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 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, 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, 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.

Article 57

SIS data and national files

1 Article 56(2) shall be without prejudice to the right of a Member State to keep in its national files SIS data in connection with which action has been taken on its territory. Such data shall be kept in national files for a maximum period of three years, except if specific provisions in national law provide for a longer retention period.

2 Article 56(2) shall be without prejudice to the right of a Member State to keep in its national files data contained in a particular alert entered in SIS by that Member State.

Article 58

Information in the case of non-execution of an alert

If a requested action cannot be performed, the Member State from which action is requested shall immediately inform the issuing Member State through the exchange of supplementary information.

Article 59

Quality of the data in SIS

1 An issuing Member State shall be responsible for ensuring that the data are accurate, up-to-date, and entered and stored in SIS lawfully.

2 Where an issuing Member State receives relevant additional or modified data as listed in Article 20(3), it shall complete or modify the alert without delay.

3 Only the issuing Member State shall be authorised to modify, add to, correct, update or delete data which it has entered into SIS.

4 Where a Member State other than the issuing Member State has relevant additional or modified data as listed in Article 20(3), 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. If the additional or modified data relate to persons they shall only be transmitted if the identity of the person is ascertained.

5 Where a Member State other than the issuing Member State has evidence suggesting that an item of data is factually incorrect or has 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 item in question without delay.

6 Where the Member States are unable to reach an agreement within two months of the time when evidence first came to light as referred to in paragraph 5 of this Article, the Member State which did not enter the alert shall submit the matter to the supervisory

authorities concerned and to the European Data Protection Supervisor for a decision, by means of cooperation in accordance with Article 71.

7 The Member States shall exchange supplementary information in cases where a person complains that he or she is not the intended subject of an alert. Where the outcome of the check shows that the intended subject of an alert is not the complainant, the complainant shall be informed of the measures laid down in Article 62 and of the right to redress under Article 68(1).

Article 60

Security incidents

1 Any event that has or may have an impact on the security of SIS or may cause damage or loss to SIS data or to the supplementary information shall be considered to be a security incident, especially where unlawful access to data may have occurred or where the availability, integrity and confidentiality of data has or may have been compromised.

2 Security incidents shall be managed in a way as to ensure a quick, effective and proper response.

3 Without prejudice to the notification and communication of a personal data breach pursuant to Article 33 of Regulation (EU) 2016/679 or to Article 30 of Directive (EU) 2016/680, Member States, Europol, Eurojust and the European Border and Coast Guard Agency shall notify the Commission, eu-LISA, the competent supervisory authority and the European Data Protection Supervisor without delay of security incidents. eu-LISA shall notify the Commission and the European Data Protection Supervisor without delay of any security incident concerning Central SIS.

4 Information regarding a security incident that has or may have an impact on the operation of SIS in a Member State or within eu-LISA, on the availability, integrity and confidentiality of the data entered or sent by other Member States or on supplementary information exchanged, shall be provided to all Member States without delay and reported in compliance with the incident management plan provided by eu-LISA.

5 The Member States and eu-LISA shall collaborate in the event of a security incident.

6 The Commission shall report serious incidents immediately to the European Parliament and to the Council. Those reports shall be classified as EU RESTRICTED/ RESTREINT UE in accordance with applicable security rules.

7 Where a security incident is caused by the misuse of data, Member States, Europol, Eurojust and the European Border and Coast Guard Agency shall ensure that penalties are imposed in accordance with Article 73.

Article 61

Distinguishing between persons with similar characteristics

1 Where upon a new alert being entered it becomes apparent that there is already an alert in SIS on a person with the same description of identity, the SIRENE Bureau shall contact the issuing Member State through the exchange of supplementary information within 12 hours to cross-check whether the subjects of the two alerts are the same person.

2 Where the cross-check reveals that the subject of the new alert and the person subject to the alert already entered in SIS are indeed one and the same person, the SIRENE Bureau shall apply the procedure for entering multiple alerts referred to in Article 23.

3 Where the outcome of the cross-check is that there are in fact two different persons, the SIRENE Bureau shall approve the request for entering the second alert by adding the data necessary to avoid any misidentifications.

Article 62

Additional data for the purpose of dealing with misused identities

1 Where confusion may arise between the person intended to be the subject of an alert and a person whose identity has been misused, the issuing Member State shall, subject to the explicit consent of the person whose identity has been misused, add data relating to the latter to the alert in order to avoid the negative consequences of misidentification. Any person whose identity has been misused shall have the right to withdraw his or her consent regarding the processing of the added personal data.

2 Data relating to a person whose identity has been misused shall be used only for the following purposes:

a to allow the competent authority to distinguish the person whose identity has been misused from the person intended to be the subject of the alert; and

b to allow the person whose identity has been misused to prove his or her identity and to establish that his or her identity has been misused.

3 For the purpose of this Article, and subject to the explicit consent of the person whose identity has been misused for each data category, only the following personal data of the person whose identity has been misused may be entered and further processed in SIS:

a surnames;

b forenames;

c names at birth;

d previously used names and any aliases possibly entered separately;

e any specific objective and physical characteristic not subject to change;

f place of birth;

g date of birth;

h gender;

i photographs and facial images;

j fingerprints, palm prints or both;

k any nationalities held;

l the category of the person's identification documents;

m the country of issue of the person's identification documents;

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

o the date of issue of a person's identification documents;

p address of the person;

q person's father's name;

r person's mother's name.

4 The Commission shall adopt implementing acts to lay down and develop technical rules necessary for entering and further processing the data referred to in paragraph 3 of

this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 76(2).

5 The data referred to in paragraph 3 shall be deleted at the same time as the corresponding alert or earlier where the person so requests.

6 Only the authorities having a right of access to the corresponding alert may access the data referred to in paragraph 3. They may do so for the sole purpose of avoiding misidentification.

Article 63

Links between alerts

1 A Member State may create a link between alerts it enters in SIS. The effect of such a link shall be to establish a relationship between two or more alerts.

2 The creation of a link shall not affect the specific action to be taken on the basis of each linked alert or the review period of each of the linked alerts.

3 The creation of a link shall not affect the rights of access provided for in this Regulation. Authorities with no right of access to certain categories of alerts shall not be able to see the link to an alert to which they do not have access.

4 A Member State shall create a link between alerts when there is an operational need.

5 Where a Member State considers that the creation by another Member State of a link between alerts is incompatible with its national law or its international obligations, it may take the necessary measures to ensure that there can be no access to the link from its national territory or by its authorities located outside its territory.

6 The Commission shall adopt implementing acts to lay down and develop technical rules for linking alerts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 76(2).

Article 64

Purpose and retention period of supplementary information

1 Member States shall keep a reference to the decisions giving rise to an alert at the SIRENE Bureau in order to support the exchange of supplementary information.

2 Personal data held in files by the SIRENE Bureau as a result of information exchanged shall be kept only for such time as may be required to achieve the purposes for which they were supplied. They shall in any event be deleted at the latest one year after the related alert has been deleted from SIS.

3 Paragraph 2 shall be without prejudice to the right of a Member State to keep in national files data relating to a particular alert which that Member State has entered or to an alert in connection with which action has been taken on its territory. The period for which such data may be kept in those files shall be governed by national law.

Article 65

Transfer of personal data to third parties

Data processed in SIS and the related supplementary information exchanged pursuant to this Regulation shall not be transferred or made available to third countries or to international organisations.

Status:
Point in time view as at 31/12/2020.

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.