Council of the European Union

Brussels, 1 October 2021
(OR. en)

Interinstitutional File: 2020/0350(COD)

10862/4/21
REV 4

LIMITE

SIRIS 83
ENFOPOL 286
COPEN 326
SCHENGEN 73
COMIX 389
CODEC 1097
IXIM 150

NOTE

From:	Presidency
To:	Delegations
No. Cion doc.:	13882/20
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters as regards the entry of alerts by Europol

Delegations will find in annex the Presidency's compromise proposals on the abovementioned amendments to the SIS Regulation.

All changes proposed by the Presidency, as compared to the Commission proposal in 13882/20 (recitals) or to Regulation (EU) 2018/1862[1] currently in force (operative part starting on page 9), appear as ~~strikethrough~~ and **bold underlined**.

[1] Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56) amended by Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 (OJ L 135, 22.05.2019, p. 85).

This revised version includes a number of modifications and/ or additions in Articles 37a and 48. These changes appear highlighted in yellow.

The Presidency's compromise proposals gathered a broad support at the informal meeting of the members of the Working Party on JHA Information Exchange (IXIM) held on 30 September. Unless there are substantial reservations by delegations by next **Tuesday 5 October 2021 cob**, the Presidency intends to seek the endorsement of these compromise proposals by Coreper in order to start negotiations with the EP.

ANNEX

2020/0350 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

amending Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters as regards the entry of alerts by Europol

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 point (a) of Article 88(2) thereof,

Having regard to the proposal from the European Commission,

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

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The Schengen Information System ('SIS') constitutes an essential tool for maintaining a high level of security within the area of freedom, security and justice of the Union by supporting operational cooperation between national competent authorities, in particular border guards, the police, customs authorities, immigration authorities, and authorities responsible for the prevention, detection, investigation or prosecution of criminal offences or execution of criminal penalties. Regulation (EU) 2018/1862 of the European Parliament and of the Council[1] constitutes the legal basis for SIS in respect of matters falling within the scope of Chapters 4 and 5 of Title V of Part Three of the Treaty on Functioning of the European Union (TFEU).

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

(2) Alerts on persons and objects entered in SIS are in real time made available directly to all end-users of the competent national authorities of Member States that use SIS pursuant to Regulation (EU) 2018/1862. SIS alerts contain information about a particular person or object as well as instructions for the authorities on what to do when the person or object has been found.

(3) The European Union Agency for Law Enforcement Cooperation (Europol), established by Regulation (EU) 2016/794 of the European Parliament and of the Council[2], plays an important role in the use of SIS and in the exchange of supplementary information with Member States on SIS alerts. ~~Nevertheless, according to existing rules, alerts in SIS can only be issued by Member States' competent authorities.~~

(3a) The fight against serious crime and terrorism should be subject to continuous coordination amongst the Member States on the processing of data and on the insertion of alerts into the SIS.

(4) Given the increasingly global nature of serious crime and terrorism brought about by growing mobility, the information that third countries and international organisations, such as the International Criminal Police Organization and the International Criminal Court, obtain about criminals and terrorists is increasingly relevant for the Union's security. Such information should contribute to the comprehensive efforts to ensure internal security in the European Union. Some of this information is only shared with Europol. While Europol holds valuable information received from external partners on serious criminals and terrorists, it cannot issue alerts in SIS. Member States are also not always able to issue alerts in SIS on the basis of such information.

(5) In order to bridge the gap in information sharing on serious crime and terrorism, in particular on foreign terrorist fighters – where the monitoring of their movement is crucial – it is necessary to ensure **that upon the proposal of Europol, Member States are able to enter an alert in the interest of the Union,** ~~Europol is able~~ to make this information available directly and in real-time to front-line officers in Member States.

~~(6) Europol should therefore be authorised to enter alerts in SIS pursuant to Regulation (EU) 2018/1862, in full respect of fundamental rights and data protection rules.~~

(7) To that end, a specific category of alert should be created in SIS, to be issued **by the Member States at their discretion and subject to their verification and analysis upon the proposal of Europol in the interest of the Union on third-country nationals** ~~exclusively by Europol~~, in order to inform end-users carrying out a search in SIS that the person concerned is suspected of being involved in a criminal offence in respect of which Europol is competent, and in order for **Member States and** Europol to obtain confirmation that the person who is subject to the alert has been located.

---

[2] 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. 53–114).

