Council of the European Union

Brussels, 7 June 2017
(OR. en)

Interinstitutional File: 2016/0408 (COD)

9593/17

LIMITE

SIRIS 94
FRONT 242
SCHENGEN 30
COMIX 382
CODEC 906

NOTE

From:	Presidency
To:	Working Party for Schengen Matters (Acquis) / Mixed Committee (EU/Iceland, Norway and Switzerland, Liechtenstein)
No. prev. doc.:	8109/17
No. Cion doc.:	15813/16
Subject:	Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending Regulation (EU) No 515/2014 and repealing Regulation (EU) No 1987/2006 - Draft compromise text

Delegations will find attached a Presidency draft compromise text of the abovementioned proposal, taking into account the discussions held at the Working Party for Schengen Matters (Acquis) and the written comments subsequently sent by the delegations. The Working Party discussed on 16 January 2017 Articles 1 to 12 of the proposal set out in 15813/16, on 8 February 2017 Articles 13 to 19, Articles 30 to 32B and Articles 46 to 58, on 6 and 7 March 2017 Articles 20 to 29, and on 15 and 16 May 2017 Articles 33 to 45, completing thereby the first round of discussions on this proposal.

General scrutiny reservations on this instrument are pending from AT, BG, CZ, DE, FI, HU, IT, LT, NL, PL, PT, SE, and SI. Parliamentary reservations are pending from DE and PL. Reservations on specific provisions are indicated in footnotes.

Changes to the original Commission proposal are marked as follows: new or modified text is in **bold underlined**. Deletions are in ~~strikethrough~~.

Articles marked with " * " are deemed as agreed at the Working Party level.

_____

ANNEX

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 ~~apply~~**ensure the application of** the provisions of Chapter 2 of Title V of Part Three of the Treaty on the Functioning of the European Union relating to the movement of persons ~~in~~**on** their territories, using information communicated via this system.

*Article 2**

Scope

1. This Regulation establishes the conditions and procedures for the entry and processing in SIS of alerts in respect of third-country nationals, 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, the responsibilities of the Member States and of the European Agency ~~on~~**for** the operational management of large-scale IT systems in the area of freedom, security and justice, general data processing, the rights of the persons concerned and liability.

Article 3

Definitions

1. For the purposes of this Regulation, the following definitions shall apply:

(a) 'alert' means a set of data, including biometric identifiers as referred to in Article 22, entered in SIS allowing the competent authorities to identify a person with a view to taking specific action;

(b) 'supplementary information' means information not forming part of the alert data stored in SIS, but connected to **the purpose of** SIS alerts, which is to be exchanged **via the SIRENE Bureaux**:

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

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

(3) when the required action cannot be taken;

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

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

(6) when dealing with rights of access;

(c) 'additional data' means the data stored in SIS and connected with SIS alerts 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 searches made therein;

(d)[1] 'third-country national' means any person who is not a citizen of the Union within the meaning of Article 20(1) of the TFEU, with the exception of persons who enjoy rights of free movement equivalent to those of Union citizens under agreements between the Union, or the Union and its Member States on the one hand, and third countries on the other hand;

[1] DE entered a reservation on this provision. DE considers that a consistent definition for 'third-country national' should be used in all legal acts, including the Dublin Regulation.

(e) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’);

(f) ‘an identifiable natural person’ is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(g) ‘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, 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;

(h) a ‘hit’ in SIS means:

(1) a search is conducted by a**n end-**user**;**

(2) the search reveals an alert ~~in~~ entered by ~~another~~ **a** Member State in SIS**;**

(3) data concerning the alert in SIS match~~es~~ the search data**;**

(3a) the match is confirmed by the end-user; and

(4) further actions are requested ~~as a result of the hit~~**.**

(i) ‘issuing Member State’ means the Member State which entered the alert in SIS;

(ia) "granting Member State" means the Member State which consider granting or extending or has granted or extended a residency permit or long stay visa and is involved in the consultation procedure;

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

(k) ‘end-users’ mean competent authorities directly searching CS-SIS, N.SIS or a technical copy thereof**;**

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

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

(ma) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;[2]

(n) ‘dactylo~~graphic~~**scopic** data’ means data on fingerprints and palm prints which due to their unique character ~~of uniqueness~~ and the reference points contained therein enable accurate and conclusive comparisons on a person's identity;

(na) 'facial image' means digital images of the face with sufficient image resolution and quality to be used in automated biometric matching;[3]

(o) ‘serious crime’ means offences listed in Article 2(1) and (2) of Framework Decision 2002/584/JHA of 13 June 2002;[4]

---

[2] Same definition as in Article 3(13) of Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89). However, in the EES proposal, 'biometric data' is defined as 'fingerprint data and facial image' (see Article 3(17) in 9465/17).

[3] Same definition as in the EES proposal (see Article 3(16) in 9465/17)

[4] Council Framework Decision (2002/584/JHA) of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.07.2002, p. 1).

(p) 'terrorist offences' means offences under national law referred to in Articles ~~1-4 of Framework Decision 2002/475/JHA of 13 June 2002~~[5] **3 to 14 of Directive (EU) 2017/541**[6]**.**

(q) 'residence permit' means:

(a) all residence permits issued by the Member States according to the uniform format laid down by Council Regulation (EC) No 1030/2002[7] **and residence cards issued in accordance with Directive 2004/38/EC;**

(b) all other documents issued by a Member State to third-country nationals authorising a stay on its territory that have been the subject of a notification and subsequent publication in accordance with Article 39 of the Regulation (EU) 2016/399[8]**, with the exception of:**

(i) temporary permits issued pending examination of a first application for a residence permit as referred to in point (a) or an application for asylum; and

(ii) visas issued by the Member States in the uniform format laid down by Council Regulation (EC) No 1683/95[9]**;**

(r) 'long-stay visa' means a national visa for stays exceeding 90 days issued by one of the Member States in accordance with its national law or Union law, as referred to in Article 1(1) of the Regulation (EU) No 265/2010[10]**.**

~~[5] Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ L 164, 22.6.2002, p. 3).~~

[6] 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, 31/03/2017, p. 6.

[7] Council Regulation (EC) No 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third-country nationals (OJ L 157, 15.6.2002, p. 1).

[8] 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).

[9] Council Regulation (EC) No 1683/95 of 29 May 1995 laying down a uniform format for visas (OJ L 164, 14.7.1995, p. 1).

[10] Regulation (EU) No 265/2010 of the European Parliament and of the Council of 25 March 2010 amending the Convention Implementing the Schengen Agreement and Regulation (EC) No 562/2006 as regards movement of persons with a long-stay visa (OJ L 85, 31.3.2010. p. 1).

Article 4[11]

Technical architecture and ways of operating SIS

1. SIS shall be composed of:

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

   – a technical support function ('CS-SIS') containing a database, the 'SIS database',

   – a uniform national interface (NI-SIS);

   (b)[12] a national system (N.SIS) in each of the Member States, consisting of the national data systems which communicate with Central SIS. An N.SIS shall contain a data file (a 'national copy'), containing a complete or partial copy of the SIS database as well as a backup N.SIS. The N.SIS and its backup may be used simultaneously to ensure uninterrupted availability to end-users;

   (c) a communication infrastructure between 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).

2. ~~SIS data~~ **Member States** shall ~~be~~ entere~~d~~, update~~d~~, delete~~d~~ and search~~ed~~ **SIS data** via the various N.SIS. A partial or a full national copy shall be available for the purpose of carrying out automated searches in the territory of each of the Member States using such a copy. The partial national copy shall contain at least the data listed in Article 20(2) (a) **to** (v) of this Regulation. It shall not be possible to search the data files of other Member States' N.SIS.

---

11 SI entered a scrutiny reservation on this Article.

12 FI, supported by NO, opposed the obligation for the Member States to have a national copy and entered a reservation on this provision. PT also entered a reservation on this provision, as it favoured the existence of national copies, taking into account the high number of future queries, in particular for the purposes of border checks.

