►B REGULATION (EU) 2018/1861 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 border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006

(OJ L 312, 7.12.2018, p. 14)

Amended by:

		Official Journal		
		No	page	date
►M1	Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019	L 135	27	22.5.2019

Corrected by:

►C1 Corrigendum, OJ L 288, 3.9.2020, p. 29 (2018/1861)

▼B

REGULATION (EU) 2018/1861 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 border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006

CHAPTER I

GENERAL PROVISIONS

Article 1

General purpose of SIS

The purpose of SIS shall be to ensure a high level of security within the area of freedom, security and justice of the Union, including the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States, and to ensure the application of the provisions of Chapter 2 of Title V of Part Three TFEU relating to the movement of persons on their territories, using information communicated through this system.

Article 2

Subject matter

1. This Regulation establishes the conditions and procedures for the entry and processing of alerts in SIS on third-country nationals and for the exchange of supplementary information and additional data for the purpose of refusing entry into and stay on the territory of the Member States.

2. This Regulation also lays down provisions on the technical architecture of SIS, on the responsibilities of the Member States and of the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), on data processing, on the rights of the persons concerned and on liability.

Article 3

Definitions

For the purposes of this Regulation, the following definitions apply:

(1) ‘alert’ means a set of data entered into SIS allowing the competent authorities to identify a person with a view to taking specific action;

(2) ‘supplementary information’ means information not forming part of the alert data stored in SIS, but connected to alerts in SIS, which is to be exchanged through the SIRENE Bureaux:

(a) in order to allow Member States to consult or inform each other when entering an alert;

(b) following a hit in order to allow the appropriate action to be taken;

▼B

(c) when the required action cannot be taken;

(d) when dealing with the quality of SIS data;

(e) when dealing with the compatibility and priority of alerts;

(f) when dealing with rights of access;

(3) ‘additional data’ means the data stored in SIS and connected with alerts in SIS which are to be immediately available to the competent authorities where a person in respect of whom data has been entered in SIS is located as a result of conducting a search in SIS;

(4) ‘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 rights of free movement equivalent to those of citizens of the Union under agreements between the Union, or the Union and its Member States on the one hand, and third countries on the other hand;

(5) ‘personal data’ means personal data as defined in point 1 of Article 4 of Regulation (EU) 2016/679;

(6) ‘processing of personal data’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, logging, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(7) a ‘match’ means the occurrence of the following steps:

(a) a search has been conducted in SIS by an end-user;

(b) that search has revealed an alert entered into SIS by another Member State; and

(c) data concerning the alert in SIS match the search data;

(8) a ‘hit’ means any match which fulfils the following criteria:

(a) it has been confirmed by:

(i) the end-user; or

(ii) the competent authority in accordance with national procedures, where the match concerned was based on the comparison of biometric data;

and

(b) further actions are requested;

(9) ‘issuing Member State’ means the Member State which entered the alert into SIS;

(10) ‘granting Member State’ means the Member State which is considering granting or extending or which has granted or extended a residence permit or long-stay visa and which is involved in the consultation procedure with another Member State;

▼B

(11) ‘executing Member State’ means the Member State which takes or has taken the required actions following a hit;

(12) ‘end-user’ means a member of staff of a competent authority authorised to search directly CS-SIS, N.SIS or a technical copy thereof;

(13) ‘biometric data’ means personal data resulting from specific technical processing relating to the physical or physiological characteristics of a natural person, which allow or confirm the unique identification of that natural person, namely photographs, facial images and dactyloscopic data;

(14) ‘dactyloscopic data’ means data on fingerprints and palm prints which due to their unique character and the reference points contained therein enable accurate and conclusive comparisons on a person's identity;

(15) ‘facial image’ means digital images of the face with sufficient image resolution and quality to be used in automated biometric matching;

(16) ‘return’ means return as defined in point 3 of Article 3 of Directive 2008/115/EC;

(17) ‘entry ban’ means an entry ban as defined in point 6 of Article 3 of Directive 2008/115/EC;

(18) ‘terrorist offences’ means offences under national law referred to in Articles 3 to 14 of Directive (EU) 2017/541 of the European Parliament and of the Council [1], or equivalent to one of those offences for the Member States which are not bound by that Directive;

(19) ‘residence permit’ means a residence permit as defined in point (16) of Article 2 of Regulation (EU) 2016/399 of the European Parliament and of the Council [2];

(20) ‘long-stay visa’ means a long-stay visa as referred to in Article 18(1) of Convention implementing the Schengen Agreement;

(21) ‘threat to public health’ means a threat to public health as defined in point (21) of Article 2 of Regulation (EU) 2016/399;

▼M1

(22) ‘ESP’ means the European search portal established by Article 6(1) of Regulation (EU) 2019/817 of the European Parliament and of the Council [3];

---

[1] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, p. 6).

[2] Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ L 77, 23.3.2016, p. 1).

[3] Regulation (EU) 2019/817 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 borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27).

▼M1

(23) ‘shared BMS’ means the shared biometric matching service established by Article 12(1) of Regulation (EU) 2019/817;

(24) ‘CIR’ means the common identity repository established by Article 17(1) of Regulation (EU) 2019/817;

(25) ‘MID’ means the multiple-identity detector established by Article 25(1) of Regulation (EU) 2019/817.

▼B

Article 4

Technical architecture and ways of operating SIS

1. SIS shall be composed of:

(a) a central system (Central SIS) composed of:

(i) a technical support function (‘CS-SIS’) containing a database, (the ‘SIS database’), and including a backup CS-SIS,

(ii) a uniform national interface (‘NI-SIS’);

▼M1

(b) a national system (N.SIS) in each of the Member States, consisting of the national data systems which communicate with Central SIS, including at least one national or shared backup N.SIS;

(c) a communication infrastructure between CS-SIS, backup CS-SIS and NI-SIS (‘the Communication Infrastructure’) that provides an encrypted virtual network dedicated to SIS data and the exchange of data between SIRENE Bureaux, as referred to in Article 7(2); and

(d) a secure communication infrastructure between CS-SIS and the central infrastructures of the ESP, the shared BMS and the MID.

▼B

An N.SIS as referred to in point (b) may contain a data file (a ‘national copy’) containing a complete or partial copy of the SIS database. Two or more Member States may establish in one of their N.SIS a shared copy which may be used jointly by those Member States. Such shared copy shall be considered as the national copy of each of those Member States.

A shared backup N.SIS as referred to in point (b) may be used jointly by two or more Member States. In such cases, the shared backup N.SIS shall be considered as the backup N.SIS of each of those Member States. The N.SIS and its backup may be used simultaneously to ensure uninterrupted availability to end-users.

Member States intending to establish a shared copy or shared backup N.SIS to be used jointly shall agree their respective responsibilities in writing. They shall notify their arrangement to the Commission.