(8) In order **for the requested Member State** to assess whether a concrete case is adequate, relevant and important enough to warrant the entry of an alert in SIS, and in order to confirm the reliability of the source of information and the accuracy of the information on the person concerned, Europol should **share all of the information it holds on the case, in particular the outcome of** ~~carry out a detailed individual assessment of each case including further consultations with the third country or international organisation that shared the data on the person concerned, as well as further analysis of the case, in particular by~~ cross~~-~~checking ~~it~~ **the data** against ~~information it already holds in~~ its databases, **information relating** to the accuracy **and reliability** of the ~~information and complement it with other data on the basis of its own databases~~**data and** ~~. The detailed individual assessment should include~~ the analysis of whether there are sufficient grounds for considering that the person has committed or taken part in, or will commit a criminal offence in respect of which Europol is competent.

(8 *bis*) In order to ensure the lawfulness, completeness and accuracy of SIS data, Europol should transmit additional or modified data in relation to an alert that was entered upon its proposal to the issuing Member State without delay, in order to allow the issuing Member State to complete or modify the alert, in particular, if Europol becomes aware that the information received from the authorities of a third country or international organisation was incorrect or was communicated to Europol for unlawful purposes, for example if sharing the information on the person was motivated by political reasons.

~~(9) Europol should only be able to enter an alert in SIS if the person concerned is not already subject to a SIS alert issued by a Member State. A further precondition for the creation of such an alert should be that Member States do not object to the alert being issued in SIS. Therefore, it is necessary to establish rules on the obligations of Europol prior to entering data in SIS, in particular the obligation to consult the Member States in line with Regulation (EU) 2016/794. It should also be possible for Member States to request the deletion of an alert by Europol, in particular if they obtain new information about the person who is the subject of the alert, if their national security requires so or when it is likely that the alert would represent a risk for official or legal inquiries, investigations or procedures.~~

~~(10) Europol should keep records of the individual assessment of each case, which should include the grounds for entering the alert, for the purposes of verifying the lawfulness of the data processing, self-monitoring and ensuring proper data integrity and security. In accordance with Regulation (EU) 2016/794, Europol should co-operate with the European Data Protection Supervisor and make these records available upon request, so that they can be used for monitoring processing operations.~~

~~(11) It is necessary to establish rules concerning the deletion of alerts entered in SIS by Europol. An alert should be kept only for the time required to achieve the purpose for which it was entered. It is therefore appropriate to set out detailed criteria to determine when the alert should be deleted. An alert entered by Europol in SIS should be deleted in particular if a Member State objects, another alert is entered in SIS by a Member State, or if Europol becomes aware that the information received from the third country or international organisation was incorrect or was communicated to Europol for unlawful purposes, for example if sharing the information on the person was motivated by political reasons.~~

(12) ~~When entering alerts in SIS, Europol should be bound by the same requirements and obligations applicable to the Member States pursuant to Regulation (EU) 2018/1862 when they enter alerts in SIS. In particular, Europol should comply with common standards, protocols and technical procedures established to ensure the compatibility of its technical interface with Central SIS for the prompt and effective transmission of data. Requirements concerning general data processing rules, proportionality, data quality, data security, reporting and obligations related to collecting statistics applicable to Member States when entering alerts in SIS should apply to Europol as well.~~

(13) Regulation (EU) 2018/1725 of the European Parliament and of the Council[3] and Regulation (EU) 2016/794 should apply to the processing of personal data by Europol when carrying out its responsibilities under this Regulation. ~~The European Data Protection Supervisor should carry out periodic audits on the data processing of Europol concerning SIS and the exchange of supplementary information.~~

(14) Since the objectives of this Regulation, namely the establishment and regulation of a specific alert category issued **by Member States upon a proposal by Europol in the interest of the Union** ~~by Europol~~ in SIS in order to exchange information on persons who represent a threat to the internal security of the European Union, cannot be sufficiently achieved by the Member States, but can rather, by reason of their nature be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity, as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.

(15) This Regulation respects fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. In particular, this Regulation fully respects the protection of personal data in accordance with Article 8 of the Charter of Fundamental Rights of the European Union while seeking to ensure a safe environment for all persons residing on the territory of the Union.

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

---

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

(17) Ireland is taking part in this Regulation in accordance with Article 5(1) of Protocol No 19 annexed to the TEU and to the TFEU and Article 6(2) of Council Decision 2002/192/EC[4] and Council Implementing Decision (EU) 2020/1745[5].

(18) As regards Iceland and Norway, this Regulation constitutes a development of provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latters' association with the implementation, application and development of the Schengen *acquis*[6], which fall within the area referred to in Article 1, point (G) of Council Decision 1999/437/EC[7].

(19) As regards Switzerland, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*[8], which fall within the area referred to in Article 1, point (G), of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/149/JHA[9].

---

4 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).