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 this system. CS-SIS and the backup CS-SIS shall be located in the two technical sites of the European Agency for the operational management of large-scale information systems in the area of freedom, security and justice established by Regulation (EU) No 1077/2011 ('the Agency'). CS-SIS or backup CS-SIS may contain an additional copy of the SIS database and may be used simultaneously in active operation provided that each of them is capable to process all transactions related to SIS alerts.

4. CS-SIS shall provide the services necessary for the entry and processing of SIS data, including searches in the SIS database. CS-SIS shall:

   (a) provide online update of the national copies;

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

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

   (d) provide uninterrupted availability.

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 European Union.

2. These costs shall include work done with respect to CS-SIS that ensures the provision of the services referred to in Article 4(4).

3. 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[13]

Article 6[*]

National systems

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

Each Member State shall be responsible for ensuring the continuous operation of the N.SIS, its connection to NI-SIS and the uninterrupted availability of SIS data to the end-users.

Each Member State shall transmit its alerts via its N.SIS.[14]

Article 7

N.SIS Office and SIRENE Bureau

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

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

   ~~Each Member State shall transmit its alerts via its N.SIS Office.~~[15]

[13] Articles 6 to 14 are also applicable to the Returns Proposal (15812/16) by virtue of Article 13 of the Returns Proposal.

[14] Moved from Article 7(1) *in fine*, excluding the word 'Office' at the end of the sentence.

[15] Moved to Art. 6 *in fine*.

2. Each Member State shall designate the authority which shall ensure the exchange and availability of all supplementary information (the SIRENE Bureau) in accordance with the provisions of the SIRENE Manual, as referred to in Article 8.

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

3. The Member States shall inform the Agency of their N.SIS ~~II~~ Office and of their SIRENE Bureau. The Agency shall publish the list of them together with the list referred to in Article 36(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 ~~personal~~**human** resources to ensure the continuous availability and exchange of supplementary information. In the event that the ~~the~~ Communication Infrastructure is unavailable, Member States may use other adequately secured technical means to exchange supplementary information.

2. Supplementary information shall be used only for the purpose for which it was transmitted in accordance with Article 43 unless prior consent is obtained from the issuing Member State.

3. The SIRENE Bureaux shall carry out their task in a quick and efficient manner, in particular by ~~replying~~ **reacting** to a request as soon as possible but **preferably** not later than 12 hours after the receipt of the request.

4. **The Commission shall adopt implementing acts to lay down d**etailed rules for the exchange of supplementary information **in the form of a manual entitled the 'SIRENE Manual'. Those implementing acts** shall be adopted ~~by means of implementing measures~~ in accordance with the examination procedure referred to in Article 55(2) ~~in the form of a manual called the 'SIRENE Manual'~~.

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 CS-SIS for the prompt and effective transmission of data. ~~Those common standards, protocols and technical procedures shall be adopted by means of implementing measures in accordance with the examination procedure referred to in Article 55(2).~~[16]

2. Member States shall ensure, by means of the services provided by CS-SIS, that data stored in the national copy are, by means of automatic updates referred to in Article 4(4), 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. End-users shall receive the data required to perform their tasks, in particular all data required for the identification of the data subject and to take the required action.

3.[17] **The Commission shall adopt implementing acts to lay down and develop common Standards, protocols and technical procedures, referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 55(2).**

[16] Moved to paragraph 3.
[17] Moved from paragraph 1, *in fine*.

Article 10

Security – Member States

1. Each Member State shall[18], in relation to its N.SIS, adopt the necessary measures, including a security plan, a business continuity plan and a disaster recovery plan in order to:

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

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

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

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

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

   (f) 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 ~~identities~~**identifiers**[19] and confidential access modes only (data access control);

   (g) 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 these profiles available to the national supervisory authorities referred to in Article 50(1) without delay upon their request (personnel profiles);

[18] eu-LISA proposes to insert the words: "in consultation with the Agency".
[19] Same wording as in Article 12(2) and (3) and Article 18(2) and (3).

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

(i) 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 the data were input (input control);

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

(k) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring (self-auditing).

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 securing the premises of the SIRENE Bureau.

3. Member States shall take measures equivalent to those referred to in paragraph 1 as regards security in respect of the processing of SIS data by the authorities referred to in Article 29.

4. The measures described in paragraphs 1 to 3 may be part of a generic security approach and plan at national level. However, the requirements foreseen in this Article and its applicability to the SIS shall be clearly identifiable in and ensured by that plan.

*Article 11**

Confidentiality – Member States

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.

Article 12

Keeping of logs at national level

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

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 transmitted and the ~~name~~**individual and unique user identifiers**[20] of both the competent authority and the person responsible for processing the data.

3. If the search is carried out with dactylo~~graphic~~**scopic** data or facial image in accordance with Article 22 the logs shall show, in particular, the type of data used to perform a search, a reference to the type of data transmitted and the ~~name~~**individual and unique user identifiers**[21] of both the competent authority and the person responsible for processing the data.

4. The logs may be used only for the purpose referred to in paragraph 1 and shall be deleted at the earliest one year, and at the latest three years, after their creation.

5. Logs may be kept longer if they are required for monitoring procedures that are already under way.

6. The ~~competent~~ national **supervisory** authorities in charge of checking whether or not searches are lawful, monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of the N.SIS, data integrity and security, shall have access, within the limits of their competence and at their request, to these logs for the purpose of fulfilling their duties.

---

20 Same wording as in paragraph 3 and Article 10(1)(f).

21 Same wording as in paragraph 2 and Article 10(1)(f).

7.[22] The Commission shall adopt implementing acts to establish the content of the log, referred to in paragraph 7. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 55(2).

*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 national supervisory authority.

*Article 14**

Staff training

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 about data-security, data-protection rules and the procedures on data processing as set out in the SIRENE Manual. The staff shall be informed of any relevant criminal offences and penalties.

[22] Text moved from paragraph 7.

CHAPTER III

RESPONSIBILITIES OF THE AGENCY[23]

Article 15

Operational management

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

2. [24] The Agency 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;

3. [25] The Commission shall be responsible for all other tasks relating to the Communication Infrastructure, in particular:

   (a) tasks relating to implementation of the budget;

   (b) acquisition and renewal;

   (c) contractual matters.

---

[23] Articles 15 –18 are also applicable to the proposal on Returns by virtue of Article 13 of the Returns Proposal.

[24] This provision would be redrafted in the context of the coming proposals on eu-LISA.

[25] This provision would be redrafted in the context of the coming proposals on eu-LISA.

4. The Agency shall also be responsible for the following tasks relating to the SIRENE Bureaux and communication between the SIRENE Bureaux:

   (a) the coordination**,** ~~and~~ management **and support** of testing **activities**;[26]

   (b) the maintenance and update of technical specifications for the exchange of supplementary information between SIRENE Bureaux and the **C**ommunication **I**nfrastructure and managing the impact of technical changes where it affects both SIS and the exchange of supplementary information between SIRENE Bureaux.

5. The Agency shall develop and maintain a mechanism and procedures for carrying out quality checks on the data in CS-SIS and shall provide regular reports to the Member States[27]. The Agency shall provide a regular report to the Commission covering the issues encountered and the Member States concerned. ~~This mechanism, procedures and interpretation of data quality compliance shall be laid down an developed by means of implementing measures in accordance with the examination procedure referred to in Article 55(2).~~[28]

6. Operational management of Central SIS shall consist of all the tasks necessary to keep Central SIS functioning 24 hours a day, seven 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 also include **the coordination, management and support of** testing activities **for Central SIS and the national systems,** ensuring that Central SIS and the national systems operate in accordance with the technical and functional requirements in accordance with Article 9 of this Regulation.

7.[29] **The Commission shall adopt implementing acts to establish the mechanism and procedures for the quality checks on the data in CS-SIS, referred to in paragraph 5, and the interpretation of data quality compliance. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 55(2).**

---

[26] PT, RO, eu-LISA expressed concerns on this provision.
[27] eu-LISA would prefer more clear provisions on its competences regarding access to data.
[28] Text moved to new paragraph 7.
[29] Text moved from paragraph 5.

