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 II

Responsibilities of the Member States

Article 6

National systems

Each Member State shall be responsible for setting up, operating, maintaining and further developing its N.SIS and connecting it to NI-SIS.

Each Member State shall be responsible for ensuring the uninterrupted availability of SIS data to end-users.

Each Member State shall transmit its alerts through its N.SIS.

Article 7

N.SIS Office and SIRENE Bureau

1 Each Member State shall designate an authority (the N.SIS Office), which shall have central responsibility for its N.SIS.

That authority shall be responsible for the smooth operation and security of the N.SIS, shall ensure the access of the competent authorities to SIS and shall take the necessary measures to ensure compliance with this Regulation. It shall be responsible for ensuring that all functionalities of SIS are made available to the end users appropriately.

2 Each Member State shall designate a national authority which shall be operational 24 hours a day, 7 days a week and which shall ensure the exchange and availability of all supplementary information (the SIRENE Bureau) in accordance with the SIRENE Manual. Each SIRENE Bureau shall serve as a single contact point for its Member State to exchange supplementary information regarding alerts and to facilitate the requested actions to be taken when alerts on persons or objects have been entered in SIS and those persons or objects are located following a hit.

Each SIRENE Bureau shall, in accordance with national law, have easy direct or indirect access to all relevant national information, including national databases and all information on its Member States' alerts, and to expert advice, in order to be able to react to requests for supplementary information swiftly and within the deadlines provided for in Article 8.

The SIRENE Bureaux shall coordinate the verification of the quality of the information entered in SIS. For those purposes they shall have access to data processed in SIS.

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) View outstanding changes*

[F1 2a The SIRENE Bureaux shall also ensure the manual verification of different identities in accordance with Article 29 of Regulation (EU) 2019/818. To the extent necessary to carry out this task, the SIRENE Bureaux shall have access to the data stored in the CIR and the MID for the purposes laid down in Articles 21 and 26 of Regulation (EU) 2019/818.**]**

3 The Member States shall provide eu-LISA with details of their N.SIS Office and of their SIRENE Bureau. eu-LISA shall publish the list of the N.SIS Offices and the SIRENE Bureaux together with the list referred to in Article 56(7).

Textual Amendments

F1 Inserted by Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816.

Article 8

Exchange of supplementary information

1 Supplementary information shall be exchanged in accordance with the provisions of the SIRENE Manual and using the Communication Infrastructure. Member States shall provide the necessary technical and human resources to ensure the continuous availability and timely and effective exchange of supplementary information. In the event that the Communication Infrastructure is unavailable, Member States shall use other adequately secured technical means to exchange supplementary information. A list of adequately secured technical means shall be laid down in the SIRENE Manual.

2 Supplementary information shall be used only for the purpose for which it was transmitted in accordance with Article 64 unless prior consent for another use is obtained from the issuing Member State.

3 The SIRENE Bureaux shall carry out their tasks in a quick and efficient manner, in particular by replying to a request for supplementary information as soon as possible but not later than 12 hours after the receipt of the request. In case of alerts for terrorist offences, of alerts on persons wanted for arrest for surrender or extradition purposes, and in cases of alerts on children referred to in point (c) of Article 32(1) the SIRENE Bureaux shall act immediately.

Requests for supplementary information with the highest priority shall be marked ‘URGENT’ in the SIRENE forms, and the reason for the urgency shall be specified.

4 The Commission shall adopt implementing acts to lay down detailed rules for the tasks of the SIRENE Bureaux pursuant to this Regulation and the exchange of supplementary information in the form of a manual entitled the ‘SIRENE Manual’. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 76(2).

Article 9

Technical and functional compliance

1 When setting up its N.SIS, each Member State shall comply with common standards, protocols and technical procedures established to ensure the compatibility of its N.-SIS with Central SIS for the prompt and effective transmission of data.

***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) View outstanding changes*

2 If a Member State uses a national copy, it shall ensure, by means of the services provided by CS-SIS and by means of automatic updates referred to in Article 4(6), that the data stored in the national copy are identical to and consistent with the SIS database and that a search in its national copy produces a result equivalent to that of a search in the SIS database.

3 End-users shall receive the data required to perform their tasks, in particular, and where necessary, all the available data allowing for the identification of the data subject and for the requested action to be taken.

4 Member States and eu-LISA shall undertake regular tests to verify the technical compliance of the national copies referred to in paragraph 2. The results of those tests shall be taken into consideration as part of the mechanism established by Council Regulation (EU) No 1053/2013[(1)].

5 The Commission shall adopt implementing acts to lay down and develop common standards, protocols and technical procedures, referred to in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 76(2).

