

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

### *CHAPTER XIII*

#### ***Right of access and review of alerts***

##### *Article 44*

#### **National competent authorities having a right to access data in SIS**

1 National competent authorities shall have access to data entered in SIS and the right to search such data directly or in a copy of the SIS database for the purposes of:

- a border control, in accordance with Regulation (EU) 2016/399;
- b police and customs checks carried out within the Member State concerned, and the coordination of such checks by designated authorities;
- c the prevention, detection, investigation or prosecution of terrorist offences or other serious criminal offences or the execution of criminal penalties, within the Member State concerned, provided that Directive (EU) 2016/680 applies;
- d examining the conditions and taking decisions related to the entry and stay of third-country nationals on the territory of the Member States, including on residence permits and long-stay visas, and to the return of third-country nationals, as well as carrying out checks on third country nationals who are illegally entering or staying on the territory of the Member States;
- e security checks on third-country nationals who apply for international protection, insofar as authorities performing the checks are not ‘determining authorities’ as defined in point (f) of Article 2 of Directive 2013/32/EU of the European Parliament and of the Council<sup>(1)</sup>, and, where relevant, providing advice in accordance with Council Regulation (EC) No 377/2004<sup>(2)</sup>.

2 The right to access data in SIS and the right to search such data directly may be exercised by national competent authorities responsible for naturalisation, as provided for in national law, for the purposes of examining an application for naturalisation.

3 The right to access data entered in SIS and the right to search such data directly may also be exercised by national judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to charging a person, in the performance of their tasks, as provided for in national law, and by their coordinating authorities.

4 The competent authorities referred to in this Article shall be included in the list referred to in Article 56(7).

---

*Status: Point in time view as at 28/11/2018.*

*Changes to legislation: There are outstanding changes not yet made to Regulation (EU) 2018/1862 of the European Parliament and of the Council. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details)*

---

## Article 45

### Vehicle registration services

1 The services in the Member States responsible for issuing registration certificates for vehicles, as referred to in Council Directive 1999/37/EC<sup>(3)</sup>, shall have access to data entered into SIS in accordance with points (a), (b), (c), (m) and (p) of Article 38(2) of this Regulation for the sole purpose of checking whether vehicles and accompanying vehicle registration certificates and number plates presented to them for registration have been stolen, misappropriated, lost, purport to be such a document but are false or are sought as evidence in criminal proceedings.

Access to the data by the services referred to in first subparagraph shall be governed by the national law and shall be limited to the specific competence of the services concerned.

2 Services referred to in paragraph 1 that are government services shall have the right to access the data in SIS directly.

3 Services referred to in paragraph 1 of this Article that are non-government services shall have access to data in SIS only through the intermediary of an authority referred to in Article 44. That authority shall have the right to access the data directly and to pass them on to the service concerned. The Member State concerned shall ensure that the service in question and its employees are required to respect any limitations on the permissible use of data conveyed to them by the authority.

4 Article 39 shall not apply to access to SIS gained in accordance with this Article. The communication to the police or judicial authorities by services referred to in paragraph 1 of this Article of any information obtained through access to SIS shall be governed by national law.

## Article 46

### Registration services for boats and aircraft

1 The services in the Member States responsible for issuing registration certificates or ensuring traffic management for boats, including boat engines, and aircraft, including aircraft engines, shall have access to the following data entered into SIS in accordance with Article 38(2), for the sole purpose of checking whether boats, including boat engines, and aircraft, including aircraft engines, presented to them for registration or subject to traffic management have been stolen, misappropriated, lost or are sought as evidence in criminal proceedings:

- a data on boats;
- b data on boat engines;
- c data on aircraft;
- d data on aircraft engines.

Access to the data by the services referred to in first subparagraph shall be governed by the national law and shall be limited to the specific competence of the services concerned.

2 Services referred to in paragraph 1 that are government services shall have the right to access the data in SIS directly.

---

*Status: Point in time view as at 28/11/2018.*

*Changes to legislation: There are outstanding changes not yet made to Regulation (EU) 2018/1862 of the European Parliament and of the Council. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details)*

---

3 Services referred to in paragraph 1 of this Article that are non-government services shall have access to data in SIS only through the intermediary of an authority referred to in Article 44. That authority shall have the right to access the data directly and to pass them on to the service concerned. The Member State concerned shall ensure that the service in question and its employees are required to respect any limitations on the permissible use of data conveyed to them by the authority.

4 Article 39 shall not apply to access to SIS gained in accordance with this Article. The communication to the police or judicial authorities by services referred to in paragraph 1 of this Article of any information obtained through access to SIS shall be governed by national law.