Article 16[*]

Security

1. The Agency shall adopt the necessary measures[30], including of 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) 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 ~~identities~~**identifiers** and confidential access modes only (data access control);

   (g) create profiles describing the functions and responsibilities for persons who are authorised to access the data or the data processing facilities and make these profiles available to the European Data Protection Supervisor referred to in Article 51 without delay upon its request (personnel profiles);

30 eu-LISA asked to include in recital 40 a reference to Commission Decision 2017/46.

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

(i) 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 the data were input (input control);

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

(k) 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).

2. The Agency 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 – Agency

1. Without prejudice to Article 17 of the Staff Regulations of officials and the Conditions of Employment of other servants of the European Union, the Agency shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality of comparable standards to those laid down in Article 11 of this Regulation to all its staff required to work with SIS data. This obligation shall also apply after those persons leave office or employment or after the termination of their activities.

2. The Agency 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.

Article 18[*]

Keeping of logs at central level

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

2. The logs shall show, in particular, the history of the ~~alerts~~**alert**[31], the date and time of the data transmitted, the ~~type of~~ data used to perform searches, ~~the~~ **a** reference to the ~~type of~~ data transmitted and the ~~name~~**individual and unique user identifiers**[32] of the competent authority responsible for processing the data.

3. If the search is carried out with dactylo~~graphic~~**scopic** data or facial image in accordance with Articles 22 and 28 the logs shall show, in particular, the type of data used to perform a search, a reference to the type **of** data transmitted and the ~~names~~**individual and unique identifiers** of both the competent authority and the person responsible for processing the data.

4. The logs may only be used for the purposes mentioned in paragraph 1 and shall be deleted at the earliest one year, and at the latest three years, after their creation. The logs which include the history of alerts shall be erased after one to three years after deletion of the alerts.

5. Logs may be kept longer if they are required for monitoring procedures that are already underway.

6. The ~~competent authorities in charge of checking whether or not a search is lawful, monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of CS-SIS, data integrity and security,~~**European Data Protection Supervisor** shall have access, within the limits of ~~their~~**its** competence and at ~~their~~**its** request, to those logs for the purpose of fulfilling ~~their~~**its** tasks.

---

31 Singular, as in Article 12(2).

32 Same wording as in Articles 10(1)(f) and 12(2) and (3).

CHAPTER IV

INFORMATION TO THE PUBLIC[33]

Article 19[*]

SIS information campaigns

The Commission, in cooperation with the national supervisory authorities and the European Data Protection Supervisor, shall regularly carry out campaigns informing the public about the objectives of SIS, the data stored, the authorities having access to SIS and the rights of data subjects. Member States shall, in cooperation with their national supervisory authorities, devise and implement the necessary policies to inform their citizens about SIS generally.

CHAPTER V

ALERTS ISSUED IN RESPECT OF THIRD-COUNTRY NATIONALS FOR THE PURPOSE OF REFUSING ENTRY AND STAY

Article 20

Categories of data

1. Without prejudice to Article 8(1) or 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 of the Member States, as required for the purposes laid down in Article**s** 24 **and 27**.

2. The information on persons in relation to whom an alert has been issued shall only contain the following data:

   (a) surname~~(s)~~;

   (b) forename~~(s)~~;

[33] Article 19 is also applicable to the Returns Proposal by virtue of Article 13 of the Returns Proposal (15812/16).

(c) name~~(s)~~ 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**~~sex~~;

(i) nationality/nationalities;

(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 a~~n~~ **terrorism-related** activity ~~as referred to in Articles 1, 2 , 3 and 4 of Council Framework Decision 2002/475/JHA on combating terrorism~~;

(k) reason for the alert;

(l) authority issuing the alert;

(m) a reference to the decision giving rise to the alert;

(n) action to be taken;

(o) link~~(s)~~ to other alerts issued in SIS pursuant to Article **4**~~38~~;

(p) whether the person concerned is a family member of an EU citizen or other person who enjoys rights of free movement as referred to in Article 25;

(q) whether the decision on refusal of entry ~~is based on~~**concerns**:

– ~~a previous conviction as referred to in Article 24(2)(a)~~ **a third-country national posing a threat to public policy, public security or national security**;

– ~~a serious security threat as referred to in Article 24(2)(b);~~

– ~~an entry ban as referred to in Article 24(3)~~ **a third-country national who has been illegaly staying**; or

– ~~a restrictive measure as referred to in Article 27~~ **a third-country national subject to a restrictive measure**;

(r) type of offence (for alerts issued pursuant to Article 24(2) **and (3)** of this Regulation);

(s) the category of the person's identification document**s**;

(t) the country of issue of the person's identification document**s**;

(u) the number(s) of the person's identification document**s**;

(v) the date of issue of the person's identification document**s**;

(w) photographs and facial images;

(x) dactylo**scop**~~graph~~ic data;

(y) a ~~colour~~ copy of the identification document**s**.

3. The technical rules necessary for entering, updating, deleting and searching the data referred to in paragraph 2 shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 55(2).

4. ~~The technical rules necessary for searching the data referred to in paragraph 2 shall be laid down and developed in accordance with the examination procedure referred to in Article 55(2).~~[34] These technical rules shall be similar for searches in CS-SIS, in national copies and in technical copies, as referred to in Article 36 and they shall be based upon common standards laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 55(2).

Article 21

Proportionality

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

2. In the application of Article 24(2) Member States shall~~, in all circumstances,~~ create such an alert in relation to third country nationals if the offence falls under Articles **3 to 14 of Directive (EU) 2017/541**[35] ~~1-4 of Council Framework Decision 2002/475/JHA on combating terrorism~~[36]**, provided that it does not obstruct official or legal inquiries, investigations or procedures related to public or national security, or is not contrary to the principle of non-refoulement**[37].

---

[34] Redundant with previous paragraph.

[35] **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, 31/03/2017, p. 6.**

[36] ~~Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ L 164, 22.6.2002, p. 3).~~

[37] AT, BE, DE, FR, NL, SE, UK expressed concerns on the compulsory character of this provision. UK entered a reservation on this paragraph.

Article 22[*]

*Specific rules for entering photographs, facial images and dactylo**sco**~~graph~~ic data*

1. Data referred to in Article 20(2)(w) and (x) shall only be entered into SIS following a quality check to ascertain the fulfilment of a minimum data quality standard.

2. Quality standards shall be established for the storage of the data referred to under paragraph 1. The specification of these standards shall be laid down by means of implementing measures and updated in accordance with the examination procedure referred to in Article 55(2).

Article 23

Requirement for an alert to be entered

1[38]. ~~Where available, a~~**A**ll ~~other~~ data listed in Article 20(2) shall ~~also~~ be entered **where available**.

2[39]. An alert may not be entered without the data referred to in Article 20(2)(a), (g), **(h),** (k), (m), (n) and (q). ~~Where an alert is based upon a decision taken under Article 24 (2) the data referred to in Article 20(2)(r) shall also be entered.~~

Article 24

*Conditions for issuing alerts **for**~~on~~ refusal of entry and stay*

1. Data on third-country nationals in respect of whom an alert has been issued for the purposes of refusing entry and stay shall be entered in SIS on the basis of a national alert resulting from a decision taken by the competent administrative or judicial authorities in accordance with the rules of procedure laid down by national law taken on the basis of an individual assessment. Appeals against those decisions shall be made in accordance with national law.

[38] Moved from paragraph 2.
[39] Moved from paragraph 1.

2. An alert shall be entered where the decision referred to in paragraph 1 is based on a threat to public policy or public security or to national security which the presence of the third-country national in question in the territory of a Member State may pose. This situation shall arise in particular in the case of:

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

(b) a third-country national in respect of whom there are serious grounds for believing that he has committed a serious crime or in respect of whom there are clear indications of an intention to commit such an offence in the territory of a Member State.