The Communication Infrastructure shall support and contribute to ensuring the uninterrupted availability of SIS. It shall include redundant and separated paths for the connections between CS-SIS and the backup CS-SIS and shall also include redundant and separated paths for the connections between each SIS national network access point and CS-SIS and backup CS-SIS.

▼B

2. Member States shall enter, update, delete and search SIS data through their own N.SIS. The Member States using a partial or a complete national copy or a partial or complete shared copy shall make that copy available for the purpose of carrying out automated searches in the territory of each of those Member States. The partial national or shared copy shall contain at least the data listed in points (a) to (v) of Article 20(2). It shall not be possible to search the data files of other Member States' N.SIS, except in the case of shared copies.

3. CS-SIS shall perform technical supervision and administration functions and have a backup CS-SIS, capable of ensuring all functionalities of the principal CS-SIS in the event of failure of that system. CS-SIS and the backup CS-SIS shall be located in the two technical sites of eu-LISA.

4. eu-LISA shall implement technical solutions to reinforce the uninterrupted availability of SIS either through the simultaneous operation of CS-SIS and the backup CS-SIS, provided that the backup CS-SIS remains capable of ensuring the operation of SIS in the event of a failure of CS-SIS, or through duplication of the system or its components. Notwithstanding the procedural requirements laid down in Article 10 of Regulation (EU) 2018/1726 eu-LISA shall, no later than 28 December 2019, prepare a study on the options for technical solutions, containing an independent impact assessment and cost-benefit analysis.

5. Where necessary in exceptional circumstances, eu-LISA may temporarily develop an additional copy of the SIS database.

6. CS-SIS shall provide the services necessary for the entry and processing of SIS data, including searches in the SIS database. For the Member States which use a national or shared copy, CS-SIS shall:

(a) provide online updates for the national copies;

(b) ensure synchronisation of and consistency between the national copies and the SIS database; and

(c) provide the operation for initialisation and restoration of the national copies.

7. CS-SIS shall provide uninterrupted availability.

▼M1

8. Without prejudice to paragraphs 1 to 5, SIS data may also be searched via the ESP.

9. Without prejudice to paragraphs 1 to 5, SIS data may also be transmitted via the secure communication infrastructure referred to in point (d) of paragraph 1. These transmissions shall be limited to the extent that the data are required for the purposes of Regulation (EU) 2019/817.

▼B

Article 5

Costs

1. The costs of operating, maintaining and further developing Central SIS and the Communication Infrastructure shall be borne by the general budget of the Union. Those costs shall include work done with respect to CS-SIS, in order to ensure the provision of the services referred to in Article 4(6).

2. Funding is allocated from the envelope of EUR 791 million foreseen under point (b) Article 5(5) of Regulation (EU) No 515/2014 to cover the costs of implementation of this Regulation.

3. From the envelope referred to in paragraph 2, and without prejudice to further funding for this purpose from other sources of the general budget of the Union, an amount of EUR 31 098 000 is allocated to eu-LISA. Such funding shall be implemented under indirect management and shall contribute to carrying out the technical developments required under this Regulation concerning Central SIS and the Communication Infrastructure, as well as related training activities.

4. From the envelope referred to in paragraph 2, the Member States participating in Regulation (EU) No 515/2014 shall receive an additional global allocation of EUR 36 810 000 to be distributed in equal shares through a lump sum to their basic allocation. Such funding shall be implemented under shared management and shall be entirely devoted to the quick and effective upgrade of the national systems concerned in line with the requirements of this Regulation.

5. The costs of setting up, operating, maintaining and further developing each N.SIS shall be borne by the Member State concerned.

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.

▼B

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 have been entered in SIS and those persons 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.

▼M1

2a. The SIRENE Bureaux shall also ensure the manual verification of different identities in accordance with Article 29 Regulation (EU) 2019/817. 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) 2019/817.

▼B

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 41(8).

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 49 unless prior consent for another use is obtained from the issuing Member State.

▼B

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.

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 62(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.

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 62(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:

([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).

▼B

(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 55(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);

(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);

▼B

(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 34.

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

▼M1

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).

▼M1

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.

▼B

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 33, 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.

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.

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 59.

▼B

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.

CHAPTER III

RESPONSIBILITIES OF eu-LISA

Article 15

Operational management

1. eu-LISA shall be responsible for the operational management of Central SIS. eu-LISA shall, in cooperation with the Member States, ensure that at all times the best available technology is used for Central SIS, subject to a cost-benefit analysis.

2. eu-LISA shall also be responsible for the following tasks relating to the Communication Infrastructure:

(a) supervision;

(b) security;

(c) the coordination of relations between the Member States and the provider;

(d) tasks relating to implementation of the budget;

(e) acquisition and renewal; and

(f) contractual matters.

3. eu-LISA shall also be responsible for the following tasks relating to the SIRENE Bureaux and communication between the SIRENE Bureaux:

(a) the coordination, management and support of testing activities;

(b) the maintenance and updating of technical specifications for the exchange of supplementary information between SIRENE Bureaux and the Communication Infrastructure; and

(c) managing the impact of technical changes where it affects both SIS and the exchange of supplementary information between SIRENE Bureaux.

▼B

4. eu-LISA shall develop and maintain a mechanism and procedures for carrying out quality checks on the data in CS-SIS. It shall provide regular reports to the Member States in this regard.

eu-LISA shall provide a regular report to the Commission covering the issues encountered and the Member States concerned.

The Commission shall provide the European Parliament and the Council with a regular report on data quality issues that are encountered.

5. eu-LISA shall also perform tasks related to providing training on the technical use of SIS and on measures for improving the quality of SIS data.

6. The operational management of Central SIS shall consist of all the tasks necessary to keep Central SIS functioning 24 hours a day, 7 days a week in accordance with this Regulation, in particular the maintenance work and technical developments necessary for the smooth running of the system. Those tasks shall also include the coordination, management and support of testing activities for Central SIS and the N.SIS that ensure that Central SIS and the N.SIS operate in accordance with the requirements for technical and functional compliance set out in Article 9.

7. The Commission shall adopt implementing acts to set out the technical requirements for the Communication Infrastructure. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).

Article 16

Security – eu-LISA

1. eu-LISA shall adopt the necessary measures, including a security plan, a business continuity plan and a disaster recovery plan for Central SIS and the Communication Infrastructure 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);

▼B

(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) create profiles describing the functions and responsibilities of persons who are authorised to access the data or the data processing facilities and make those profiles available to the European Data Protection Supervisor without delay upon its 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 and by whom (input control);

(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 interrupted operations, installed systems can be restored to normal operation (recovery);

(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); and

(o) ensure the security of its technical sites.

2. eu-LISA shall take measures equivalent to those referred to in paragraph 1 as regards security in respect of the processing and exchange of supplementary information through the Communication Infrastructure.