#### *Article 47*

### **Registration services for firearms**

1 The services in the Member States responsible for issuing registration certificates for firearms shall have access to data on persons entered into SIS in accordance with Articles 26 and 36 and to data on firearms entered into SIS in accordance with Article 38(2). The access shall be exercised for the purpose of checking whether the person requesting registration is wanted for arrest for surrender or extradition purposes or for the purposes of discreet, inquiry or specific checks or whether firearms presented for registration are sought for seizure or for use as evidence in criminal proceedings.

2 Access to the data by the services referred to in paragraph 1 shall be governed by the national law and shall be limited to the specific competence of the services concerned.

3 Services referred to in paragraph 1 that are government services shall have the right to access the data in SIS directly.

4 Services referred to in paragraph 1 that are non-government services shall only have access to data in SIS through the intermediary of an authority referred to in Article 44. That authority shall have the right to access the data directly and shall inform the service concerned if the firearm can be registered. The Member State concerned shall ensure that the service in question and its employees are required to respect any limitations to the permissible use of data conveyed to them by the intermediating authority.

5 Article 39 shall not apply to access to SIS gained in accordance with this Article. The communication to the police or the judicial authorities by services referred to in paragraph 1 of this Article of any information obtained through access to SIS shall be governed by national law.

#### *Article 48*

### **Access to data in SIS by Europol**

1 The European Union Agency for Law Enforcement Cooperation (Europol), established by Regulation (EU) 2016/794, 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

---

*Status: Point in time view as at 28/11/2018.*

*Changes to legislation: There are outstanding changes not yet made to Regulation (EU) 2018/1862 of the European Parliament and of the Council. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details)*

---

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. 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 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.

---

*Status: Point in time view as at 28/11/2018.*

*Changes to legislation: There are outstanding changes not yet made to Regulation (EU) 2018/1862 of the European Parliament and of the Council. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details)*

---

8 Member States shall inform Europol through the exchange of supplementary information of any hit on alerts related to terrorist offences. Member States may exceptionally not inform Europol 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 49*

### **Access to data in SIS by Eurojust**

1 Only the national members of Eurojust and their assistants shall, where necessary to fulfil their mandate, have the right to access and search data in SIS within their mandate, in accordance with Articles 26, 32, 34, 38 and 40.

2 Where a search by a national member of Eurojust reveals the existence of an alert in SIS, that national member shall inform the issuing Member State. Eurojust shall only communicate information obtained from such a search to third countries and third bodies with the consent of the issuing Member State and in full compliance with Union law on data protection.

3 This Article is without prejudice to the provisions of Regulation (EU) 2018/1727 of the European Parliament and of the Council<sup>(4)</sup> and Regulation (EU) 2018/1725 concerning data protection and the liability for any unauthorised or incorrect processing of such data by national members of Eurojust or their assistants, and to the powers of the European Data Protection Supervisor pursuant to those Regulations.

4 For the purpose of verifying the lawfulness of data processing, self-monitoring and ensuring proper data security and integrity, Eurojust shall keep logs of every access to and search in SIS made by a national member of Eurojust or an assistant in accordance with the provisions of Article 12.

5 No parts of SIS shall be connected to any system for data collection and processing operated by or at Eurojust nor, shall the data in SIS to which the national members or their assistants have access be transferred to such a system. No part of SIS shall be downloaded or copied. The logging of access and searches shall not be considered to be unlawful downloading or copying of SIS data.

6 Eurojust shall adopt and apply measures to ensure security, confidentiality and self-monitoring in accordance with Articles 10, 11 and 13.

#### *Article 50*

### **Access to data in SIS by the European Border and Coast Guard teams, teams of staff involved in return-related tasks, and members of the migration management support teams**

1 In accordance with Article 40(8) of Regulation (EU) 2016/1624, the members of the teams referred to in points (8) and (9) of Article 2 of that Regulation shall, within their mandate and provided that they are authorised to carry out checks in accordance with Article 44(1) of this Regulation and have received the required training in accordance with Article 14(1) of this Regulation, have the right to access and search data in SIS insofar it is necessary for the

---

*Status: Point in time view as at 28/11/2018.*

*Changes to legislation: There are outstanding changes not yet made to Regulation (EU) 2018/1862 of the European Parliament and of the Council. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details)*

---

performance of their task and as required by the operational plan for a specific operation. Access to data in SIS shall not be extended to any other team members.

2 Members of the teams referred to in paragraph 1 shall exercise the right to access and search data in SIS in accordance with paragraph 1 through a technical interface. The technical interface shall be set up and maintained by the European Border and Coast Guard Agency and shall allow direct connection to Central SIS.