3.[40] An alert shall **also** be entered where the ~~decision referred to in paragraph 1 is~~ **third country national in question is the subject of** an entry ban issued in accordance with procedures respecting Directive 2008/115/EC. The issuing Member State shall ensure that the alert **is entered in SIS as soon as the third-country national concerned has left the territory of the Member States in order to prevent his or her re-entry.** ~~takes effect in SIS at the point of return of the third-country national concerned. The confirmation of return shall be communicated to the issuing Member State in accordance with Article 6 of Regulation (EU) 2018/xxx [Return Regulation].~~

Article 25

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

1. An alert concerning a third-country national who is a beneficiary of the right of free movement within the Union, within the meaning of Directive 2004/38/EC of the European Parliament and of the Council[41] **or within the meaning of 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 ~~entered in accordance~~ **in conformity** with the ~~measures~~ **rules** adopted ~~to~~ **in** implement**ation of** that Directive **or that agreement**.

---

[40] BE and FR entered a scrutiny reservation on this paragraph.

[41] OJ L 158, 30.4.2004, p.77.

2. Where there is a hit on an alert pursuant to Article 24 concerning a third-country national who is a beneficiary of the right of free movement within the Union, the Member State executing the alert 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.

Article 26[42]

Consultation procedure

1. Where a Member State considers granting **or extending** a residence permit or ~~other authorisation offering a right to stay~~ **a 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, ~~it~~ **the granting Member State** shall first consult the issuing Member State through the exchange of supplementary information ~~and shall take account of the interests of that Member State~~. The issuing Member State shall ~~provide a definite reply within seven days~~ **inform the granting Member State within seven**[43] **working days about the reasons for its decision on prohibition of entry**. **The granting Member State shall take account of the interests of the issuing Member State, in particular when it concerns a third country national posing a threat to public policy, public security or national security.** Where the **granting** Member State ~~considering granting a permit or other authorisation offering a right to stay~~ decides to grant ~~it~~ **or extend the residence permit or long-stay visa**, the alert for refusal of entry and stay shall be deleted. **The issuing Member State may include the third-country national in its national list of alerts for the purpose of refusing entry into or stay on its territory. If the circumstances of the case so require the third-country national may also be included in SIS for discreet, inquiry or specific checks in accordance with Article 36 of Regulation (EU) 2018/xxx [police cooperation and judicial cooperation in criminal matters].**

---

42 AT and FR entered a scrutiny reservation on this Article.

43 AT, ES, HU, LU, PT, RO and SI considered seven days too short. HU entered a reservation on this delay. CZ agrees with seven days.

2. Where a Member State **is aware that a third-country national who is the subject of a refusal of entry decision in accordance with Article 24(1) is the holder of a valid residence permit or long-stay visa issued by another Member State and it** considers entering a~~n~~ **corresponding** alert for refusal of entry and stay ~~concerning a third-country national who is the holder of a valid residence permit or other authorisation offering a right to stay issued by another Member State~~, it shall first **inform** ~~consult~~ the Member State that issued the permit **or long-stay visa** through the exchange of supplementary information **in order to allow that Member State to decide whether there are reasons justifying the withdrawal of the permit or long-stay visa. The Member State that issued the permit or long-stay visa shall take into account the interests of the other Member State, in particular when the decision in accordance with Article 24(1) is based on a threat to public policy or national security which the presence of the third-country national concerned on the territory of this Member State may pose**~~and shall take account of the interests of that Member State~~. The Member State that issued the permit **or long-stay visa** shall provide a definite reply within seven **working** days. If the Member State that issued the permit **or long-stay visa** decides to maintain it, the alert for refusal of entry and stay shall not be entered. **The issuing Member State may include the third-country national in its national list of alerts for the purpose of refusing entry into or stay on its territory. If the circumstances of the case so require the third-country national may also be included in SIS for discreet, inquiry or specific checks in accordance with Article 36 of Regulation (EU) 2018/xxx [police cooperation and judicial cooperation in criminal matters].**

2a.[44] Where it emerges that an alert for the purposes of refusing entry has been issued for a third-country national who holds a valid residence permit or long-stay visa issued by a Member-State, the issuing Member State shall consult the granting Member State in order to determine whether there are sufficient reasons for withdrawing the residence permit or long-stay visa. The granting Member State shall take into account the interests of the issuing Member State, in particular when the decision in accordance with Article 24(1) is based on a threat to public policy or national security which the presence of the third-country national concerned on the territory of this Member State may pose. If the residence permit or long-stay visa is not withdrawn, the issuing Member State shall delete the alert but may nevertheless include the third-country national concerned on its national list of alerts for the purpose of refusing entry into or stay on its territory. If the circumstances of the case so require the third-country national may also be included in SIS for discreet, inquiry or specific checks ~~.~~in accordance with Article 36 of Regulation (EU) 2018/xxx [police cooperation and judicial cooperation in criminal matters].

3. In the event of a hit on an alert for refusal of entry and stay concerning a third-country national who is the holder of a valid residence permit or **long-stay visa**~~other authorisation offering a right to stay~~, the executing Member State shall consult immediately the Member State that issued the residence permit and the Member State that entered the alert, respectively, via the exchange of supplementary information in order to decide without delay if the action may be taken. **In addition, the Member State that issued the residence permit or long-stay visa and the Member State that entered the alert shall carry out a consultation in accordance with paragraph 2.** If it is **nevertheless** decided to maintain the residence permit **or long-stay visa**, the alert **for refusal of entry and stay** shall be deleted. **The issuing Member State and the executing Member State may include the third-country national concerned in their national lists of alerts for the purpose of refusing entry or stay in their territories. If the circumstances of the case so require the third-country national may also be included in SIS for discreet, inquiry or specific checks in accordance with Article 36 of Regulation (EU) 2018/xxx [police cooperation and judicial cooperation in criminal matters].**

---

44 Based on Article 25(2) of the Convention Implementing the Schengen Agreement (CISA), (OJ L 239, 22.9.2000, p.19).

4. Member States shall provide on an annual basis statistics to the Agency about the consultations carried out in accordance with paragraphs 1 to 3.

Article 27

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

1. Alerts relating to 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 in SIS for the purpose of refusing entry and stay.

2. The Member State responsible for entering, updating and deleting these alerts on behalf of all Member States shall be designated at the moment of the adoption of the relevant measure taken in accordance with Article 29 of the Treaty on European Union. The procedure for designating the Member State responsible shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 55(2).

Article 27A

Execution of action based on an alert

1. Where there is a hit on a third-country national pursuant to in Article 24 or 27, the competent authorities shall, without prejudice to Article 25(2):~~,~~

(a) refuse granting him or her a visa, or;

(b) refuse the entry into the territory.

In case the hit occurs inside the territory, the third-country national concerned shall be stopped, questioned and handed-over to the competent authority in order to take the necessary action.

2. Further details concerning the execution of action based on alert, exchange of supplementary information and further measures shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 55(2).

CHAPTER VI

SEARCH WITH BIOMETRIC DATA

Article 28

*Specific rules for verification or search with photographs, facial images and dactylo**sco**~~graph~~ic data*

1. Photographs, facial images and dactylo**sco**~~graph~~ic data shall be retrieved from SIS to verify the identity of a person who has been located as a result of an alphanumeric search made in SIS.

2. Dactylo**sco**~~graph~~ic data may ~~also~~**always** be used to identify a person. Dactylo**sco**~~graph~~ic data stored in SIS shall be ~~used~~ **searched** for identification purposes if the identity of the person cannot be ascertained by other means.

3. Dactylo**sco**~~graph~~ic data stored in SIS in relation to alerts issued under Article**s** 24 **and 27** may also be searched with complete or incomplete sets of fingerprints or palm prints discovered at the scenes of crimes under investigation and where it can be established to a high degree of probability that they belong to the perpetrator of the offence provided that the competent authorities are unable to establish the identity of the person by using any other national, European or international database.