Article 17

Confidentiality – eu-LISA

1. Without prejudice to Article 17 of the Staff Regulations eu-LISA shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality of a comparable standard to those laid down in Article 11 of this Regulation to all its staff required to work with SIS data. That obligation shall also apply after those persons leave office or employment or after the termination of their activities.

▼B

2. eu-LISA shall take measures equivalent to those referred to in paragraph 1 as regards confidentiality in respect of the exchange of supplementary information through the Communication Infrastructure.

3. Where eu-LISA 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.

4. The operational management of CS-SIS shall not be entrusted to private companies or private organisations.

Article 18

Keeping of logs at central level

1. eu-LISA shall ensure that every access to and all exchanges of personal data within CS-SIS are logged for the purposes stated in Article 12(1).

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 the competent authority processing the data.

3. By way of derogation from paragraph 2 of this Article, if the search is carried out with dactyloscopic data or facial images in accordance with Article 33, 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 purposes 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 longer than the periods referred to in paragraph 4 if they are required for monitoring procedures that are already underway.

6. For the purposes of self-monitoring and ensuring the proper functioning of CS-SIS, data integrity and security, eu-LISA shall have access to the logs within the limits of its competence.

The European Data Protection Supervisor shall have access to those logs on request, within the limits of its competence and for the purpose of fulfilling its tasks.

▼B

CHAPTER IV

INFORMATION TO THE PUBLIC

Article 19

SIS information campaigns

At the start of the application of this Regulation, the Commission, in cooperation with the supervisory authorities and the European Data Protection Supervisor, shall carry out a campaign informing the public about the objectives of SIS, the data stored in SIS, the authorities having access to SIS and the rights of data subjects. The Commission shall repeat such campaigns regularly, in cooperation with the supervisory authorities and the European Data Protection Supervisor. The Commission shall maintain a website available to the public providing all relevant information concerning SIS. Member States shall, in cooperation with their supervisory authorities, devise and implement the necessary policies to inform their citizens and residents about SIS generally.

CHAPTER V

ALERTS FOR REFUSAL OF ENTRY AND STAY ON THIRD-COUNTRY NATIONALS

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 24 and 25.

2. 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;

▼B

(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 48;

(p) whether the person concerned is a family member of a citizen of the Union or other person who is a beneficiary of the right of free movement as referred to in Article 26;

(q) whether the decision for refusal of entry and stay is based on:

(i) a previous conviction as referred to in point (a) of Article 24(2);

(ii) a serious security threat as referred to in point (b) of Article 24(2);

(iii) circumvention of Union or national law on entry and stay as referred to in point (c) of Article 24(2);

(iv) an entry ban as referred to in point (b) of Article 24(1); or

(v) a restrictive measure referred to in Article 25;

(r) the type of offence;

(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;

▼B

(w) photographs and facial images;

(x) dactyloscopic data;

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

3. 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 paragraph 2 of this Article and the common standards referred to in paragraph 4 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).

4. Technical rules shall be similar for searches in CS-SIS, in national or shared copies and in technical copies made under Article 41(2). They shall be based on common standards.

Article 21

Proportionality

1. Before entering an alert and when extending the period of validity of an alert, Member States shall determine whether the case is adequate, relevant and important enough to warrant an alert in SIS.

2. Where the decision to refuse entry and stay referred to in point (a) of Article 24(1) is related to a terrorist offence, the case shall be considered adequate, relevant and important enough to warrant an alert in SIS. For public or national security reasons, Member States may exceptionally refrain from entering an alert when it is likely to obstruct official or legal inquiries, investigations or procedures.

Article 22

Requirement for an alert to be entered

1. The minimum set of data necessary in order to enter an alert into SIS shall be the data referred to in points (a), (g), (k), (m), (n) and (q) of Article 20(2). The other data referred to in that paragraph shall also be entered into SIS, if available.

2. The data referred to in point (e) of Article 20(2) of this Regulation shall only be entered when this is strictly necessary for the identification of the third-country national concerned. When such data are entered, Member States shall ensure that Article 9 of Regulation (EU) 2016/679 is complied with.

Article 23

Compatibility of alerts

1. Before entering an alert, the Member State shall check whether the person concerned is already the subject of an alert in SIS. For that purpose, a check with dactyloscopic data shall also be carried out if such data are available.

2. Only one alert per person per Member State shall be entered into SIS. Where necessary, new alerts may be entered on the same person by other Member States, in accordance with paragraph 3.

▼B

3. Where a person is already the subject of an alert in SIS, a Member State wishing to enter a new alert shall check that there is no incompatibility between the alerts. If there is no incompatibility, the Member State may enter the new alert. If the alerts are incompatible, the SIRENE Bureaux of the Member States concerned shall consult each other by exchanging supplementary information in order to reach an agreement. Rules on the compatibility of alerts shall be laid down in the SIRENE Manual. Departures from the compatibility rules may be made after consultation between the Member States if essential national interests are at stake.

4. In the case of hits on multiple alerts on the same person, the executing Member State shall observe the priority rules for alerts laid down in the SIRENE Manual.

If a person is subject to multiple alerts entered by different Member States, alerts for arrest entered in accordance with Article 26 of Regulation (EU) 2018/1862 shall be executed as a priority, subject to Article 25 of that Regulation.

Article 24

Conditions for entering alerts for refusal of entry and stay

1. Member States shall enter an alert for refusal of entry and stay when one of the following conditions is met:

(a) the Member State has concluded, based on an individual assessment which includes an assessment of the personal circumstances of the third-country national concerned and the consequences of refusing him or her entry and stay, that the presence of that third-country national on its territory poses a threat to public policy, to public security or to national security, and the Member State has consequently adopted a judicial or administrative decision in accordance with its national law to refuse entry and stay and issued a national alert for refusal of entry and stay; or

(b) the Member State has issued an entry ban in accordance with procedures respecting Directive 2008/115/EC in respect of a third-country national.

2. The situations covered by point (a) of paragraph 1 shall arise where:

(a) a third-country national has been convicted in a Member State of an offence carrying a penalty involving the deprivation of liberty of at least one year;

(b) there are serious grounds for believing that a third-country national has committed a serious criminal offence, including a terrorist offence, or there are clear indications of his or her intention to commit such an offence in the territory of a Member State; or

(c) a third-country national has circumvented or attempted to circumvent Union or national law on entry into and stay on the territory of the Member States.

▼B

3. The issuing Member State shall ensure that the alert takes effect in SIS as soon as the third-country national concerned has left the territory of the Member States or as soon as possible where the issuing Member State has obtained clear indications that the third-country national has left the territory of the Member States, in order to prevent the re-entry of that third-country national.