5 Council Implementing Decision (EU) 2020/1745 of 18 November 2020 on the putting into effect of the provisions of the Schengen acquis on data protection and on the provisional putting into effect of certain provisions of the Schengen acquis in Ireland (OJ L 393, 23.11.2020, p. 3).

6 OJ L 176, 10.7.1999, p. 36.

7 Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis* (OJ L 176, 10.7.1999, p. 31).

8 OJ L 53, 27.2.2008, p. 52.

9 Council Decision 2008/149/JHA of 28 January 2008 on the conclusion on behalf of the European Union of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L 53, 27.2.2008, p. 50).

(20) 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*[10], which fall within the area referred to in Article 1, point (G), of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/349/EU[11].

(21) As regards Bulgaria and Romania, this Regulation constitutes an act building upon, or otherwise relating to, the Schengen *acquis* within the meaning of Article 4(2) of the 2005 Act of Accession and should be read in conjunction with Council Decisions 2010/365/EU[12] and (EU) 2018/934[13].

(22) As regards Croatia, this Regulation constitutes an act building upon, or otherwise relating to, the Schengen *acquis* within the meaning of Article 4(2) of the 2011 Act of Accession and should be read in conjunction with Council Decision (EU) 2017/733[14].

(23) Concerning Cyprus, this Regulation constitutes an act building upon, or otherwise relating to, the Schengen *acquis* within the meaning of Article 3(2) of the 2003 Act of Accession [to add eventual Council Decision].

---

10 OJ L 160, 18.6.2011, p. 21.

11 Council Decision 2011/349/EU of 7 March 2011 on the conclusion on behalf of the European Union of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*, relating in particular to judicial cooperation in criminal matters and police cooperation (OJ L 160, 18.6.2011, p. 1).

12 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).

13 Council Decision (EU) 2018/934 of 25 June 2018 on the putting into effect of the remaining provisions of the Schengen *acquis* relating to the Schengen Information System in the Republic of Bulgaria and Romania (OJ L 165, 2.7.2018, p. 37).

14 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).

(24) The European Data Protection Supervisor was consulted, in accordance with Article 41(2) of Regulation (EU) 2018/1725 of the European Parliament and the Council[15].

(25) Regulation (EU) No 2018/1862 should therefore be amended accordingly,

HAVE ADOPTED THIS REGULATION:

Article 1

Amendments to Regulation (EU) 2018/1862

Article 3

Definitions

(8) 'flag' means a suspension of the validity of an alert at the national level that may be added to alerts for arrest, alerts on missing and vulnerable persons**,** ~~and~~ alerts for discreet, inquiry and specific checks **and information alerts on third-country nationals in the interest of the Union**;

(22) 'third-country national' means any person who is not a citizen of the Union within the meaning of Article 20(1) TFEU, with the exception of persons who are beneficiaries of the right of free movement within the Union in accordance with Directive 2004/38/EC or with an agreement between the Union or the Union and its Members States on the one hand, and a third country on the other hand;

[15] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

Article 20

Categories of data

1. Without prejudice to Article 8(1) or to the provisions of this Regulation providing for the storage of additional data, SIS shall contain only those categories of data which are supplied by each Member State, as required for the purposes laid down in Articles 26, 32, 34, 36, **37a,** 38 and 40.

2. The categories of data shall be as follows:

   (a) information on persons in relation to whom an alert has been entered;

   (b) information on objects referred to in Articles 26, 32, 34, 36**, 37a,** and 38.

3. Any alert in SIS which includes information on persons shall contain only the following data:

   (a) surnames;

   (b) forenames;

   (c) names at birth;

   (d) previously used names and aliases;

   (e) any specific, objective, physical characteristics not subject to change;

   (f) place of birth;

   (g) date of birth;

   (h) gender;

   (i) any nationalities held;

   (j) whether the person concerned:

      (i) is armed;

      (ii) is violent;

(iii) has absconded or escaped;

(iv) poses a risk of suicide;

(v) poses a threat to public health; or

(vi) is involved in an activity referred to in Articles 3 to 14 of Directive (EU) 2017/541;

(k) the reason for the alert;

(l) the authority which created the alert;

(m) a reference to the decision giving rise to the alert;

(n) the action to be taken in the case of a hit;

(o) links to other alerts pursuant to Article 63;

(p) the type of offence;

(q) the person's registration number in a national register;

(r) for alerts referred to in Article 32(1), a categorisation of the type of case;

(s) the category of the person's identification documents;

(t) the country of issue of the person's identification documents;

(u) the number(s) of the person's identification documents;

(v) the date of issue of the person's identification documents;

(w) photographs and facial images;

(x) in accordance with Article 42(3), relevant DNA profiles;

(y) dactyloscopic data;

(z) a copy of the identification documents, in colour wherever possible.