4. As soon as this becomes technically possible, and while ensuring a high degree of reliability of identification, photographs and facial images may be used to identify a person. ~~Identification based on photographs or facial images shall only be used in the context of regular border crossing points where self-service systems and automated border control systems are in use.~~

5. Before these functionalities are implemented in SIS, the Commission shall present a report on the availability and readiness of the required technology, on which the European Parliament shall be consulted.[45]

[45] Similar to the text of Article 22(c) of Regulation (EC) No 1987/2006 of 20 December on the establishment, operation and use of the second generation Schengen Information System (SIS II).

CHAPTER VII

RIGHT TO ACCESS AND RETENTION OF ALERTS

Article 29

Authorities having a right to access alerts

1. **National competent authorities shall have a** ~~A~~ccess to data entered in SIS and the right to search such data directly or in a copy of SIS data ~~shall be reserved to the authorities responsible for the identification of third-country nationals~~ for the purposes of:

   (a) border control, in accordance with 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);

   (b) police and customs checks carried out within the Member State concerned, and the coordination of such checks by designated authorities;

   (c) other ~~law enforcement~~ activities carried out for the prevention, detection**,** ~~and~~ investigation **or prosecution** of criminal offences **or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security** within the Member State concerned;[46]

   (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 **or naturalisation**, and to the return of third-country nationals;

   (e) examining visa applications and taking decisions related to those applications including on whether to annul, revoke or extend visas, in accordance with Regulation (EU) No 810/2009 of the European Parliament and of the Council.[47]

[46] In line with text of Article 3(7) of Directive 2016/680**.**

[47] 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).

(f) checks on third-country nationals who are illegaly entering or staying on the territory of the Member States as well as on applicants for international protection and third-country nationals arriving at hotspot areas as defined in Article 2(10) of Regulation (EU) 2016/1624;

2. For the purposes of Article 24(2) and (3) and Article 27 the right to access data entered in SIS and the right to search such data directly may also be exercised by national judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to charge, in the performance of their tasks, as provided for in national legislation, and by their coordinating authorities.

3. The right to access data concerning documents relating to persons entered in accordance with Article 38(2)(j) and (k) of Regulation (EU) 2018/xxx [police cooperation and judicial cooperation in criminal matters] and the right to search such data may also be exercised by the authorities referred to in paragraph 1(~~d~~**e**). Access to data by these authorities shall be governed by the law of each Member State.

4. The authorities referred to in this Article shall be included in the list referred to in Article 36(8).

Article 30[48]

Access to SIS data by Europol

1. The European Union Agency for Law Enforcement Cooperation (Europol) shall have**,** within its mandate, ~~have~~ the right to access and search data entered into SIS.

2. Where a search by Europol reveals the existence of an alert in SIS, Europol shall inform the issuing Member State via the **exchange of supplementary information. Until such time that Europol has implemented this functionality, it shall inform the issuing Member State via the** channels defined by Regulation (EU) 2016/794.

[48] DE entered a scrutiny reservation on this Article.

3. The use of information obtained from a search in the SIS is subject to the consent of the **issuing** Member State. If the Member State allows the use of such information, the handling thereof by Europol shall be governed by Regulation (EU) 2016/794. Europol may only communicate such information to third countries and third bodies with the consent of the **issuing** Member State ~~concerned~~.

4. ~~Europol may request further information from the Member State concerned in accordance with the provisions of Regulation (EU) 2016/794.~~

5. Europol shall:

   (a) without prejudice to paragraphs 3, 4 and 6, not connect parts of SIS nor transfer the data contained therein to which it has access to any computer system for data collection and processing operated by or at Europol nor download or otherwise copy any part of SIS;

   (b) limit access to data entered in SIS to specifically authorised staff of Europol;

   (c) adopt and apply measures provided for in Articles 10 and 11;

   (d) allow the European Data Protection Supervisor to review the activities of Europol in the exercise of its right to access and search data entered in SIS.

6. Data may only be copied for technical purposes, provided that such copying is necessary in order for duly authorised Europol staff to carry out a direct search. The provisions of this Regulation shall apply to such copies. The technical copy shall 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 construed to be an 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. Any copies, as referred to in paragraph 6, which lead to off-line databases may be retained for a period not exceeding 48 hours. That period may be extended in an emergency until the emergency comes to an end. Europol shall report any such extensions to the European Data Protection Supervisor.

8. ~~Europol may receive and process supplementary information on corresponding SIS alerts provided that the data processing rules referred to in paragraphs (2)-(7) are applied as appropriate.~~

9. For the purpose of verifying the lawfulness of data processing, self-monitoring and ensuring proper data security and integrity Europol should keep logs of every access to and search in SIS **in accordance with Article 12**. Such logs and documentation shall not be considered to be the unlawful downloading or copying of any part of SIS.

Article 31

Access to SIS data by the European Border and Coast Guard teams, teams of staff involved in return-related tasks, and members of the migration management support teams[49]

1. ~~In accordance with Article 40(8) of Regulation (EU) 2016/1624,~~ **T**he members of the European Border and Coast Guard teams or teams of staff involved in return-related tasks as well as the members of the migration management support teams**, set up in accordance with Articles 18, 20 and 32 of Regulation (EU) 2016/1624** shall, within their mandate **and provided that they are authorised to carry out checks in accordance with Article 29(1)**, have the right to access and search data entered in SIS ~~within their mandate~~. **Access to data entered in SIS shall not be extended to any other team members**.[50]

2. Members of the European Border and Coast Guard teams or teams of staff involved in return-related tasks as well as the members of the migration management support teams shall **exercise this right to** access and search data entered in SIS in accordance with paragraph 1 via the technical interface set up and maintained by the European Border and Coast Guard Agency as referred to in Article 32(2).

[49] It should be plural ("teams") in both instruments.
[50] Text moved from paragraph 5.

3. Where a search by a member of the European Border and Coast Guard teams or teams of staff involved in return-related tasks or by a member of the migration management support teams 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 may 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. Every instance of access and every search made by a member of the European Border and Coast Guard teams or teams of staff involved in return-related tasks or by a member of the migration management support teams shall be logged in accordance with the provisions of Article 12 and every use made by them of data accessed by them shall be ~~registered~~**logged**.

5. ~~Access to data entered in SIS shall be limited to a member of the European Border and Coast Guard teams or teams of staff involved in return-related tasks or by a member of the migration management support teams and shall not be extended to any other team member.~~[51]

6. **The European Border and Coast Guard teams or teams of staff involved in return-related tasks or members of the migration management support teams shall take** ~~M~~**m**easures to ensure security and confidentiality as provided for in Articles 10 and 11 ~~shall be adopted and applied~~.

Article 32

Access to SIS data by the European Border and Coast Guard Agency

1. The European Border and Coast Guard Agency shall, for the purpose of analysing the threats that may affect the functioning or security of the external borders, have the right to access and search data entered in SIS, in accordance with Articles 24 and 27.

2. For the purposes of Article 31(2) and paragraph~~s~~ 1 of this Article the European Border and Coast Guard Agency shall set up and maintain a technical interface which allows a direct connection to Central SIS.

[51] Merged with paragraph 1.

3. Where a search by the European Border and Coast Guard Agency reveals the existence of an alert in SIS, it shall inform the issuing Member State. **Wherever the existence of an alert is found by a member of the European Border and Coast Guard teams or teams of staff involved in return-related tasks or by a member of the migration management support teams, such member of staff shall immediately inform the officer of the hosting Member State so that the latter notifies the SIRENE Bureau about the hit.**

4. ~~The European Border and Coast Guard Agency shall, for the purpose of performing its tasks conferred on it by the Regulation establishing a European Travel Information and Authorisation System (ETIAS), have the right to access and verify data entered in SIS, in accordance with Articles 24 and 27.~~[52]

5. ~~Where a verification by the European Border and Coast Guard Agency for the purposes of paragraph 2 reveals the existence of an alert in SIS the procedure set out in Article 22 of Regulation establishing a European Travel Information and Authorisation System (ETIAS) applies.~~[53]

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

7. Every instance of access and every search made by the European Border and Coast Guard Agency shall be logged in accordance with the provisions of Article 12 and every use made of data accessed by the European Border and Coast Guard Agency shall be ~~registered~~**logged**.