Article 10

Security — Member States

1 Each Member State shall, in relation to its N.SIS, adopt the necessary measures, including a security plan, a business continuity plan and a disaster recovery plan, in order to:

a physically protect data, including by making contingency plans for the protection of critical infrastructure;

b deny unauthorised persons access to data-processing facilities used for processing personal data (facilities access control);

c prevent the unauthorised reading, copying, modification or removal of data media (data media control);

d prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);

e prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);

f prevent the unauthorised processing of data in SIS and any unauthorised modification or erasure of data processed in SIS (control of data entry);

g ensure that persons authorised to use an automated data-processing system have access only to the data covered by their access authorisation, by means of individual and unique user identifiers and confidential access modes only (data access control);

h ensure that all authorities with a right of access to SIS or to the data processing facilities create profiles describing the functions and responsibilities of persons who are authorised to access, enter, update, delete and search the data and make those profiles available to the supervisory authorities referred to in Article 69(1) without delay upon their request (personnel profiles);

i ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);

j ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems, when, by whom and for what purpose (input control);

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) View outstanding changes*

k prevent the unauthorised reading, copying, modification or deletion of personal data during the transmission of personal data or during the transport of data media, in particular by means of appropriate encryption techniques (transport control);

l monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Regulation (self-auditing);

m ensure that, in the event of interruption, installed systems can be restored to normal operation (recovery); and

n ensure that SIS performs its functions correctly, that faults are reported (reliability) and that personal data stored in SIS cannot be corrupted by means of the system malfunctioning (integrity).

2 Member States shall take measures equivalent to those referred to in paragraph 1 as regards security in respect of the processing and exchange of supplementary information, including by securing the premises of the SIRENE Bureaux.

3 Member States shall take measures equivalent to those referred to in paragraph 1 of this Article as regards security in respect of the processing of SIS data by the authorities referred to in Article 44.

4 The measures described in paragraphs 1, 2 and 3 may be part of a generic security approach and plan at national level encompassing multiple IT systems. In such cases, the requirements set out in this Article and their applicability to SIS shall be clearly identifiable in and ensured by that plan.

Article 11

Confidentiality — Member States

1 Each Member State shall apply its rules of professional secrecy or other equivalent duties of confidentiality to all persons and bodies required to work with SIS data and supplementary information, in accordance with its national law. That obligation shall also apply after those persons leave office or employment or after the termination of the activities of those bodies.

2 Where a Member State cooperates with external contractors in any SIS-related tasks, it shall closely monitor the activities of the contractor to ensure compliance with all provisions of this Regulation, in particular on security, confidentiality and data protection.

3 The operational management of N.SIS or of any technical copies shall not be entrusted to private companies or private organisations.

Article 12

Keeping of logs at national level

1 Member States shall ensure that every access to and all exchanges of personal data within CS-SIS are logged in their N.SIS for the purposes of checking whether the search was lawful, monitoring the lawfulness of data processing, self-monitoring, ensuring the proper functioning of N.SIS, as well as for data integrity and security. This requirement does not apply to the automatic processes referred to in points (a), (b) and (c) of Article 4(6).

***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) View outstanding changes*

[[F1]Member States shall ensure that every access to personal data via the ESP is also logged for the purposes of checking whether the search was lawful, monitoring the lawfulness of data processing, self-monitoring, and data integrity and security.**]**

2 The logs shall show, in particular, the history of the alert, the date and time of the data processing activity, the data used to perform a search, a reference to the data processed and the individual and unique user identifiers of both the competent authority and the person processing the data.

3 By way of derogation from paragraph 2 of this Article, if the search is carried out with dactyloscopic data or a facial image in accordance with Article 43, the logs shall show the type of data used to perform the search instead of the actual data.

4 The logs shall only be used for the purpose referred to in paragraph 1 and shall be deleted three years after their creation. The logs which include the history of alerts shall be deleted three years after deletion of the alerts.

5 Logs may be kept for longer than the periods referred to in paragraph 4 if they are required for monitoring procedures that are already underway.

6 The national competent authorities in charge of checking whether searches are lawful, monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of N.SIS and data integrity and security, shall have access, within the limits of their competence and at their request, to the logs for the purpose of fulfilling their duties.

7 Where Member States, in accordance with national law, carry out automated scanned searches of the number plates of motor vehicles, using Automatic Number Plate Recognition systems, Member States shall maintain a log of the search in accordance with national law. If necessary, a full search may be carried out in SIS in order to verify whether a hit has been achieved. Paragraphs 1 to 6 shall apply to any full search.

8 The Commission shall adopt implementing acts to establish the content of the log, 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).

Textual Amendments

F1 Inserted by Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816.

Article 13

Self-monitoring

Member States shall ensure that each authority entitled to access SIS data takes the measures necessary to comply with this Regulation and cooperates, where necessary, with the supervisory authority.

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) View outstanding changes*

Article 14

Staff training

1 Before being authorised to process data stored in SIS and periodically after access to SIS data has been granted, the staff of the authorities having a right to access SIS shall receive appropriate training on data security, on fundamental rights including data -protection, and on the rules and procedures for data processing set out in the SIRENE Manual. The staff shall be informed of any relevant provisions on criminal offences and penalties, including those provided for in Article 73.

2 Member States shall have a national SIS training programme which shall include training for end-users as well as the staff of the SIRENE Bureaux.

That training programme may be part of a general training programme at national level encompassing training in other relevant areas.

3 Common training courses shall be organised at Union level at least once a year to enhance cooperation between SIRENE Bureaux.

***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) View outstanding changes*

(**1**) Council Regulation (EU) No 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen *acquis* and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen (OJ L 295, 6.11.2013, p. 27).

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.
View outstanding changes

Changes and effects yet to be applied to :

– Regulation revoked in part by S.I. 2019/742, reg. 119(2)(h) (as inserted) by S.I. 2020/1408 reg. 35(b)