4. Persons in respect of whom a decision for refusal of entry and stay is taken as referred in paragraph 1 shall have the right to appeal. Such appeals shall be conducted in accordance with Union and national law, which shall provide for an effective remedy to be requested before a court.

Article 25

Conditions for entering alerts on third-country nationals subject to restrictive measures

1. Alerts on third-country nationals who are the subject of a restrictive measure intended to prevent entry into or transit through the territory of Member States taken in accordance with legal acts adopted by the Council, including measures implementing a travel ban issued by the Security Council of the United Nations, shall, insofar as data-quality requirements are satisfied, be entered into SIS for the purpose of refusing entry and stay.

2. The alerts shall be entered, kept up-to-date and deleted by the competent authority of the Member State which holds the Presidency of the Council of the European Union at the time of the adoption of the measure. If that Member State does not have access to SIS or to alerts entered in accordance with this Regulation, the responsibility shall be taken up by the Member State which holds the subsequent Presidency and which has access to SIS, including to alerts entered in accordance with this Regulation.

Member States shall put in place the necessary procedures for entering, updating and deleting such alerts.

Article 26

Conditions for entering alerts on third-country nationals who are beneficiaries of the right of free movement within the Union

1. An alert on a third-country national who is a beneficiary 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, shall be in conformity with the rules adopted in implementation of that Directive or agreement.

2. Where there is a hit on an alert entered in accordance with Article 24 on a third-country national who is a beneficiary of the right of free movement within the Union, the executing Member State shall immediately consult the issuing Member State, through the exchange of supplementary information, in order to decide without delay on the action to be taken.

▼B

Article 27

Prior consultation before granting or extending a residence permit or long-stay visa

Where a Member State considers granting or extending a residence permit or long-stay visa to a third-country national who is the subject of an alert for refusal of entry and stay entered by another Member State, the Member States involved shall consult each other through the exchange of supplementary information, in accordance with the following rules:

(a) the granting Member State shall consult the issuing Member State prior to granting or extending the residence permit or long-stay visa;

(b) the issuing Member State shall reply to the consultation request within 10 calendar days;

(c) the absence of a reply by the deadline referred to in point (b) shall mean that the issuing Member State does not object to the granting or extending of the residence permit or long-stay visa;

(d) when making the relevant decision, the granting Member State shall take into account the reasons for the decision of the issuing Member State and shall consider, in accordance with national law, any threat to public policy or to public security which the presence of the third-country national in question on the territory of the Member States may pose;

(e) the granting Member State shall notify the issuing Member State of its decision; and

(f) where the granting Member State notifies the issuing Member State that it intends to grant or extend the residence permit or long-stay visa or that it has decided to do so, the issuing Member State shall delete the alert for refusal of entry and stay.

The final decision on whether to grant a residence permit or long-stay visa to a third-country national rests with the granting Member State.

Article 28

Prior consultation before entering an alert for refusal of entry and stay

Where a Member State has taken a decision referred to in Article 24(1) and considers entering an alert for refusal of entry and stay on a third-country national who is the holder of a valid residence permit or long-stay visa granted by another Member State, the Member States involved shall consult each other through the exchange of supplementary information, in accordance with the following rules:

(a) the Member State that has taken the decision referred to in Article 24(1) shall inform the granting Member State of the decision;

(b) the information exchanged under point (a) of this Article shall include sufficient detail on the reasons for the decision referred to in Article 24(1);

▼B

(c) on the basis of the information provided by the Member State that has taken the decision referred to in Article 24(1), the granting Member State shall consider whether there are reasons for withdrawing the residence permit or long-stay visa;

(d) when making the relevant decision, the granting Member State shall take into account the reasons for the decision of the Member State that has taken the decision referred to in Article 24(1) and shall consider, in accordance with national law, any threat to public policy or to public security which the presence of the third-country national in question on the territory of the Member States may pose;

(e) within 14 calendar days of receipt of the request for consultation the granting Member State shall notify the Member State that has taken the decision referred to in Article 24(1) of its decision or, where it has been impossible for the granting Member State to take a decision within that period, shall make a reasoned request to extend exceptionally the time period for its response for a maximum of a further 12 calendar days;

(f) where the granting Member State notifies the Member State that has taken the decision referred to in Article 24(1) that it is maintaining the residence permit or long-stay visa, the Member State that has taken the decision shall not enter the alert for refusal of entry and stay.

Article 29

A posteriori consultation after entering an alert for refusal of entry and stay

Where it emerges that a Member State has entered an alert for refusal of entry and stay on a third-country national who is the holder of a valid residence permit or long-stay visa granted by another Member State, the Member States involved shall consult each other through the exchange of supplementary information, in accordance with the following rules:

(a) the issuing Member State shall inform the granting Member State of the alert for refusal of entry and stay;

(b) the information exchanged under point (a) shall include sufficient detail on the reasons for the alert for refusal of entry and stay;

(c) on the basis of the information provided by the issuing Member State, the granting Member State shall consider whether there are reasons for withdrawing the residence permit or long-stay visa;

(d) when making its decision, the granting Member State shall take into account the reasons for the decision of the issuing Member State and shall consider, in accordance with national law, any threat to public policy or to public security which the presence of the third-country national in question on the territory of the Member States may pose;

(e) within 14 calendar days of receipt of the request for consultation the granting Member State shall notify the issuing Member State of its decision or, where it has been impossible for the granting Member State to take a decision within that period, shall make a reasoned request to extend exceptionally the time period for its response for a maximum of a further 12 calendar days;

▼B

(f) where the granting Member State notifies the issuing Member State that it is maintaining the residence permit or long-stay visa, the issuing Member State shall immediately delete the alert for refusal of entry and stay.

Article 30

Consultation in the case of a hit concerning a third-country national holding a valid residence permit or long-stay visa

Where a Member State encounters a hit on an alert for refusal of entry and stay entered by a Member State on a third-country national who is the holder of a valid residence permit or long-stay visa granted by another Member State, the Member States involved shall consult each other through the exchange of supplementary information, in accordance with the following rules:

(a) the executing Member State shall inform the issuing Member State of the situation;

(b) the issuing Member State shall initiate the procedure laid down in Article 29;

(c) the issuing Member State shall notify the executing Member State of the outcome following the consultation.

The decision on the entry of the third-country national shall be taken by the executing Member State in accordance with Regulation (EU) 2016/399.

Article 31

Statistics on exchange of information

Member States shall provide statistics to eu-LISA on an annual basis on the exchanges of information carried out in accordance with Articles 27 to 30 and on the instances in which the deadlines provided for in those Articles were not met.

CHAPTER VI

SEARCH WITH BIOMETRIC DATA

Article 32

Specific rules for entering photographs, facial images and dactyloscopic data

1. Only photographs, facial images and dactyloscopic data referred to in points (w) and (x) of Article 20(2) which fulfil minimum data quality standards and technical specifications shall be entered into SIS. Before such data are entered, a quality check shall be performed in order to ascertain whether the minimum data quality standards and technical specifications have been met.