4. The Commission shall adopt implementing acts to lay down and develop the technical rules necessary for entering, updating, deleting and searching the data referred to in paragraphs 2 and 3 of this Article and the common standards referred to in paragraph 5 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 76(2).

5. Technical rules shall be similar for searches in CS-SIS, in national or shared copies and in technical copies made under Article 56(2). They shall be based on common standards.

Article 24

General provisions on flagging

1. Where a Member State considers that to give effect to an alert entered in accordance with Article 26, 32**,** ~~or~~ 36 **or 37a** is incompatible with its national law, its international obligations or essential national interests, it may require that a flag be added to the alert to the effect that the action to be taken on the basis of the alert will not be taken in its territory. The flag shall be added by the SIRENE Bureau of the issuing Member State.

2. In order to enable Member States to require that a flag be added to an alert entered in accordance with Article 26, all Member States shall be notified automatically of any new alert of that category through the exchange of supplementary information.

3. If in particularly urgent and serious cases, an issuing Member State requests the execution of the action, the executing Member State shall examine whether it is able to allow the flag added at its behest to be withdrawn. If the executing Member State is able to do so, it shall take the necessary steps to ensure that the action to be taken can be carried out immediately.'

CHAPTER IXa

Information alerts on third-country nationals in the interest of the Union

Article 37a

Objectives and conditions for entering alerts

1. **Member States may enter information alerts on third-country nationals in SIS, in accordance with point r) of Article 4 of Regulation (EU) 2016/794, upon a proposal by Europol to enter an alert on the basis of information from the authorities of third countries or international organisations.**

2. **Such information alerts shall be issued in the interest of the Union for the purpose of informing end-users carrying out a search in SIS of the suspected involvement of those third-country nationals in terrorist offences or in serious and organised crime as listed in Annex I to Regulation (EU) 2016/794, with a view to obtain the information set out in Article 37b.**

3. **Europol may only propose the entry of information alerts on persons in one or more of the following circumstances:**

(a) **where there is a factual indication that a person intends to commit or is committing an offence referred to in paragraph 2;**

(b) **where an overall assessment of a person, in particular on the basis of past criminal offences, gives reason to believe that that person may commit an offence referred to in paragraph 2.**

4. **Europol may only propose the entry of an information alerts on persons after it has ensured all of the following:**

(a) **an analysis of the data provided in accordance with Article 17(1)(b) of Regulation (EU) 2016/794 confirmed the reliability of the source of information as well as the accuracy of the information on the person concerned, permitting Europol to determine that the conditions of paragraph 3 are met, where necessary, after having carried out further exchanges of information with the data provider in accordance with Article 25 of Regulation (EU) 2016/794;**

(b) **a search in SIS, carried out in accordance with Article 48 of this Regulation, did not disclose the existence of an alert on the person concerned.**

5. **Europol shall make available the information it holds on the case and the results of the assessment referred to in paragraphs 3 and 4 to the Member States and request one or more Member States to enter the alert.**

6. **Information alerts shall be entered in SIS at the discretion of the Member State requested to enter an alert and shall be subject to its verification and analysis of Europol's proposal. The issuing Member State shall communicate the entry of alerts under this Article to the other Member States and Europol through the exchange of supplementary information.**

7. **Member States may refuse entering the alert upon the proposal by Europol or may also, if the respective conditions are met, decide to enter another type of alert on the same person.**

8. **Member States shall put in place a periodic reporting mechanism in order to inform other Member States and Europol on the outcome of the verification and analysis and on whether or not the data has been inserted in the SIS, within a period of 12 months from the communication by Europol of its information to the Member States.**

9. **Where Europol has relevant additional or modified data in relation to an alert that was entered upon its proposal, it shall transmit them without delay, through the exchange of supplementary information, to the issuing Member State to enable the latter to complete or modify the alert.**

10. **Where Europol has evidence suggesting that data entered in SIS according to paragraph 1 of this Article are factually incorrect or have been unlawfully stored, it shall, through the exchange of supplementary information, inform the issuing Member State as soon as possible and not later than two working days after that evidence has come to its attention. The issuing Member State shall check the information and, if necessary, correct or delete the data in question without delay.**

11. **Where there is a clear indication that the objects referred to in points (a), (b), (c), (e), (g), (h), (j) and (k) of Article 38(2) or non-cash means of payment are connected with a person who is the subject of an alert pursuant to paragraph 1 of this Article, alerts on those objects may be entered in order to locate the person. In such cases, the alert on the person and the alert on the object shall be linked in accordance with Article 63.**