---

[52] Moved to Article 32A(1).
[53] Moved to Article 32A(2).

8. Except where necessary to perform the tasks for the purposes of the Regulation establishing a European Travel Information and Authorisation System (ETIAS), no parts of SIS shall be connected to any computer system for data collection and processing operated by or at the European Border and Coast Guard Agency, nor shall the data contained in SIS to which the European Border and Coast Guard Agency has access be transferred to such a system. No part of SIS shall be downloaded. The logging of access and searches shall not be construed to be the downloading or copying of SIS data.

9. **The European Border and Coast Guard Agency shall take** ~~M~~**m**easures to ensure security and confidentiality as provided for in Articles 10 and 11 ~~shall be adopted and applied~~.

Article 32A *

Access to SIS data by the ETIAS Central Unit

1. The European Border and Coast Guard Agency shall, for the purpose of performing its tasks conferred on it by the Regulation establishing a European Travel Information and Authorisation System (ETIAS), have the right to access and search data entered in SIS, in accordance with Articles 24 and 27.

2. Where a verification by the European Border and Coast Guard Agency reveals the existence of an alert in SIS the procedure set out in Article 22 of Regulation establishing a European Travel Information and Authorisation System (ETIAS) applies.

Article 32B

Evaluation of the use of SIS by Europol and the European Border and Cost Guard Agency

The Commission shall carry out an evaluation of the operation and the use of SIS in accordance with this Regulation by Europol and the European Border and Cost Guard Agency at least every four years. To this end the Commission shall be assisted by a maximum of four experts designated by Member States. The Commission shall draw up an evaluation report in consultation with the designated Member State experts. Europol and the European Border and Cost Guard Agency respectively, shall be given the opportunity to make comments prior to the adoption of the report. The evaluation report shall be sent to the European Parliament and to the Council. The evaluation report shall be classified as EU RESTRICTED/RESTREINT UE in accordance with applicable security rules. Classification shall not preclude information being made available to the European Parliament.

Article 33
Scope of access

End-users, including Europol, ~~and~~ the European Border and Coast Guard Agency, **the members of the European Border and Coast Guard teams or teams of staff involved in return-related tasks as well as the members of the migration management support teams** may only access data which they require for the performance of their tasks.

Article 34
Retention period of alerts

1. Alerts entered in SIS pursuant to this Regulation shall be kept only for the time required to achieve the purposes for which they were entered.

2. A**n issuing** Member State ~~issuing an alert~~ shall, within five years of its entry into SIS, review the need to retain it.

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

4. In cases where it becomes clear to staff in the SIRENE Bureau, who are responsible for coordinating and verifying of data quality, that an alert on a person has achieved its purpose and should be deleted from SIS, the staff shall **bring this matter to the attention of** ~~notify~~ the authority which created the alert ~~to bring this issue to the attention of the authority~~. The authority shall have 30 ~~calendar~~ days from the receipt of this notification to indicate that the alert has been or shall be deleted or shall state reasons for the retention of the alert. If the 30-day period expires without such a reply**,** the alert shall**, where permissible under national law,** be deleted by the staff of the SIRENE Bureau[54]. SIRENE Bureaux shall report any recurring issues in this area to their national supervisory authority.

5. Within the review period, the **issuing** Member State ~~issuing the alert~~ may, following a comprehensive individual assessment, which shall be recorded, decide to keep the alert longer, should this prove necessary for the purposes for which the alert was issued. In such a case, paragraph 2 shall apply also to the extension. Any extension of an alert shall be communicated to CS-SIS.

6. Alerts shall automatically be erased after the review period referred to in paragraph 2 except where the **issuing** Member State ~~issuing the alert~~ has informed CS-SIS about the extension of the alert ~~to CS-SIS~~ pursuant to paragraph 5. CS-SIS shall automatically inform the Member States of the scheduled deletion of data from the system four months in advance.

7. Member States shall keep statistics about the number of alerts **f**or which the retention period has been extended in accordance with paragraph 5.

---

[54] AT, DE, ES, PL, SI and CH expressed concerns regarding the deletion of alerts by the SIRENE Bureaux.

Article 35
Deletion of alerts

1. Alerts on refusal of entry and stay pursuant to Article 24 shall be deleted when the decision on which the alert was entered has been withdrawn **or annuled** by the competent authority, where applicable following the consultation procedure referred to in Article 26.

2. Alerts relating to third-country nationals who are the subject of a restrictive measure as referred to in Article 27 shall be deleted when the measure implementing the travel ban has been terminated, suspended or annulled.

3. Alerts issued in respect of a person who has acquired citizenship of any State whose nationals are beneficiaries of the right of free movement ~~within~~ **under** the Union **Law** shall be deleted as soon as the issuing Member State becomes aware, or is informed pursuant to Article 38 that the person in question has acquired such citizenship.

CHAPTER VIII

GENERAL DATA PROCESSING RULES

Article 36
Processing of SIS data

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

2. Data may only be copied for technical purposes, provided that such copying is necessary in order for the authorities referred to in Article 29 to carry out a direct search. The provisions of this Regulation shall apply to such 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, as referred to in paragraph 2, which lead to off-line databases may be retained for a period not exceeding 48 hours. That period may be extended in the event of an emergency until the emergency comes to an end.

   Notwithstanding the first subparagraph, technical copies which lead to off-line 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 national supervisory authority, and ensure that the provisions of this Regulation, in particular those of Article 10, are applied in respect of those copies.

4. Access to data shall only be authorised within the limits of the competence of the national authorities referred to in Article 29 and to duly authorised staff.

5. Any processing of information contained in SIS for purposes other than those for which it was entered in SIS has to be linked with a specific case and justified by the need to prevent an imminent serious threat to public policy and public security, on serious grounds of national security or for the purposes of preventing a serious crime. Prior authorisation from the **issuing** Member State ~~issuing the alert~~ shall be obtained for this purpose.

6. Data concerning documents related to persons entered under Article 38(2)(j) and (k) of Regulation (EU) 2018/xxx may be used by the authorities referred to in Article 29(1)(d) **and (e)** in accordance with the laws of each Member State.

7. Any use of data which does not comply with paragraphs 1 to 6 shall be considered as misuse under the national law of each Member State.

8. Each Member State shall send to the Agency a list of its competent authorities which are authorised to search directly the data contained in SIS 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. The Agency shall ensure the annual publication of the list in the *Official Journal of the European Union*.

9. In so far as Union law does not lay down specific provisions, the law of each Member State shall apply to data entered in its N.SIS.

Article 37
SIS data and national files

1. Article 36(2) shall not prejudice 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 36(2) shall not prejudice the right of a Member State to keep in its national files data contained in a particular alert issued in SIS by that Member State.

Article 38
Information in case of non-execution of alert

If a requested action cannot be performed, the requested Member State shall immediately inform the **issuing** Member State ~~issuing the alert~~ **via the exchange of supplementary information**.

Article 39
Quality of the data processed in SIS

1. A**n issuing** Member State ~~issuing an alert~~ shall be responsible for ensuring that the data are accurate, up-to-date and entered in SIS lawfully.

2. Only the **issuing** Member State ~~issuing an alert~~ shall be authorised to modify, add to, correct, update or delete data which it has entered.

3. Where a Member State other than that which issued an alert 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 at the earliest opportunity and not later than 10 days after the said evidence has come to its attention. The issuing Member State shall check the communication and, if necessary, correct or delete the item in question without delay.

4. Where the Member States are unable to reach agreement within two months of the time when the evidence first came to light, as described in paragraph 3, the Member State which did not issue the alert shall submit the matter to the **European Data Protection Supervisor who shall, jointly with the** national supervisory authorities concerned ~~for a decision~~ **act as a mediator**.

5. The Member States shall exchange supplementary information where a person complains that he or she is not the person wanted by an alert. Where the outcome of the check shows that there are in fact two different persons the complainant shall be informed of the measures laid down in Article 42.

6. Where a person is already the subject of an alert in SIS, a Member State which enters a further alert shall reach agreement on the entry of the alert with the Member State which entered the first alert. The agreement shall be reached on the basis of the exchange of supplementary information.