2. Dactyloscopic data entered in SIS may consist of one to ten flat fingerprints and one to ten rolled fingerprints. It may also include up to two palm prints.

▼B

3. Minimum data quality standards and technical specifications shall be established in accordance with paragraph 4 of this Article for the storage of the biometric data referred to in paragraph 1 of this Article. Those minimum data quality standards and technical specifications shall set the level of quality required for using the data to verify the identity of a person in accordance with Article 33(1) and for using the data to identify a person in accordance with Article 33(2) to (4).

4. The Commission shall adopt implementing acts to lay down the minimum data quality standards and technical specifications referred to in paragraphs 1 and 3 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).

Article 33

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

1. Where photographs, facial images and dactyloscopic data are available in an alert in SIS, such photographs, facial images and dactyloscopic data 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 24 and 25 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.

4. As soon as it becomes technically possible, and while ensuring a high degree of reliability of identification, photographs and facial images may be used to identify a person in the context of regular border crossing points.

Before this functionality is implemented in SIS, the Commission shall present a report on the availability, readiness and reliability of the required technology. The European Parliament shall be consulted on the report.

After the start of the use of the functionality at regular border crossing points, the Commission shall be empowered to adopt delegated acts in accordance with Article 61 to supplement this Regulation concerning the determination of other circumstances in which photographs and facial images may be used to identify persons.

▼B

CHAPTER VII

RIGHT OF ACCESS AND REVIEW AND DELETION OF ALERTS

Article 34

National competent authorities having a right to access data in SIS

1. National competent authorities responsible for the identification of third-country nationals 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 ([1]), and, where relevant, providing advice in accordance with Council Regulation (EC) No 377/2004 ([2]);

(f) examining visa applications and taking decisions related to those applications including on whether to annul, revoke or extend visas, in accordance with Regulation (EC) No 810/2009 of the European Parliament and of the Council ([3]);

▼M1

(g) verifying different identities and combating identity fraud in accordance with Chapter V of Regulation (EU) 2019/817.

([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]) Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code) (OJ L 243, 15.9.2009, p. 1).

▼B

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. For the purposes of Articles 24 and 25 the right to access data 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 right to access data concerning documents relating to persons entered in accordance with Article 38(2)(k) and (l) of Regulation (EU) 2018/1862 and the right to search such data may also be exercised by the authorities referred to in point (f) of paragraph 1 of this Article.

5. The competent authorities referred to in this Article shall be included in the list referred to in Article 41(8).

Article 35

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 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.

▼B

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.

▼B

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 36

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 34(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 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.

▼B

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 37

Evaluation of the use of SIS by Europol 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 and the teams referred to in Article 36(1) at least every five years.

2. Europol 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.

Article 38

Scope of access

End-users, including Europol 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 39

Review period for alerts

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

2. An issuing Member State shall, within three years of the entry of an alert into SIS, review the need to retain it. However, if the national decision on which the alert is based provides for a longer period of validity than three years, the alert shall be reviewed within five years.

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

▼B

4. Within the review period, the issuing Member State may, following a comprehensive individual assessment, which shall be recorded, decide to retain the alert for longer than the review period, where this proves necessary and proportionate for the purposes for which the alert was entered. In such a case, paragraph 2 shall also apply to the extension. Any such extension shall be communicated to CS-SIS.

5. Alerts shall be deleted automatically after the review period referred to in paragraph 2 has expired except where the issuing Member State has informed CS-SIS of an extension pursuant to paragraph 4. CS-SIS shall automatically inform the issuing Member State of the scheduled deletion of data four months in advance.

6. Member States shall keep statistics on the number of alerts the retention periods of which have been extended in accordance with paragraph 4 of this Article and transmit them, upon request, to the supervisory authorities referred to in Article 55.

7. As soon as it becomes clear to a SIRENE Bureau that an alert 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 by the SIRENE Bureau. SIRENE Bureaux shall report any recurring issues they encounter when acting under this paragraph to their supervisory authority.

Article 40

Deletion of alerts

1. Alerts for refusal of entry and stay pursuant to Article 24 shall be deleted:

(a) when the decision on the basis of which the alert was entered has been withdrawn or annulled by the competent authority; or

(b) where applicable, following the consultation procedure referred to in Article 27 and Article 29.

2. Alerts on third-country nationals who are the subject of a restrictive measure intended to prevent entry into or transit through the territory of Member States shall be deleted when the restrictive measure has been terminated, suspended or annulled.

3. Alerts on a person who has acquired citizenship of a Member State or of any State whose nationals are beneficiaries of the right of free movement under Union law shall be deleted as soon as the issuing Member State becomes aware, or is so informed pursuant to Article 44 that the person in question has acquired such citizenship.

4. Alerts shall be deleted upon expiry of the alert in accordance with Article 39.

▼B

CHAPTER VIII

GENERAL DATA PROCESSING RULES

Article 41

Processing of SIS data

1. The Member States shall only process the data referred to in Article 20 for the purposes of refusing entry into and stay on their territories.

2. Data shall only be copied for technical purposes, where such copying is necessary in order for the competent authorities referred to in Article 34 to carry out a direct search. This Regulation shall apply to those copies. A Member State shall not copy 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.

Notwithstanding the first subparagraph, technical copies which result in offline databases to be used by visa-issuing authorities shall not be permitted, except for copies made to be used only in an emergency following the unavailability of the network for more than 24 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 34 shall only be authorised within the limits of their competence and only to duly authorised staff.

5. Any processing of SIS data by Member States 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. Data concerning documents related to persons that are entered into SIS under points (k) and (l) of Article 38(2) of Regulation (EU) 2018/1862 may be used by the competent authorities referred to in point (f) of Article 34(1) in accordance with the laws of each Member State.

7. Any use of SIS data which does not comply with paragraphs 1 to 6 of this Article shall be considered as misuse under the national law of each Member State and subject to penalties in accordance with Article 59.

▼B

8. 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.

9. 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 42

SIS data and national files

1. Article 41(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 41(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 43

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 44

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(2), 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(2), 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. The data shall only be transmitted if the identity of the third-country national is ascertained.

▼B

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 57.

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 47 and of the right to redress under Article 54(1).

Article 45

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 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.

▼B

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.

▼C1

7. Where a security incident is caused by the misuse of data, Member States, Europol and the European Border and Coast Guard Agency shall ensure that penalties are imposed in accordance with Article 59.

▼B

Article 46

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 47

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.

▼B

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 62(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 48

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.

▼B

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 62(2).

Article 49

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 50

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.

