible for the manual verification of different identities or~~ ***competent authority*** of any Member State, who shall examine and reply to the request.

2. ~~The Member State responsible for the manual verification of different identities as referred to in Article 29 or the Member State to which the request has been made~~ ***The Member State which examined such request*** shall reply ~~to such requests~~ within ~~45~~ ***60*** days of receipt of the request. ***Member States may decide that these replies are given by central offices.***

3. If a request for ~~correction~~ ***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***.*** ~~and t~~***T***he Member State responsible ***for the manual verification of different identities*** shall check the accuracy of the data and the lawfulness of the data processing within ~~30~~ ***45*** days of such contact.

3a. 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 within 45 days of such contact.

4. Where, following an examination, it is found that the data stored in the ~~multiple-identity detector (~~MID~~)~~ are ~~factually~~ 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*** ~~applicable,~~ the Member State to which the request has been made shall correct or delete these data.

5. Where data ***stored*** in the MID is amended by ***a*** ~~the responsible~~ Member State during its validity period, ~~the responsible~~ ***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 ~~hit~~ ***match***, ~~the responsible~~ ***that*** Member State ~~or, where applicable, the Member State to which the request has been made~~ shall delete the data from the identity confirmation file. Where the automated processing reports one or several ***match(es)*** ~~hit(s)~~, ~~the responsible~~ ***that*** Member State shall create or update the relevant link in accordance with the relevant provisions of this Regulation.

6. Where the ~~responsible~~ 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 ~~factually~~ 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 rectification or erasure of personal data*** ~~referred in paragraph 3~~ 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 ~~competent~~ national supervisory authorities.

8. Any request ***for rectification or erasure of personal data*** ~~made pursuant to paragraph 3~~ 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 ~~paragraph 3~~ ***this Article*** and shall be erased immediately afterwards.

9. The ~~responsible~~ 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 rectification or erasure of personal data*** ~~referred to in paragraph 3~~ was made and how it was addressed, and shall make that document available to ~~competent data protection~~ national supervisory authorities without delay.

Article 47a[63]
Penalties

Member States shall lay down the rules on penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.

63 Articles 47a and 47b are copied from the text agreed with the EP on the ETIAS Regulation.

Article 47b
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 (EC) 45/2001:

(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 eu-LISA incompatible with this Regulation shall be entitled to receive compensation from that agency. eu-LISA shall be liable for unlawful personal data processing operations in accordance with its role as processor or, where applicable, controller.

That Member State 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 held liable for such damage, unless and insofar as eu-LISA or another Member State participating in the interoperability components 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 48

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

Without prejudice to [Article 55 of the ETIAS Regulation], Article 41 of Regulation (EU) 2017/2226, and Article 31 of Regulation (EC) 767/2008, ~~*P*~~***p***ersonal data stored in or accessed by the interoperability components shall not be transferred or made available to any third country, to any international organisation or to any private party, with the exception of transfers to Interpol for the purpose of carrying out the automated processing referred to in [Article 18(2)(b) and (m) of the ETIAS Regulation] or for the purposes of Article 8(2) of Regulation (EU) 2016/399. Such transfers of personal data to Interpol shall be compliant with the provisions of Article 9 of Regulation (EC) No 45/2001 ***[or Chapter V of Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC]*** and Chapter V of Regulation (EU) 2016/679.

Article 49

Supervision by the ~~*national*~~ *supervisory* ~~*authority*~~ ***authorities***

1. The supervisory ~~authority or~~ authorities ~~designated pursuant to Article 49 of Regulation (EU) 2016/679~~ 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.

2. Member States shall ensure that their supervisory ~~authority has~~ ***authorities have*** sufficient resources to fulfil the tasks entrusted to ~~it~~ ***them*** under this Regulation.

3. 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.

Article 50
*~~Supervision~~ **Audit** by the European Data Protection Supervisor*

The European Data Protection Supervisor shall ensure that an audit of ~~eu-LISA's~~ personal data processing ~~activities~~ ***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***,*** ~~and~~ the Member States ***and the EU agency concerned***. eu-LISA***, [the ETIAS Central Unit] and Europol*** shall be given an opportunity to make comments before the reports are adopted.

Article 51
Cooperation between ~~national~~ supervisory authorities and the European Data Protection Supervisor

1. The European Data Protection Supervisor shall act in close cooperation with national supervisory authorities with respect to specific issues requiring national involvement, 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, or in the context of questions raised by one or more ~~national~~ supervisory authorities on the implementation and interpretation of this Regulation.