Article 40
Security incidents

1. Any event that has or may have an impact on the security of SIS and may cause damage or loss to SIS data shall be considered to be a security incident, especially where 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 to ensure a quick, effective and proper response.

3. Member States shall notify the Commission, the Agency and the European Data Protection Supervisor of security incidents. The Agency shall notify the Commission and the European **D**~~d~~ata Protection Supervisor of security incidents.

4. Information regarding a security incident that has or may have an impact on the operation of SIS in a Member State or within the Agency or on the availability, integrity and confidentiality of the data entered or sent by other Member States, shall be provided to the Member States and reported in compliance with the incident management plan provided by the Agency.

Article 41
Distinguishing between persons with similar characteristics

Where it becomes apparent, when a new alert is entered, that there is already a person in SIS with the same identity description element, the following procedure shall apply:

(a) the SIRENE Bureau shall contact the requesting authority to clarify whether or not the alert is on the same person;

(b) where the cross-check reveals that the subject of the new alert and the person already in SIS are indeed one and the same, the SIRENE Bureau shall apply the procedure for entering multiple alerts as referred to in Article 39(6). Where the outcome of the 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 necessary elements to avoid any misidentifications.

Article 42
Additional data for the purpose of dealing with misused identities

1. Where confusion may arise between the person actually intended as the subject of an alert and a person whose identity has been misused, the issuing Member State shall, subject to that person's explicit consent, add data relating to the latter to the alert in order to avoid the negative consequences of misidentification.

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 actually intended as the subject of the alert;

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

3. For the purpose of this Article, only the following personal data **of the person whose identity has been misused** may be entered and further processed in SIS:

   (a) surname~~(s)~~

   (b) forename~~(s)~~,

   (c) name~~(s)~~ 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) ~~sex~~ **gender**;

(i) **photographs and** facial images;

(j) fingerprints;

(k) nationality**/nationalit**~~(~~ies~~)~~;

(l) the category of the person's ~~identity~~ **identification** document**s;**

(m) the country of issue of the person's ~~identity~~ **identification** document**s;**

(n) the number(s) of the person's ~~identity~~ **identification** document**s;**

(o) the date of issue of a person's ~~identity~~ **identification** document**s;**

(p) address of the ~~victim~~**person;**

(q) ~~victim~~**person**'s father's name**;**

(r) ~~victim~~**person**'s mother's name**.**

4. The technical rules necessary for entering and further processing the data referred to in paragraph 3 shall be established by means of implementing measures laid down and developed in accordance with the examination procedure referred to in Article 55(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 43
Links between alerts

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

2. The creation of a link shall not affect the specific action to be taken on the basis of each linked alert or the retention 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 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 technical rules for linking alerts shall be laid down and developed in accordance with the examination procedure defined in Article 55(2).

Article 44
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 not prejudice the right of a Member State to keep in national files data relating to a particular alert which that Member State has issued or to an alert in connection with which action has been taken on its territory. The period for which such data may be held in such files shall be governed by national law.

Article 45
Transfer of personal data to third parties

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

CHAPTER IX

DATA PROTECTION[55]

Article 46[*]

Applicable legislation

1. Regulation (EC) No 45/2001 shall apply to the processing of personal data by the Agency under this Regulation.

2. Regulation **(EU)** 2016/679 shall apply to the processing of personal data by the authorities referred to in Article 29 of this Regulation ~~provided that~~**. Where it does not apply,** national provisions transposing Directive (EU) 2016/680 **shall** ~~do not~~ apply.[56]

3. **National provisions transposing Directive (EU) 2016/680 shall apply f**or processing of data by competent national authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences of the execution of criminal penalties including the safeguarding against the prevention of threat to public security ~~national provisions transposing Directive (EU) 2016/680 shall apply~~.

*Article **46A***[57*]

Right of information

1. Third-country nationals who are the subject of an alert issued in accordance with this Regulation shall be informed in accordance with Articles ~~10~~**13** and ~~11~~**14** of ~~Directive 95/46/EC~~**Regulation (EU) 2016/679, or with Articles 12 and 13 of Directive (EU) 2016/680, respectively**. 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).

---

55 Articles 46 to 52 are also applicable to Returns by virtue of Article 13 of the Returns Proposal.

56 Reworded taking into account COM and CLS suggestions. Should be also reflected in recital 28.

57 Moved from Article 48.

2. This information shall not be provided:

(f) where:

i) the personal data have not been obtained from the third-country national in question;

and

ii) the provision of the information proves impossible or would involve a disproportionate effort;

(g) where the third country national in question already has the information;

(h) 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, investigation, detection and prosecution of criminal offences.

Article 47

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

1. The right of data subjects to have access to data relating to them entered in SIS and to have such data rectified or erased shall be exercised in accordance with the law of the Member State before which they invoke that right.

2. ~~If national law so provides, the national supervisory authority shall decide whether information is to be communicated and by what means.~~

3. A Member State other than that which has issued an alert may communicate information **to a data subject** concerning such data only ~~if it first gives the~~ **once each issuing** Member State ~~issuing the alert an~~ **gives** ~~opportunity to state~~ its ~~position~~ **consent**. This shall be done through the exchange of supplementary information.

4. A Member State shall take a decision not to communicate 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 ~~natural person~~ **data subject** concerned, in order **notably** 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.

5. **Following an application for access, rectification or erasure, t**he ~~person concerned~~ **data subject** shall be informed as soon as possible **from the date of application, as to the follow-up given to the exercise of these rights** ~~and in any event not later than 60 days from the date on which he applies for access or sooner if national law so provides~~.[58].

6. ~~The person concerned shall be informed about the follow-up given to the exercise of his rights of rectification and erasure as soon as possible and in any event not later than three months from the date on which he applies for rectification or erasure or sooner if national law so provides.~~[59]

[58] Paragraph merged with paragraph 6.
[59] Merged with paragraph 5.

Article 48[60*]

Right of information

~~1. Third-country nationals who are the subject of an alert issued in accordance with this Regulation shall be informed in accordance with Articles 10 and 11 of Directive 95/46/EC. 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).~~

~~2. This information shall not be provided:~~

~~(f) where:~~

~~i) the personal data have not been obtained from the third-country national in question;~~

~~and~~

~~ii) the provision of the information proves impossible or would involve a disproportionate effort;~~

~~(g) where the third country national in question already has the information;~~

~~(h) 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, investigation, detection and prosecution of criminal offences.~~

Article 49[*]

Remedies

1. Any person may bring an action before **any** competent authorit**ies, including** courts**,** under the law of any Member State to access, rectify, ~~delete~~ erase **or obtain** information or to obtain compensation in connection with an alert relating to him.

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 the provisions of Article 53.

60 Moved to Article 46A.

3. ~~In order to gain a consistent overview of the functioning of remedies~~ **T**he national ~~supervisory~~ authorities shall ~~be invited to develop a standard statistical system for~~ repor**t** annually on:

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

(b) the number of subject access requests submitted to the national 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 the erasure of unlawfully stored data to the data controller and the number of cases where the data were ~~corrected~~ **rectified** or ~~deleted~~ **erased**;

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

(e)[61] the number of cases which are heard before the courts;

(f) the number of cases where the court ruled in favour of the applicant in any aspect of the case; **and**

(g)[62] any observations on cases of mutual recognition of final decisions handed down by the courts or authorities of other Member States on alerts created by the ~~alert~~ issuing Member State.

The reports from the national supervisory authorities shall be forwarded to the cooperation mechanism set out in Article 52.

Article 50[*]

Supervision of N.SIS

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

---

61 SI, SK, NL suggested the deletion of this point. COM opposed.

62 NL suggested the deletion of this point.

2. The national supervisory authority 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 national supervisory authorit**y,** or the national supervisory authorit**y** shall directly order the audit from an independent data protection auditor. The national supervisory authority shall at all times retain control over and undertake the responsibilities of the independent auditor.