▼B

CHAPTER IX

DATA PROTECTION

Article 51

Applicable legislation

1. Regulation (EU) 2018/1725 shall apply to the processing of personal data by eu-LISA and by the European Border and Coast Guard Agency under this Regulation. Regulation (EU) 2016/794 shall apply to the processing of personal data by Europol under this Regulation.

2. Regulation (EU) 2016/679 shall apply to the processing of personal data under this Regulation by the competent authorities referred to in Article 34 of this Regulation with the exception of processing for the purposes of the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security where Directive (EU) 2016/680 applies.

Article 52

Right of information

1. Third-country nationals who are the subject of an alert in SIS shall be informed of this in accordance with Articles 13 and 14 of Regulation (EU) 2016/679 or Articles 12 and 13 of Directive (EU) 2016/680. This information shall be provided in writing, together with a copy of or a reference to the national decision giving rise to the alert, as referred to in Article 24(1) of this Regulation.

2. This information shall not be provided where national law allows for the right of information to be restricted, in particular in order to safeguard national security, defence, public security, and the prevention, detection, investigation and prosecution of criminal offences.

Article 53

Right of access, rectification of inaccurate data and erasure of unlawfully stored data

1. Data subjects shall be able to exercise the rights laid down in Articles 15, 16 and 17 of Regulation (EU) 2016/679 and in Article 14 and Article 16(1) and (2) of Directive (EU) 2016/680.

2. A Member State other than the issuing Member State may provide to the data subject information concerning any of the data subject's personal data that are being processed, only if it first gives the issuing Member State an opportunity to state its position. The communication between those Member States shall be done through the exchange of supplementary information.

▼B

3. A Member State shall take a decision not to provide information to the data subject, in whole or in part, in accordance with national law, to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the data subject concerned, in order to:

(a) avoid obstructing official or legal inquiries, investigations or procedures;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect public security;

(d) protect national security; or

(e) protect the rights and freedoms of others.

In cases referred to in the first subparagraph, the Member State shall inform the data subject in writing, without undue delay, of any refusal or restriction of access and of the reasons for the refusal or restriction. Such information may be omitted where its provision would undermine any of the reasons set out in points (a) to (e) of the first subparagraph. The Member State shall inform the data subject of the possibility of lodging a complaint with a supervisory authority or of seeking a judicial remedy.

The Member State shall document the factual or legal reasons on which the decision not to provide information to the data subject is based. That information shall be made available to the supervisory authorities.

For such cases, the data subject shall also be able to exercise his or her rights through the competent supervisory authorities.

4. Following an application for access, rectification or erasure, the Member State shall inform the data subject as soon as possible and in any event within the deadlines referred to in Article 12(3) of Regulation (EU) 2016/679 about the follow-up given to the exercise of the rights under this Article, regardless of whether the data subject is in a third country or not.

Article 54

Remedies

1. Without prejudice to the provisions on remedies of Regulation (EU) 2016/679 and of Directive (EU) 2016/680, any person may bring an action before any competent authority, including a court, under the law of any Member State to access, rectify, erase, obtain information or obtain compensation in connection with an alert relating to him or her.

2. The Member States undertake mutually to enforce final decisions handed down by the courts or authorities referred to in paragraph 1 of this Article, without prejudice to Article 58.

▼B

3. Member States shall report annually to the European Data Protection Board on:

(a) the number of access requests submitted to the data controller and the number of cases where access to the data was granted;

(b) the number of access requests submitted to the supervisory authority and the number of cases where access to the data was granted;

(c) the number of requests for the rectification of inaccurate data and for the erasure of unlawfully stored data to the data controller and the number of cases where the data were rectified or erased;

(d) the number of requests for the rectification of inaccurate data and the erasure of unlawfully stored data submitted to the supervisory authority;

(e) the number of court proceedings initiated;

(f) the number of cases where the court ruled in favour of the applicant;

(g) any observations on cases of mutual recognition of final decisions handed down by the courts or authorities of other Member States on alerts entered by the issuing Member State.

A template for the reporting referred to in this paragraph shall be developed by the Commission.

4. The reports from the Member States shall be included in the joint report referred to in Article 57(4).

Article 55

Supervision of N.SIS

1. Member States shall ensure that the independent supervisory authorities designated in each Member State and endowed with the powers referred to in Chapter VI of Regulation (EU) 2016/679 or Chapter VI of Directive (EU) 2016/680 monitor the lawfulness of the processing of personal data in SIS on their territory, its transmission from their territory and the exchange and further processing of supplementary information on their territory.

2. The supervisory authorities shall ensure that an audit of the data processing operations in its N.SIS is carried out in accordance with international auditing standards at least every four years. The audit shall either be carried out by the supervisory authorities, or the supervisory authorities shall directly order the audit from an independent data protection auditor. The supervisory authorities shall at all times retain control over and undertake the responsibilities of the independent auditor.

3. Member States shall ensure that their supervisory authorities have sufficient resources to fulfil the tasks entrusted to them under this Regulation and have access to advice from persons with sufficient knowledge of biometric data.

▼B

Article 56

Supervision of eu-LISA

1. The European Data Protection Supervisor shall be responsible for monitoring the processing of personal data by eu-LISA and for ensuring that it is carried out in accordance with this Regulation. The tasks and powers referred to in Articles 57 and 58 of Regulation (EU) 2018/1725 shall apply accordingly.

2. The European Data Protection Supervisor shall carry out an audit of the processing of personal data by eu-LISA in accordance with international auditing standards at least every four years. A report on that audit shall be sent to the European Parliament, to the Council, to eu-LISA, to the Commission and to the supervisory authorities. eu-LISA shall be given an opportunity to make comments before the report is adopted.

Article 57

Cooperation between supervisory authorities and the European Data Protection Supervisor

1. The supervisory authorities and the European Data Protection Supervisor, each acting within the scope of their respective competences, shall actively cooperate within the framework of their responsibilities and shall ensure coordinated supervision of SIS.

2. The supervisory authorities and the European Data Protection Supervisor shall, each acting within the scope of their respective competences, exchange relevant information, assist each other in carrying out audits and inspections, examine difficulties in the interpretation or application of this Regulation and other applicable Union legal acts, study problems that are revealed through the exercise of independent supervision or through the exercise of the rights of data subjects, draw up harmonised proposals for joint solutions to any problems and promote awareness of data protection rights, as necessary.

3. For the purposes laid down in paragraph 2, the supervisory authorities and the European Data Protection Supervisor shall meet at least twice a year as part of the European Data Protection Board. The costs and servicing of these meetings shall be borne by the European Data Protection Board. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary.

4. A joint report of activities as regards coordinated supervision shall be sent annually by the European Data Protection Board to the European Parliament, to the Council, and to the Commission.