12. **Member States shall put in place the necessary procedures for entering, updating and deleting information alerts in SIS in accordance with this Regulation.**

13. **Europol shall keep records relating to its requests for entering alerts in SIS under this Article and provide reports to Member States every six months on the alerts inserted in the SIS and the cases where Member States did not enter the alerts.**

14. **The Commission shall adopt implementing acts to lay down and develop rules necessary for entering, updating, deleting and searching the data referred to in paragraph 11 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 76(2).**

Article 37b

Execution of the action based on an alert

1. In the event of a hit on an information alert, the executing Member State shall collect and communicate to the issuing Member State all or some of the following information:

(a) the fact that the person who is the subject of an alert has been located;

(b) the place, time and reason for the check;

(c) the route of the journey and destination;

(d) the persons accompanying the subject of the alert who can reasonably be expected to be associated with the subject of the alert;

(e) objects used or carried, including travel documents;

(f) the circumstances in which the person was located.

2. The executing Member State shall communicate the information referred to in paragraph 1 through the exchange of supplementary information.

3. The executing Member State shall ensure the discreet collection of as much information described in paragraph 1 as possible during routine activities carried out by its national competent authorities. The collection of this information shall not jeopardise the discreet nature of the checks and the subject of the alert shall in no way be made aware of the existence of the alert.

Article 43

Specific rules for verification or search with photographs, facial images, dactyloscopic data and DNA profiles

1. Where photographs, facial images, dactyloscopic data and DNA profiles are available in an alert in SIS, such photographs, facial images, dactyloscopic data and DNA profiles shall be used to confirm the identity of a person who has been located as a result of an alphanumeric search made in SIS.

2. Dactyloscopic data may be searched in all cases to identify a person. However, dactyloscopic data shall be searched to identify a person where the identity of the person cannot be ascertained by other means. For that purpose, the Central SIS shall contain an Automated Fingerprint Identification System (AFIS).

3. Dactyloscopic data in SIS in relation to alerts entered in accordance with Articles 26, 32, 36**,** **37a,** and 40 may also be searched using complete or incomplete sets of fingerprints or palm prints discovered at the scenes of serious crimes or terrorist offences under investigation, where it can be established to a high degree of probability that those sets of prints belong to a perpetrator of the offence and provided that the search is carried out simultaneously in the Member State's relevant national fingerprints databases.

Article 48

Access to and search of data in SIS by Europol

1. ~~The European Union Agency for Law Enforcement Cooperation (Europol), established by Regulation (EU) 2016/794~~ **Europol** shall, where necessary to fulfil its mandate, have the right to access and search data in SIS. Europol may also exchange and further request supplementary information in accordance with the provisions of the SIRENE Manual.

2. Where a search by Europol reveals the existence of an alert in SIS, Europol shall inform the issuing Member State through the exchange of supplementary information by means of the Communication Infrastructure and in accordance with the provisions set out in the SIRENE Manual. Until Europol is able to use the functionalities intended for the exchange of supplementary information, it shall inform issuing Member States through the channels defined by Regulation (EU) 2016/794.

3. Europol may process the supplementary information that has been provided to it by Member States for the purposes of comparing it with its databases and operational analysis projects, aimed at identifying connections or other relevant links and for the strategic, thematic or operational analyses referred to in points (a), (b) and (c) of Article 18(2) of Regulation (EU) 2016/794. Any processing by Europol of supplementary information for the purpose of this Article shall be carried out in accordance with that Regulation.

4. Europol's use of information obtained from a search in SIS or from the processing of supplementary information shall be subject to the consent of the ~~issuing~~ Member State **that provided information**. If the Member State allows the use of such information, its handling by Europol shall be governed by Regulation (EU) 2016/794. Europol shall only communicate such information to third countries and third bodies with the consent of the ~~issuing~~ Member State **that provided information** and in full compliance with Union law on data protection.

5. Europol shall:

   (a) without prejudice to paragraphs 4 and 6, not connect parts of SIS nor transfer the data contained in it to which it has access to any system for data collection and processing operated by or at Europol, nor download or otherwise copy any part of SIS;

(b) notwithstanding Article 31(1) of Regulation (EU) 2016/794, delete supplementary information containing personal data at the latest one year after the related alert has been deleted. By way of derogation, where Europol has information in its databases or operational analysis projects on a case to which the supplementary information is related, in order for Europol to perform its tasks, Europol may exceptionally continue to store the supplementary information when necessary. Europol shall inform the issuing and the executing Member State of the continued storage of such supplementary information and present a justification for it;

(c) limit access to data in SIS, including supplementary information, to specifically authorised staff of Europol who require access to such data for the performance of their tasks;

(d) adopt and apply measures to ensure security, confidentiality and self-monitoring in accordance with Articles 10, 11 and 13;

(e) ensure that its staff who are authorised to process SIS data receive appropriate training and information in accordance with Article 14(1); and

(f) without prejudice to Regulation (EU) 2016/794, allow the European Data Protection Supervisor to monitor and review the activities of Europol in the exercise of its right to access and search data in SIS and in the exchange and processing of supplementary information.