3 Where a search by a member of the teams referred to in paragraph 1 of this Article reveals the existence of an alert in SIS, the issuing Member State shall be informed thereof. In accordance with Article 40 of Regulation (EU) 2016/1624, members of the teams shall only act in response to an alert in SIS under instructions from and, as a general rule, in the presence of border guards or staff involved in return-related tasks of the host Member State in which they are operating. The host Member State may authorise members of the teams to act on its behalf.

4 For the purpose of verifying the lawfulness of data processing, self-monitoring and ensuring proper data security and integrity, the European Border and Coast Guard Agency shall keep logs of every access to and search in SIS in accordance with the provisions of Article 12.

5 The European Border and Coast Guard Agency shall adopt and apply measures to ensure security, confidentiality and self-monitoring in accordance with Articles 10, 11 and 13 and shall ensure that the teams referred to in paragraph 1 of this Article apply those measures.

6 Nothing in this Article shall be interpreted as affecting the provisions of Regulation (EU) 2016/1624 concerning data protection or the European Border and Coast Guard Agency's liability for any unauthorised or incorrect processing of data by it.

7 Without prejudice to paragraph 2, no parts of SIS shall be connected to any system for data collection and processing operated by the teams referred to in paragraph 1 or by the European Border and Coast Guard Agency, nor shall the data in SIS to which those teams have access be transferred to such a system. No part of SIS shall be downloaded or copied. The logging of access and searches shall not be considered to be unlawful downloading or copying of SIS data.

8 The European Border and Coast Guard Agency shall allow the European Data Protection Supervisor to monitor and review the activities of the teams referred to in this Article in the exercise of their right to access and search data in SIS. This shall be without prejudice to the further provisions of Regulation (EU) 2018/1725.

#### *Article 51*

### **Evaluation of the use of SIS by Europol, Eurojust and the European Border and Coast Guard Agency**

1 The Commission shall carry out an evaluation of the operation and the use of SIS by Europol, the national members of Eurojust and their assistants and the teams referred to in Article 50(1) at least every five years.

2 Europol, Eurojust and the European Border and Coast Guard Agency shall ensure adequate follow-up to the findings and recommendations stemming from the evaluation.

3 A report on the results of the evaluation and follow-up to it shall be sent to the European Parliament and to the Council.

---

*Status: Point in time view as at 28/11/2018.*

*Changes to legislation: There are outstanding changes not yet made to Regulation (EU) 2018/1862 of the European Parliament and of the Council. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details)*

---

## Article 52

### Scope of access

End-users, including Europol, the national members of Eurojust and their assistants and the members of the teams referred to in points (8) and (9) of Article 2 of Regulation (EU) 2016/1624, shall only access data which they require for the performance of their tasks.

## 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 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, 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 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 has expired, except where the issuing Member State has informed CS-SIS of an extension pursuant to paragraph 6. 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.

9 As soon as it becomes clear to a SIRENE Bureau that an alert on a person has achieved its purpose and should therefore be deleted, it shall immediately notify the authority which created the alert. The authority shall have 15 calendar days from the receipt of that notification to reply that the alert has been or shall be deleted or shall state reasons for the retention of the alert. If no reply has been received by the end of the 15-day period, the SIRENE Bureau shall ensure that the alert is deleted. Where permissible under national law, the alert shall be deleted

---

*Status: Point in time view as at 28/11/2018.*

*Changes to legislation: There are outstanding changes not yet made to Regulation (EU) 2018/1862 of the European Parliament and of the Council. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details)*

---

by the SIRENE Bureau. SIRENE Bureaux shall report any recurring issues they encounter when acting under this paragraph to their supervisory authority.

#### *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 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.



---

**Status:** Point in time view as at 28/11/2018.

**Changes to legislation:** There are outstanding changes not yet made to Regulation (EU) 2018/1862 of the European Parliament and of the Council. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details)

---

- (1) Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection ([OJ L 180, 29.6.2013, p. 60](#)).
- (2) Council Regulation (EC) No 377/2004 of 19 February 2004 on the creation of an immigration liaison officers network ([OJ L 64, 2.3.2004, p. 1](#)).
- (3) Council Directive 1999/37/EC of 29 April 1999 on the registration documents for vehicles ([OJ L 138, 1.6.1999, p. 57](#)).
- (4) Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA ([OJ L 295, 21.11.2018, p. 138](#)).

**Status:**

Point in time view as at 28/11/2018.

**Changes to legislation:**

There are outstanding changes not yet made to Regulation (EU) 2018/1862 of the European Parliament and of the Council. Any changes that have already been made to the legislation appear in the content and are referenced with annotations.