



Council of the  
European Union

Brussels, 15 July 2021  
(OR. en)

10862/21

---

---

**Interinstitutional File:  
2020/0350(COD)**

---

---

**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 Regulation (EU) 2018/1862<sup>1</sup> currently in force, appear as ~~strike through~~ and **bold underlined**.

---

<sup>1</sup> 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).

*Article 1*

*Amendments to Regulation (EU) 2018/1862*

*Article 3*

**Definitions**

**(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;**

*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 in the interest of the Union on third-country nationals in SIS 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, as well as for the purpose of obtaining the information set out in Article 37b.**
- 2. Information alerts shall be entered 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 third countries or international organisations. To this end, Europol shall make available the information it holds on the case to the Member State requested to enter the alert.**
- 3. Information alerts shall be entered in SIS at the discretion of the issuing Member State and shall be subject to the verification and analysis of Europol's proposal to enter an alert by the issuing Member State.**
- 4. Member States may refuse entering the alert upon the proposal by Europol or may also decide to enter another type of alert on the same person.**
- 5. 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.**

- 6. 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.**
- 7. 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.**
- 8. Member States shall put in place the necessary procedures for entering, updating and deleting information alerts in SIS in accordance with this Regulation.**
- 9. 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 7 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.

**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 the information either as issuing Member State or as executing Member State**. 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 the 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~~ alert **issued under Article 37a** ~~s related to terrorist offences~~.

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

**a) alerts issued under Article 37a; and**

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

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.

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 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.**

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 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*