6. Europol shall only copy data from SIS for technical purposes where such copying is necessary in order for duly authorised Europol staff to carry out a direct search. This Regulation shall apply to such copies. The technical copy shall only be used for the purpose of storing SIS data whilst those data are searched. Once the data have been searched they shall be deleted. Such uses shall not be considered to be unlawful downloading or copying of SIS data. Europol shall not copy alert data or additional data issued by Member States or from CS-SIS into other Europol systems.

7. For the purpose of verifying the lawfulness of data processing, self-monitoring and ensuring proper data security and integrity, Europol shall keep logs of every access to and search in SIS in accordance with the provisions of Article 12. Such logs and documentation shall not be considered to be unlawful downloading or copying of part of SIS.

8. ~~Member States shall inform Europol through the exchange of supplementary information of any hit on alerts related to terrorist offences~~.

Member States shall inform Europol through the exchange of supplementary information of any hit on:

a) alerts issued under Article 37a also when hits occur in the territory of the issuing Member State; and

b) alerts related to terrorist offences which are not issued under Article 37a.

Member States may exceptionally not inform Europol **of hits on alerts under point b) of this paragraph** if doing so would jeopardise current investigations, the safety of an individual or be contrary to essential interests of the security of the issuing Member State.

~~9. Paragraph 8 shall apply from the date that Europol is able to receive supplementary information in accordance with paragraph 1.~~

Article 53

Review period for alerts on persons

1. Alerts on persons shall be kept only for the time required to achieve the purposes for which they were entered.

2. A Member State may enter an alert on a person for the purposes of Article 26 and points (a) and (b) of Article 32(1) for a period of five years. The issuing Member State shall review the need to retain the alert within the five year period.

3. A Member State may enter an alert on a person for the purposes of Articles 34 and 40 for a period of three years. The issuing Member State shall review the need to retain the alert within the three year period.

4. A Member State may enter an alert on a person for the purposes of points (c), (d) and (e) of Article 32 (1)**,** ~~and~~ of Article 36**, and of Article 37a** for a period of one year. The issuing Member State shall review the need to retain the alert within the one year period.

5. Each Member State shall, where appropriate, set shorter review periods in accordance with its national law.

6. Within the review period referred to in paragraphs 2, 3**,** ~~and~~ 4~~,~~ **and 5**, the issuing Member State may, following a comprehensive individual assessment, which shall be recorded, decide to retain the alert on a person for longer than the review period, where this proves necessary and proportionate for the purposes for which the alert was entered. In such cases paragraph 2, 3**,** ~~or~~ 4~~,~~ **and 5 of this Article** shall also apply to the extension. Any such extension shall be communicated to CS-SIS.

7. Alerts on persons shall be deleted automatically after the review period referred to in paragraphs 2, 3**,** ~~and~~ 4~~,~~ **and 5** has expired, except where the issuing Member State has informed CS-SIS of an extension pursuant to paragraph 6 **of this Article**. CS-SIS shall automatically inform the issuing Member State of the scheduled deletion of data four months in advance. **CS-SIS shall also inform Europol of the scheduled deletion of data entered under Article 37a four months in advance. Europol shall assist the issuing Member State without delay with its comprehensive individual assessment mentioned in paragraph 6.**

8. Member States shall keep statistics on the number of alerts on persons the retention periods of which have been extended in accordance with paragraph 6 of this Article and transmit them, upon request, to the supervisory authorities referred to in Article 69.

Article 54

Review period for alerts on objects

1. Alerts on objects shall be kept only for the time required to achieve the purposes for which they were entered.

2. A Member State may enter an alert on objects for the purposes of Articles 36 and 38 for a period of ten years. The issuing Member State shall review the need to retain the alert within the ten-year period.

3. Alerts on objects entered in accordance with Articles 26, 32, 34, ~~and~~ 36 **and 37a** shall be reviewed pursuant to Article 53 where they are linked to an alert on a person. Such alerts shall only be kept for as long as the alert on the person is kept.

4. Within the review period referred to in paragraphs 2 and 3, the issuing Member State may decide to retain the alert on an object for longer than the review period, where this proves necessary for the purposes for which the alert was entered. In such cases paragraph 2 or 3 shall apply, as appropriate.