2. In the cases referred to in paragraph 1, coordinated supervision shall be ensured in accordance with ***[***Article 62 of Regulation (EU) XXXX/2018 ~~[revised Regulation 45/2001]~~ ***of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC]***.

CHAPTER VIII
Responsibilities

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

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

2. The interoperability components shall be hosted by eu-LISA in its technical sites and shall provide the functionalities laid down in this Regulation in accordance with the conditions of security, availability, quality and ~~speed~~ ***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, and Eurodac, and [the ECRIS-TCN system], and the European search portal ***(ESP)***, the shared biometric matching service ***(BMS)***, the common identity repository ***(CIR),*** ~~and~~ the multiple-identity detector ***(MID) and the central repository for reporting and statistics (CRRS)***.

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

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

   The development shall consist of the elaboration and implementation of the technical specifications, testing and overall project 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 ~~large-scale IT~~ ***EU information*** systems ~~managed by eu-LISA~~ 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 ~~the~~ ***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*** ~~large-scale IT systems managed by eu-LISA~~.

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 ~~and the national uniform interfaces~~. In cooperation with the Member States, it shall ensure ~~at all times~~ the best available technology, 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 necessary to keep the interoperability components functioning ***providing uninterrupted services to the Member States*** 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.

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.

3. eu-LISA shall develop and maintain a mechanism and procedures for carrying out quality checks on the data stored in the shared biometric matching service and the common identity repository 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 ~~European search portal (~~ESP~~)~~ and the ~~common identity repository (~~CIR~~)~~;

(b) the integration of the existing national systems and infrastructures with the ESP, ~~shared biometric matching service,~~ the CIR and the ~~multiple-identity detector~~ ***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 ~~and by the duly empowered staff~~ of the competent national authorities to the ESP, the CIR and the ~~multiple-identity detector~~ ***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~~(3)~~***(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 ~~implementation~~ ***compliance with*** data quality requirements ~~in the EU information systems and in the interoperability components~~ ***established under Union law***;

(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 ~~referred to in Article 4(24)~~ 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***(1)(c)***;

(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
Final provisions

Article 55a
Business Continuity

Interoperability of central EU information systems supported by this Regulation shall be accompanied by business continuity solutions, determined and implemented in accordance with [Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011], that ensure uninterrupted availability ~~for CIR and sufficient availability~~ of ~~the other~~ all interoperability components and the data stored therein. In order to ensure operational needs, the Commission, in close cooperation with the Member States and eu-LISA, shall adopt the implementing acts necessary for the development and technical implementation of such solutions ~~facilitating continuous availability of the data stored in the CIR and shared BMS, supported by the MID, and accessed by the ESP. The ESP, the shared BMS, the CIR, the MID and the possible backup solution shall be located in the technical sites of eu-LISA~~.

Article 56
Reporting and statistics

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

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

   ~~(b) (not applicable).~~

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

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

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

(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;*** ~~.~~

(e) the period of time a yellow link or a red link remained.

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[64] 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 1, 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 paragraph 1 of this Article, eu-LISA shall store the data referred to in paragraph***s*** 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 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.

---

64 Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC (OJ L 251, 16.9.2016, p. 1).

Article 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. ***Following the period referred to in paragraph 1, the Commission, in close cooperation with Member States and eu-LISA, shall assess the impact of the ESP on border checks. On the basis of this assessment, and after consultation with the Member States, the Commission may adopt a delegated act in accordance with Article 63 to extend the period referred to in paragraph 1 until any potential technical issue linked to the ESP has been solved ~~for a maximum of additional two years~~.***

Article 58
Transitional period applicable to the provisions on access to the common identity repository for ~~law enforcement~~ 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 ~~multiple-identity detector (~~MID~~)~~ and before the start of operations of the MID, the ETIAS Central Unit as referred to in [Article 33(a) of Regulation (EU) 2016/1624] shall be responsible for carrying out a multiple-identity detection between the data stored in the ***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)*** ~~hit(s)~~ and the identity data of the linked files is identical or similar, a white link shall be created in accordance with Article 33.

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

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

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

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

5. The ETIAS Central Unit or the SIRENE Bureau of the Member State that created the alert shall have access to the data contained in the identity confirmation file and shall assess the different identities and shall update the link in accordance with Articles 31, 32 and 33 and add it to the identity confirmation file.

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

7. Where a red link is created between data in the CIR, the identity confirmation file including the red link shall be stored in the MID at least for three years or for as long as the corresponding data are stored in at least one of the EU information systems.

8. Where a red link is created between data in the CIR, the linked data referred to in Article 18(1), (2) and (2a) shall be stored in the CIR at least for three years or for as long as the corresponding data are stored in at least one of the EU information systems.