CHAPTER X

LIABILITY AND PENALTIES

Article 58

Liability

1. Without prejudice to the right to compensation and to any liability under Regulation (EU) 2016/679, Directive (EU) 2016/680 and Regulation (EU) 2018/1725:

▼B

(a) any person or Member State that has suffered material or non-material damage, as a result of an unlawful personal data processing operation through the use of N.SIS or any other act incompatible with this Regulation by a Member State, shall be entitled to receive compensation from that Member State; and

(b) any person or Member State that has suffered material or non-material damage as a result of any act by eu-LISA incompatible with this Regulation shall be entitled to receive compensation from eu-LISA.

A Member State or eu-LISA shall be exempted from their liability under the first subparagraph, in whole or in part, if they prove that they are not responsible for the event which gave rise to the damage.

2. If any failure of a Member State to comply with its obligations under this Regulation causes damage to SIS, that Member State shall be held liable for such damage, unless and insofar as eu-LISA or another Member State participating in SIS failed to take reasonable measures to prevent the damage from occurring or to minimise its impact.

3. Claims for compensation against a Member State for the damage referred to in paragraphs 1 and 2 shall be governed by the national law of that Member State. Claims for compensation against eu-LISA for the damage referred to in paragraphs 1 and 2 shall be subject to the conditions provided for in the Treaties.

Article 59

Penalties

Member States shall ensure that any misuse of SIS data, or any processing of such data or any exchange of supplementary information contrary to this Regulation, is punishable in accordance with national law.

The penalties provided for shall be effective, proportionate and dissuasive.

CHAPTER XI

FINAL PROVISIONS

Article 60

Monitoring and statistics

1. eu-LISA shall ensure that procedures are in place to monitor the functioning of SIS against objectives relating to output, cost-effectiveness, security and quality of service.

2. For the purposes of technical maintenance, reporting, data quality reporting and statistics, eu-LISA shall have access to the necessary information relating to the processing operations performed in Central SIS.

▼B

3. eu-LISA shall produce daily, monthly and annual statistics showing the number of records per category of alerts, both for each Member State and in aggregate. eu-LISA shall also provide annual reports on the number of hits per category of alert, how many times SIS was searched and how many times SIS was accessed for the purpose of entering, updating or deleting an alert, both for each Member State and in aggregate. Such statistics shall include statistics on the exchanges of information under Article 27 to Article 31. The statistics produced shall not contain any personal data. The annual statistical report shall be published.

4. Member States, Europol and the European Border and Coast Guard Agency shall provide eu-LISA and the Commission with the information necessary to draft the reports referred to in paragraphs 3, 5, 7 and 8.

5. eu-LISA shall provide the European Parliament, the Council, the Member States, the Commission, Europol, the European Border and Coast Guard Agency and the European Data Protection Supervisor with any statistical reports that it produces.

In order to monitor the implementation of Union legal acts, including for the purposes of Regulation (EU) No 1053/2013, the Commission may request that eu-LISA provide additional specific statistical reports, either on a regular or ad hoc basis, on the performance of SIS, the use of SIS and on the exchange of supplementary information.

The European Border and Coast Guard Agency may request that eu-LISA provide additional specific statistical reports for the purpose of carrying out risk analyses and vulnerability assessments as referred to in Articles 11 and 13 of Regulation (EU) 2016/1624, either on a regular or ad hoc basis.

▼M1

6. For the purpose of Article 15(4) and of paragraphs 3, 4 and 5 of this Article, eu-LISA shall store data referred to in Article 15(4) and in paragraph 3 of this Article which shall not allow for the identification of individuals in the central repository for reporting and statistics referred to in Article 39 of Regulation (EU) 2019/817.

eu-LISA shall allow the Commission and the bodies referred to in paragraph 5 of this Article to obtain bespoke reports and statistics. Upon request, eu-LISA shall grant access to the central repository for reporting and statistics in accordance with Article 39 of Regulation (EU) 2019/817 to Member States, the Commission, Europol, and the European Border and Coast Guard Agency.

▼B

7. Two years after the date of application of this Regulation pursuant to the first subparagraph of Article 66(5) and every two years thereafter, eu-LISA shall submit to the European Parliament and to the Council a report on the technical functioning of Central SIS and of the Communication Infrastructure, including their security, on the AFIS and on the bilateral and multilateral exchange of supplementary information between Member States. This report shall also contain, once the technology is in use, an evaluation of the use of facial images to identify persons.

▼B

8. Three years after the date of application of this Regulation pursuant to the first subparagraph of Article 66(5) and every four years thereafter, the Commission shall carry out an overall evaluation of Central SIS and the bilateral and multilateral exchange of supplementary information between Member States. That overall evaluation shall include an examination of results achieved against objectives, and an assessment of the continuing validity of the underlying rationale, the application of this Regulation in respect of Central SIS, the security of Central SIS and any implications for future operations. The evaluation report shall also include an assessment of the AFIS and the SIS information campaigns carried out by the Commission in accordance with Article 19.

The evaluation report shall also contain statistics on the number of alerts entered in accordance with point (a) of Article 24(1)and statistics on the number of alerts entered in accordance with point (b) of that paragraph. As regards alerts falling under point (a) of Article 24(1), it shall detail how many alerts were entered following the situations referred to in point (a), (b) or (c) of Article 24(2). The evaluation report shall also contain an assessment of the application of Article 24 by Member States.

The Commission shall transmit the evaluation report to the European Parliament and to the Council.

9. The Commission shall adopt implementing acts to lay down detailed rules on the operation of the central repository referred to in paragraph 6 of this Article and the data protection and security rules applicable to that repository. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).

Article 61

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 33(4) shall be conferred on the Commission for an indeterminate period of time from 27 December 2018.

3. The delegation of power referred to in Article 33(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

▼B

6. A delegated act adopted pursuant to Article 33(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 62

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Article 63

Amendments to Regulation (EC) No 1987/2006

Regulation (EC) No 1987/2006 is amended as follows:

(1) Article 6 is replaced by the following:

'Article 6

National Systems

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

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

(2) Article 11 is replaced by the following:

'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 II data and supplementary information, in accordance with its national legislation. This obligation shall also apply after those people 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 II-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.

▼B

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

(3) Article 15 is amended as follows:

(a) the following paragraph is inserted:

'3a. The Management Authority shall develop and maintain a mechanism and procedures for carrying out quality checks on the data in CS-SIS. It shall provide regular reports to the Member States in this regard.

The Management Authority shall provide a regular report to the Commission covering the issues encountered and the Member States concerned.

The Commission shall provide the European Parliament and the Council with a regular report on data quality issues that are encountered.';

(b) paragraph 8 is replaced by the following:

'8. The operational management of Central SIS II shall consist of all the tasks necessary to keep Central SIS II functioning 24 hours a day, 7 days a week in accordance with this Regulation, in particular the maintenance work and technical developments necessary for the smooth running of the system. Those tasks shall also include the coordination, management and support of testing activities for Central SIS II and the N.SIS II that ensure that Central SIS II and the N.SIS II operate in accordance with the requirements for technical compliance set out in Article 9.';

(4) in Article 17, the following paragraphs are added:

'3. Where the Management Authority cooperates with external contractors in any SIS II-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.