5. The Commission may adopt implementing acts to establish shorter review periods for certain categories of alerts on objects. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 76(2).

6. Member States shall keep statistics on the number of alerts on objects the retention periods of which have been extended in accordance with paragraph 4.

Article 55

Deletion of alerts

1. Alerts for arrest for surrender or extradition purposes pursuant to Article 26 shall be deleted when the person has been surrendered or extradited to the competent authorities of the issuing Member State. They shall also be deleted when the judicial decision on which the alert was based has been revoked by the competent judicial authority in accordance with national law. They shall also be deleted upon the expiry of the alert in accordance with Article 53.

2. Alerts on missing persons or vulnerable persons who need to be prevented from travelling pursuant to Article 32 shall be deleted in accordance with the following rules:

   (a) concerning missing children and children at risk of abduction, an alert shall be deleted upon:

      (i) the resolution of the case, such as when the child has been located or repatriated or the competent authorities in the executing Member State have taken a decision on the care of the child;

(ii) the expiry of the alert in accordance with Article 53; or

(iii) a decision by the competent authority of the issuing Member State;

(b) concerning missing adults, where no protective measures are requested, an alert shall be deleted upon:

(i) the execution of the action to be taken, where their whereabouts are ascertained by the executing Member State;

(ii) the expiry of the alert in accordance with Article 53; or

(iii) a decision by the competent authority of the issuing Member State;

(c) concerning missing adults where protective measures are requested, an alert shall be deleted upon:

(i) the carrying out of the action to be taken, where the person is placed under protection;

(ii) the expiry of the alert in accordance with Article 53; or

(iii) a decision by the competent authority of the issuing Member State;

(d) concerning vulnerable persons who are of age who need to be prevented from travelling for their own protection and children who need to be prevented from travelling, an alert shall be deleted upon:

(i) the carrying out of the action to be taken such as the person's placement under protection;

(ii) the expiry of the alert in accordance with Article 53; or

(iii) a decision by the competent authority of the issuing Member State.

Without prejudice to the national law, where a person has been institutionalised following a decision by a competent authority an alert may be retained until that person has been repatriated.

3. Alerts on persons sought for a judicial procedure pursuant to Article 34 shall be deleted upon:

(a) the communication of the whereabouts of the person to the competent authority of the issuing Member State;

(b) the expiry of the alert in accordance with Article 53; or

(c) a decision by the competent authority of the issuing Member State.

Where the information in the communication referred to in point (a) cannot be acted upon, the SIRENE Bureau of the issuing Member State shall inform the SIRENE Bureau of the executing Member State in order to resolve the problem.

In the event of a hit where the address details were forwarded to the issuing Member State and a subsequent hit in the same executing Member State reveals the same address details, the hit shall be recorded in the executing Member State but neither the address details nor supplementary information shall be resent to the issuing Member State. In such cases the executing Member State shall inform the issuing Member State of the repeated hits and the issuing Member State shall carry out a comprehensive individual assessment of the need to retain the alert.

4. Alerts for discreet, inquiry and specific checks pursuant to Article 36, shall be deleted upon:

(a) the expiry of the alert in accordance with Article 53; or

(b) a decision to delete them by the competent authority of the issuing Member State.

4a. Information alerts in the interest of the Union pursuant to Article 37a, shall be deleted upon:

(a) the expiry of the alert in accordance with Article 53; or

(b) a decision to delete them by the competent authority of the issuing Member State, where appropriate upon a proposal by Europol.

5. Alerts on objects for seizure or use as evidence in criminal proceedings pursuant to Article 38, shall be deleted upon:

(a) the seizure of the object or equivalent measure once the necessary follow-up exchange of supplementary information has taken place between the SIRENE Bureaux concerned or the object becomes the subject of another judicial or administrative procedure;

(b) the expiry of the alert in accordance with Article 53; or

(c) a decision to delete them by the competent authority of the issuing Member State.

6. Alerts on unknown wanted persons pursuant to Article 40 shall be deleted upon:

(a) the identification of the person;

(b) the expiry of the alert in accordance with Article 53; or

(c) a decision to delete them by the competent authority of the issuing Member State.

7. Where it is linked to an alert on a person, an alert on an object entered in accordance with Articles 26, 32, 34**,** ~~and~~ 36 **and 37a** shall be deleted when the alert on the person is deleted in accordance with this Article.

CHAPTER XV

General data processing rules

Article 56

Processing of SIS data

1. The Member States shall only process the data referred to in Article 20 for the purposes laid down for each category of alert referred to in Articles 26, 32, 34, 36, **37a,** 38 and 40.