9. Where a red link is created between data in the CIR and the SIS, the linked data referred to in Article 18(1), (2) and (2a) shall be stored in the CIR for as long as the corresponding data are stored in the SIS.

10. Following the period referred to in paragraph 1, the Commission, in close cooperation with Member States and the ETIAS Central Unit, shall assess the need to extend the transitional period in which the ETIAS Central Unit performs the tasks referred to in this Article. On the basis of this assessment, and after consultation with the Member States, the Commission may adopt a delegated act in accordance with Article 63 to extend the period referred to in paragraph 1.

Article 60
Costs

1. The costs incurred in connection with the establishment and operation of the ESP, the shared biometric matching service ***(BMS)***, the ~~common identity repository (~~CIR~~)~~ and the MID shall be borne by the general budget of the Union.

2. Costs incurred in connection with the integration of the existing national infrastructures and their connection to the national uniform interfaces ~~as well as in connection with hosting the national uniform interfaces~~ shall be borne by the general budget of the Union.

   The following costs shall be excluded:

   (a) Member States' project management office (meetings, missions, offices);

   (b) hosting of national IT systems (space, implementation, electricity, cooling);

   (c) operation of national IT systems (operators and support contracts);

   (d) design, development, implementation, operation and maintenance of national communication networks.

3. 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.

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

1. The Commission shall decide the date from which each interoperability component is to start operations, after the following conditions are met:

   (a) the measures referred to in Articles 8(2), 9(7), ***13(5),*** 28(5)***, (5a)*** and (~~7~~***7***~~6~~), ***32(4a), 33(4a),*** 37(4), 38(4), 39(5), ~~and~~ 44(5)***, 57(2) and 59(10), 68(7a)*** have been adopted;

   (b) eu-LISA has declared the successful completion of a comprehensive test of the relevant interoperability component, which is to be conducted by eu-LISA in cooperation with the Member States, ***the ETIAS Central Unit and Europol***;

   (c) eu-LISA has validated the technical and legal arrangements to collect and transmit the data referred to in Articles 8(1), 13, ~~19~~ ***18***, 34 and 39 and ~~have~~ ***has*** notified them to the Commission;

   (d) the Member States have notified the Commission as referred to in Article 61(1);

   (e) for the multiple-identity detector, the ETIAS Central Unit has notified the Commission as referred to in Article 61(3).

2. The Commission shall inform the European Parliament and the Council of the results of the test carried out pursuant to paragraph 1(b).

3. The Commission decision referred to in paragraph 1 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 interoperability components from the date determined by the Commission in accordance with paragraph 1.

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 Article~~s~~ ~~8(2),~~ ~~and~~ ~~9(7)~~ ***57(2) and 59(10)*** shall be conferred on the Commission for ~~an indeterminate~~ ***a*** period of ***five years*** ~~time~~ 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.***

3. The delegation of power referred to in Article~~s~~ ~~8(2),~~ ~~and~~ ~~9(7)~~ ***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.

6. A delegated act adopted pursuant to Article~~s~~ ~~8(2),~~ ~~and~~ ~~9(7)~~ ***57(2)*** shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of [two months] of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by [two months] at the initiative of the European Parliament or of the Council.

Article 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 in order to provide it with the expertise related to interoperability, in particular in the context of the preparation of its annual work programme and its annual activity report. 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.

2. ***The staff of Member State authorities, [the ETIAS Central Unit] and Europol, authorised to process data from the interoperability components, shall receive appropriate training about data security, data protection rules and the procedures of data processing, in which particular attention is 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 in light of objectives relating to planning and costs and to monitor the functioning of the interoperability components in light of objectives relating to the technical output, cost-effectiveness, security and quality of service.

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

3. For the purposes of technical maintenance, eu-LISA shall have access to the necessary information relating to the data processing operations performed in the interoperability components.

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

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

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

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

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

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

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

   The evaluations shall include any necessary recommendations. The Commission shall transmit the evaluation report to the European Parliament, to the Council, to the European Data Protection Supervisor and to the European Union Agency for Fundamental Rights established by Council Regulation (EC) No 168/2007.[65]

[65] 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).

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.

8. While respecting the provisions of national law on the publication of sensitive information, each Member State and Europol shall prepare annual reports on the effectiveness of access to data stored in the common identity repository for law enforcement purposes, containing information and statistics on:

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

   (b) reasonable grounds given for the substantiated suspicion that the suspect, perpetrator or victim is covered by the Eurodac Regulation;

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

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

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

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

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.*

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	*For the Council*
The President	The President