3. Member States shall ensure that their national supervisory authority has sufficient resources to fulfil the tasks entrusted to it under this Regulation.

*Article 51**

Supervision of the Agency

1. The European Data Protection Supervisor shall ensure that the personal data processing activities of the Agency are carried out in accordance with this Regulation. The duties and powers referred to in Articles 46 and 47 of Regulation (EC) No 45/2001 shall apply accordingly.

2. The European Data Protection Supervisor shall ~~ensure that~~ **carry out** an audit of the Agency's personal data processing activities ~~is carried out~~ in accordance with international auditing standards at least every four years. A report on that audit shall be sent to the European Parliament, the Council, the Agency, the Commission and the National Supervisory Authorities. The Agency shall be given an opportunity to make comments before the report is adopted.

Article 52[*]

Cooperation between national supervisory authorities

and the European Data Protection Supervisor

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

2. They shall, each acting within the scope of its 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 legal acts of the Union, 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 national supervisory authorities and the European Data Protection Supervisor shall meet at least twice a year as part of the European Data Protection Board established by Regulation (EU) 2016/679. ~~The costs and servicing of these meetings shall be borne by the Board established by Regulation (EU) 2016/679.~~ 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 by the Board established by Regulation (EU) 2016/679 to the European Parliament, the Council, and the Commission ~~every two years~~ **annually**.

CHAPTER X

LIABILITY <u>AND PENALTIES</u>[6364]

Article 53[*]

Liability

1. Each Member State shall be liable<u>, in accordance with the national law,</u> for any damage caused to a person through the use of N.SIS. This shall also apply to damage caused by the issuing Member State, where the latter entered factually inaccurate data or stored data unlawfully.

2. Where the Member State against which an action is brought is not the Member State issuing the alert, the latter shall be required to reimburse, on request, the sums paid out as compensation unless the use of data by the Member State requesting reimbursement infringes this Regulation.

3. Where any failure by a Member State to comply with its obligations under this Regulation causes damage to SIS, that Member State shall be held liable for the damage, unless and in so far as the Agency or ~~another~~ **<u>other</u>** Member States participating in SIS failed to take reasonable steps to prevent the damage from occurring or to minimise its impact.

<u>Article 53A</u>[*]

<u>Penalties</u>[65]

<u>Member States shall ensure that any misuse of data entered in SIS or any exchange of supplementary information contrary to this Regulation is subject to effective, proportionate and dissuasive penalties in accordance with national law.</u>

---

63 Article 53 is also applicable to the Returns Proposal by virtue of Article 13 of the Returns Proposal.

64 "And Penalties" has been added, due to the inclusion of new Article 53A.

65 New Article, similar to Article 65 of Decision 2007/533/JHA.

CHAPTER XI

FINAL PROVISIONS[66]

Article 54

Monitoring and statistics

1. The Agency 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 and statistics, the Agency shall have access to the necessary information relating to the processing operations performed in Central SIS.

3. The Agency shall produce, daily, monthly and annual statistics showing the number of records per category of alert, **in total, and for each Member State. The Agency shall also provide reports on** the annual 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**,** in total and for each Member State, including statistics on the consultation procedure referred to in Article 26. The statistics produced shall not contain any personal data. The annual statistical report shall be published.

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

66 Article 54 is also applicable to the Returns Proposal by virtue of Article 13 of the Returns Proposal.

5. The Agency shall provide the Member States, the Commission, Europol and the European Border and Coast Guard Agency with any statistical reports that it produces. In order to monitor the implementation of legal acts of the Union, **in particular the Council Regulation (EU) No 1053/2013[67],** the Commission shall be able to request the Agency to provide additional specific statistical reports, either regular or ad-hoc, on the performance or use of **Central** SIS and ~~SIRENE communication~~ **on the exchange of supplementary information.**

6. For the purpose of paragraphs 3**, 4 or** 5 of this Article and Article 15(5), the Agency shall establish, implement and host a central repository in its technical sites containing the ~~data~~ **reports** referred to in paragraph 3 of this Article and in Article 15(5) which shall not allow for the identification of individuals and shall allow the Commission and the agencies referred to in paragraph 5 to obtain bespoke reports and statistics. The Agency shall grant access to Member States, the Commission, Europol and the European Border and Coast Guard Agency to the central repository by means of secured access through the Communication Infrastructure with control of access and specific user profiles solely for the purpose of reporting and statistics.

~~Detailed rules on the operation of the central repository and the data protection and security rules applicable to the repository shall be laid down and developed by means of implementing measures adopted in accordance with the examination procedure referred to in Article 55(2).~~[68]

7. ~~Two years after SIS is brought into operation and~~ **E**very two years ~~thereafter~~, the Agency shall submit to the European Parliament and the Council a report on the technical functioning of Central SIS and the Communication Infrastructure, including the security thereof, and the bilateral and multilateral exchange of supplementary information between Member States.

---

[67] 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).

[68] Text moved to paragraph 9.

8. ~~Three years after SIS is brought into operation and~~ **E**very four years ~~thereafter~~, the Commission shall produce 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 Commission shall transmit the evaluation to the European Parliament and the Council.

9.[69] **The Commission shall adopt implementing acts to lay down and develop** detailed rules on the operation of the central repository **referred to in paragraph 6** ~~and the data protection~~ and security rules applicable to ~~the~~ **that** repository ~~shall be laid down and developed by means of~~**. Those** implementing ~~measures~~ **acts shall be** adopted in accordance with the examination procedure referred to in Article 55(2).

Article 55

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.

[69] Text moved from paragraph 6, *in fine*.

Article 56[*]

Amendments to Regulation (EU) 515/2014[70]

Regulation (EU) 515/2014[71] is amended as follows:

In Article 6, the following paragraph 6 is ~~inserted~~ **added**:

"6. **For the implementation of the Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006; and of the Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU,** ~~During the development phase~~ Member States shall receive an additional allocation of 36,8 million EUR to be distributed via a lump sum to their basic allocation and shall entirely devote this funding to SIS national systems to ensure their quick and effective upgrading in line with **that** ~~the implementation of Central SIS as required in~~ Regulation ~~(EU) 2018/…[*] and in Regulation (EU) 2018/…[**]~~

~~[*]Regulation on the establishment, operation and use of the Schengen Information System (SIS) in the field of police and judicial cooperation for criminal matters and in Regulation (OJ…..~~

~~[**]Regulation (EU 2018/…on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks and in Regulation (OJ …)~~".

[70] UK is not participating in this Regulation.

[71] Regulation (EU) No 515/2014 of the European Parliament and of the Council of 16 April 2014 establishing, as part of the Internal Security Fund, the instrument for financial support for external borders and visa (OJ L 150, 20.5.2014, p. 143).

Article 57[*]

Repeal

Upon the date of application of this Regulation the following legal acts are repealed:

Regulation (EC) No 1987/2006 on the establishment, operation and use of the second generation Schengen Information System **(SIS II)**;

Commission Decision 2010/261/EU of 4 May 2010 on the Security Plan for Central SIS II and the Communication Infrastructure.[72]

Article 25 of the Convention implementing the Schengen Agreement.[73]

Article 58[*]

Entry into force and applicability

1. This Regulation shall enter into force on the 20th day following its publication in the Official Journal of the European Union.

2. It shall apply from the date fixed by the Commission after:

   (a) the necessary implementing measures have been adopted;

   (b) Member States have notified the Commission ~~about~~ that they have made the necessary technical and legal arrangements to process SIS data and exchange supplementary information pursuant to this Regulation;

   (c) The Agency has notified the Commission ~~about~~ **of** the **successful** completion of all testing activities with regard **to** CS-SIS and the interaction between CS-SIS and N.SIS.

3. This Regulation shall be binding in its entirety and directly applicable to Member States in accordance with the Treaty on the Functioning of the European Union.

---

[72] Commission Decision 2010/261/EU of 4 May 2010 on the Security Plan for Central SIS II and the Communication Infrastructure (OJ L 112, 5.5.2010, p.31).

[73] OJ L 239, 22.9.2000, p. 19.