Council of the European Union

Brussels, 28 February 2018
(OR. en)

6550/18

Interinstitutional File: 2017/0351 (COD)

LIMITE

COSI 42
FRONT 44
ASIM 13
DAPIX 51
ENFOPOL 90
ENFOCUSTOM 35
SIRIS 11
SCHENGEN 3
DATAPROTECT 20
VISA 32
FAUXDOC 10
JAI 174
CT 29
COMIX 89
CODEC 270

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	15119/17 + COR 1
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on establishing a framework for interoperability between EU information systems (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 - Presidency revised text of Articles 33-69

Delegations will find below the text of Articles 33-69 of the proposal for the aforementioned Regulation, as revised by the Presidency based on the outcome of discussions on this part of the proposal by DAPIX: interoperability of EU information systems on 22-23 January 2018 as well as written drafting suggestions provided by Member States and a Schengen Associated Country.

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

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

ANNEX

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]

(…)

Article 33
White link

1. A link between data from two or more 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 at least one of the information systems does not have biometric data on the person;

   (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.

2. Where the CIR or the SIS are queried and where a white link exists between one or more of the 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 information systems shall reply indicating, where relevant, all the linked data on the person, hence triggering a hit[2] 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.

---

[1] General scrutiny reservations by: **CY, CZ, DE, EE, ES, FI, FR, IT, LT, LV, MT, NL, PL, PT, SE, SK, SI, UK, CH**
NL, PL parliamentary reservations.

[2] *The use of the term "hit(s)" here and elsewhere in the text is to be aligned with the corresponding definition in Article 4.*

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.

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.[3]

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 information systems whose data is linked;

(c) a single identification number allowing to retrieve the data from the 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.

[3] The Presidency proposes that following recital be added to explain this provision: ***"Access to the MID by Member State authorities and EU bodies is not foreseen where a white link exists between data from two or more information systems. However, this will not affect the users' access rights. Where it becomes evident when accessing data from two or more information systems that a white link was wrongly created, that Member State authority or EU body should be able to correct the situation and replace the link."***

Article 35
Data retention in the multiple-identity detector

1. 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 is stored in two or more EU information systems.

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 for as long as the corresponding data is stored in at least one of the EU information systems from which the linked data originates.***

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~~ ***name of the authority querying the MID***.

2. Each Member State shall keep logs of the staff duly authorised to use the MID.

3. The logs 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.

   The logs 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. 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*** 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 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.[4]

[4] 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 affairs**.**

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 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 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 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~~ ***shall*** be considered as controllers in accordance with Article 4(7) of Regulation (EU) 2016/679 and shall have responsibility for the processing of the personal data in the ~~multiple-identity detector~~ ***MID~~;~~.***

Article 41
Data processor

In relation to the processing of personal data in ***the shared BMS,*** the CIR ***and the MID***, eu-LISA 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 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~~.~~***;***

   (j) deny unauthorised persons access to data-processing facilities used for processing personal data.

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 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]*** 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, 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 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]*** 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~~ ***That authority*** shall reply to such requests within ~~45~~ ***60*** days of receipt of the request.

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, ~~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 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 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 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*~~ ***Audit*** *by the national supervisory* ~~*authority*~~ ***authorities***

1. The ***national*** 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.

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 body 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).

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 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 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 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 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)*** 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[5]
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. Where on entry or exit, the consultation of the relevant databases including the multiple-identity detector through the European search portal referred to respectively in [Article 4(36) and (33) of Regulation 2018/XX on interoperability] results in a yellow link or detects a red link, the person being checked shall be referred to the second-line check.

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 identities 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."

[5] **PT** scrutiny reservation

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]

2a) Article 3(1)(18) shall be replaced by the following:

"(18) 'biometric data' means fingerprint data or facial image;"

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);

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), 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 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 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".

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 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 otherwise 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 is stored in the EES."

16a) Article 32(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".

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~~ ***or*** 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 (cc), 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 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; 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)".

~~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 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 is stored in the VIS."

CHAPTER X
Final provisions

Article 56
Reporting and statistics

1. The duly authorised staff of the competent authorities of Member States, the Commission and eu-LISA shall have access to consult the following data related to the 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;~~

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

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

   (c) the number of each type of link ***and the EU information systems between which each link was established;*** ~~.~~

   (d) the period of time a yellow 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[6] shall have access to consult the data referred to in paragraphs 1, 2 and 3 for the purpose of carrying out risk analyses and vulnerability assessments as referred to in Articles 11 and 13 of that Regulation.

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

Article 57
Transitional period for the use of the European search portal[7]

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 a 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 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 and investigating terrorist offences or other serious criminal offences***

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

---

[6] 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).

[7] **FR**: scrutiny reservation.

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 hit(s) and the identity data of the linked files is identical or similar, a white link shall be created in accordance with Article 33.

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

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

3. Where a yellow link is created, 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.

Article 60
Costs[8]

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.

---

[8] **CH**: scrutiny reservation

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), 28(5) and (6), 37(4), 38(4), 39(5) and 44(5) 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;

   (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 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[9]

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

2. The power to adopt delegated acts referred to in Articles 8(2)***,*** ~~and~~ 9(7) ***and 57(2)*** 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.***

[9] **FR, NL:** scrutiny reservation

3. The delegation of power referred to in Articles 8(2)**,** ~~and~~ 9(7) ***and 57(2)*** may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement 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 Articles 8(2)**,** ~~and~~ 9(7) ***and 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.

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.***

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.[10]

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.[11] 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 ***of preventing, detecting and 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 common identity repository for ~~law enforcement~~ purposes ***of preventing, detecting and investigation terrorist offences or other serious criminal offences***;

---

[10] 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).

[11] **FR:** scrutiny reservation

(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