2. Data shall only be copied for technical purposes, where such copying is necessary in order for the competent authorities referred to in Article 44 to carry out a direct search. This Regulation shall apply to those copies. A Member State shall not copy the alert data or additional data entered by another Member State from its N.SIS or from the CS-SIS into other national data files.

3. Technical copies referred to in paragraph 2 which result in offline databases may be retained for a period not exceeding 48 hours.

   Member States shall keep an up-to-date inventory of those copies, make that inventory available to their supervisory authorities, and ensure that this Regulation, in particular Article 10, is applied in respect of those copies.

4. Access to data in SIS by national competent authorities referred to in Article 44 shall only be authorised within the limits of their competence and only to duly authorised staff.

5. With regard to the alerts laid down in Articles 26, 32, 34, 36, **37a,** 38 and 40 of this Regulation, any processing of information in SIS for purposes other than those for which it was entered into SIS has to be linked with a specific case and justified by the need to prevent an imminent and serious threat to public policy and to public security, on serious grounds of national security or for the purposes of preventing a serious crime. Prior authorisation from the issuing Member State shall be obtained for this purpose.

6. Any use of SIS data which does not comply with paragraphs 1 to 5 of this Article shall be considered as misuse under the national law of each Member State and subject to penalties in accordance with Article 73.

7. Each Member State shall send to eu-LISA a list of its competent authorities which are authorised to search the data in SIS directly pursuant to this Regulation, as well as any changes to the list. The list shall specify, for each authority, which data it may search and for what purposes. eu-LISA shall ensure that the list is published in the Official Journal of the European Union annually. eu-LISA shall maintain a continuously updated list on its website containing changes sent by Member States between the annual publications.

8. Insofar as Union law does not lay down specific provisions, the law of each Member State shall apply to data in its N.SIS.

CHAPTER XVIII

Final provisions

Article 79

Entry into force, start of operation and application

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

2. No later than 28 December 2021 the Commission shall adopt a decision setting the date on which SIS operations start pursuant to this Regulation, after verification that the following conditions have been met:

   (a) the implementing acts necessary for the application of this Regulation have been adopted;

   (b) Member States have notified the Commission that they have made the necessary technical and legal arrangements to process SIS data and exchange supplementary information pursuant to this Regulation; and

   (c) eu-LISA has notified the Commission of the successful completion of all testing activities with regard to CS-SIS and to the interaction between CS-SIS and N.SIS.

3. The Commission shall closely monitor the process of gradual fulfilment of the conditions set out in paragraph 2 and shall inform the European Parliament and the Council about the outcome of the verification referred to in that paragraph.

4. By 28 December 2019 and every year thereafter until the decision of the Commission referred to in paragraph 2 has been taken, the Commission shall submit a report to the European Parliament and to the Council on the state of play of preparations for the full implementation of this Regulation. That report shall contain also detailed information about the costs incurred and information as to any risks which may impact the overall costs.

5. This Regulation shall apply from the date determined in accordance with paragraph 2.

   By way of derogation from the first subparagraph:

   (a) Article 4(4), Article 5, Article 8(4), Article 9(1) and (5), Article 12(8), Article 15(7), Article 19, Article 20(4) and (5), Article 26(6), Article 32(9), Article 34(3), Article 36(6), Article 38(3) and (4), Article 42(5), Article 43(4), Article 54(5), Article 62(4), Article 63(6), Article 74(7) and (10), Article 75, Article 76, points (1) to (5) of Article 77, and paragraphs 3 and 4 of this Article shall apply from the date of entry into force of this Regulation;

   (b) points (7) and (8) of Article 77 shall apply from 28 December 2019;

   (c) point 6 of Article 77 shall apply from 28 December 2020.

6. The Commission decision referred to in paragraph 2 shall be published in the Official Journal of the European Union.

7. The Commission shall adopt a decision setting the date on which Member States shall start entering, updating and deleting data in SIS according to Article 37a of this Regulation as amended by Regulation [XXX], after verification that the following conditions have been met:

(a) the implementing acts adopted pursuant to this Regulation have been amended to the extent necessary for the application of this Regulation as amended by Regulation [XXX];

(b) Member States and Europol have notified the Commission that they have made the necessary technical and procedural arrangements to process SIS data and exchange supplementary information pursuant to this Regulation as amended by Regulation [XXX];

(c) eu-LISA has notified the Commission of the successful completion of all testing activities with regard to CS-SIS and to the interaction between CS-SIS and N.SIS.

This decision shall be published 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.

Article 2

Entry into force

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

It shall apply from the date determined in accordance with Article 79(7) of Regulation (EU) 2018/1862.

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

Done at Brussels,

For the European Parliament *For the Council*

The President *The President*