4. The operational management of CS-SIS shall not be entrusted to private companies or private organisations.';

(5) in Article 20(2), the following point is inserted:

'(ka) the type of offence;';

(6) in Article 21, the following paragraph is added:

'Where the decision to refuse entry and stay referred to in Article 24(2) is related to a terrorist offence, the case shall be considered adequate, relevant and important enough to warrant an alert in SIS II. For public or national security reasons, Member States may exceptionally refrain from entering an alert when it is likely to obstruct official or legal inquiries, investigations or procedures.';

▼B

(7) Article 22 is replaced by the following:

'Article 22

Specific rules for entering, verification or search with photographs and fingerprints

1. Photographs and fingerprints shall only be entered following a special quality check to ascertain whether they fulfil minimum data quality standards. The specification of the special quality check shall be established in accordance with the procedure referred to in Article 51(2).

2. Where photographs and fingerprint data are available in an alert in SIS II, such photographs and fingerprint data shall be used to confirm the identity of a person who has been located as a result of an alphanumeric search made in SIS II.

3. Fingerprint data may be searched in all cases to identify a person. However, fingerprint 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 II shall contain an Automated Fingerprint Identification System (AFIS).

4. Fingerprint data in SIS II in relation to alerts entered in accordance with Articles 24 and 26 may also be searched using complete or incomplete sets of fingerprints 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.';

(8) Article 26 is replaced by the following:

'Article 26

Conditions for entering alerts on third-country nationals subject to restrictive measures

1. Alerts on third-country nationals who are the subject of a restrictive measure intended to prevent entry into or transit through the territory of Member States taken in accordance with legal acts adopted by the Council, including measures implementing a travel ban issued by the Security Council of the United Nations, shall, insofar as data-quality requirements are satisfied, be entered into SIS II for the purpose of refusing entry and stay.

2. The alerts shall be entered, kept up-to-date and deleted by the competent authority of the Member State which holds the Presidency of the Council of the European Union at the time of the adoption of the measure. If that Member State does not have access to SIS II or to alerts entered in accordance with this Regulation, the responsibility shall be taken up by the Member State which holds the subsequent Presidency and which has access to SIS II, including to alerts entered in accordance with this Regulation.

▼B

Member States shall put in place the necessary procedures for entering, updating and deleting such alerts.';

(9) the following Articles are inserted:

'Article 27a

Access to data in SIS II by Europol

1. The European Union Agency for Law Enforcement Cooperation (Europol), established by Regulation (EU) 2016/794 of the European Parliament and of the Council (*), shall, where necessary to fulfil its mandate, have the right to access and search data in SIS II. 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 II, 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 II 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 II 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 II;

(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

▼B

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 II, 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 II data receive appropriate training and information in accordance with Article 14; 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 II and in the exchange and processing of supplementary information.

6. Europol shall only copy data from SIS II 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 II 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 II data. Europol shall not copy alert data or additional data issued by Member States or from CS-SIS II 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 II 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 II.

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.

▼B

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

Article 27b

Access to data in SIS II 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 of the European Parliament and of the Council (**), 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 27(1) of this Regulation and have received the required training in accordance with Article 14 of this Regulation, have the right to access and search data in SIS II insofar it is necessary for the performance of their task and as required by the operational plan for a specific operation. Access to data in SIS II 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 II 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 II.

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 II, 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 II 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 II 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.

▼B

7. Without prejudice to paragraph 2, no parts of SIS II 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 II to which those teams have access be transferred to such a system. No part of SIS II shall be downloaded or copied. The logging of access and searches shall not be considered to be unlawful downloading or copying of SIS II 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 II. This shall be without prejudice to the further provisions of Regulation (EU) 2018/1725 of the European Parliament and of the Council (***).

_____

(*) 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).

(**) Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC (OJ L 251, 16.9.2016, p. 1).

(***) 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 64

Amendment to the Convention implementing the Schengen Agreement

Article 25 of the Convention implementing the Schengen Agreement is deleted.

Article 65

Repeal

Regulation (EC) No 1987/2006 is repealed from the date of application of this Regulation as set out in the first subparagraph of Article 66(5).

▼B

References to the repealed Regulation shall be construed as references to this Regulation and shall be read in accordance with the correlation table in the Annex.

Article 66

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 15(7), Article 19, Article 20(3) and (4), Article 32(4), Article 33(4), Article 47(4), Article 48(6), Article 60(6) and (9), Article 61, Article 62, points (1) to (6) and point (8) of Article 63, and paragraphs 3 and 4 of this Article shall apply from the date of entry into force of this Regulation;

(b) point (9) of Article 63 shall apply from 28 December 2019;

(c) point (7) of Article 63 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*.

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

▼B

ANNEX

CORRELATION TABLE

Regulation (EC) No 1987/2006	This Regulation
Article 1	Article 1
Article 2	Article 2
Article 3	Article 3
Article 4	Article 4
Article 5	Article 5
Article 6	Article 6
Article 7	Article 7
Article 8	Article 8
Article 9	Article 9
Article 10	Article 10
Article 11	Article 11
Article 12	Article 12
Article 13	Article 13
Article 14	Article 14
Article 15	Article 15
Article 16	Article 16
Article 17	Article 17
Article 18	Article 18
Article 19	Article 19
Article 20	Article 20
Article 21	Article 21
Article 22	Articles 32 and 33
Article 23	Article 22
—	Article 23
Article 24	Article 24
Article 25	Article 26
Article 26	Article 25
—	Article 27
—	Article 28
—	Article 29
—	Article 30
—	Article 31
Article 27	Article 34
Article 27a	Article 35
Article 27b	Article 36

▼B

Regulation (EC) No 1987/2006	This Regulation
—	Article 37
Article 28	Article 38
Article 29	Article 39
Article 30	Article 40
Article 31	Article 41
Article 32	Article 42
Article 33	Article 43
Article 34	Article 44
—	Article 45
Article 35	Article 46
Article 36	Article 47
Article 37	Article 48
Article 38	Article 49
Article 39	Article 50
Article 40	—
—	Article 51
Article 41	Article 53
Article 42	Article 52
Article 43	Article 54
Article 44	Article 55
Article 45	Article 56
Article 46	Article 57
Article 47	—
Article 48	Article 58
Article 49	Article 59
Article 50	Article 60
—	Article 61
Article 51	Article 62
Article 52	—
—	Article 63
—	Article 64
Article 53	—
—	Article 65
Article 54	—
Article 55	Article 66