



Brussels, 5 September 2017
(OR. en)

**Interinstitutional File:
2016/0408 (COD)**

**9593/1/17
REV 1**

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
- Revised draft compromise text

Delegations will find attached a Presidency revised draft compromise text of the abovementioned proposal, taking into account the discussions held at the Working Party for Schengen Matters (Acquis) on 19 June 2017 and 3, 4, 5 and 26 July 2017 and the written comments subsequently sent by the delegations.

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

The Articles already agreed by the Working Party are not included in the present version (Articles 1, 2, 5 to 8, 11, 13, 14, 17, 19, 22, 31, 33, 34, 36 to 38, 43, 44, 46A, 49, 53A, 56 and 57). These Articles are set out in 9593/17.

Articles 9,10, 16, 18, 27A, 31, 32A, 32B, 41 and 58 have been agreed in substance, however their final wording still has to be confirmed by the Working Party. Those Articles are marked with an asterisk (*).

Article 4 is not included in the present version and will be discussed separately.

Changes to the original Commission proposal (as set out in 15813/16) are marked as follows: new or modified text is in **bold underlined**; deletions are in ~~strikethrough~~.

CHAPTER I

GENERAL PROVISIONS

Article 3

Definitions

1. For the purposes of this Regulation, the following definitions shall apply:
 - (a) ‘alert’ means a set of data, including, **where applicable**, biometric ~~data~~ **identifiers** as referred to in Article ~~27A2~~, 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;
- (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 **the occurrence of the following steps**:
- (1) a search is conducted by **an end-user**;
 - (2) the search reveals an alert ~~in~~ entered by another ~~a~~ Member State in SIS;
 - (3) data concerning the alert in SIS ~~matches~~ the search data;

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.

(3a) the match is confirmed by the end-user or, in the case of a match based on the comparison of biometric data, the match is confirmed in accordance with national procedures for biometric verification; 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

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).

(n) ‘~~dactylographic~~**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

(p) ‘terrorist offences’ means offences under national law referred to in Articles 1-4 of Framework Decision 2002/475/JHA of 13 June 2002⁵ **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 1030/2002⁷ 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) 2016/399⁸, with the exception of:

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).

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).**

- (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 1683/95⁹;**
- (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 265/2010¹⁰;**
- (s) 'threat to public health' means any disease with epidemic potential as defined by the International Health Regulations of the World Health Organization and other infectious diseases or contagious parasitic diseases if they are the subject of protection provisions applying to nationals of the Member States.**

*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 N₂-SIS with CS-SIS for the prompt and effective transmission of data. ~~These 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).~~¹¹

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).**

¹¹ Moved to paragraph 3.

2. Member States shall ensure, by means of the services provided by CS-SIS, that data stored in the national **or shared** 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 **or shared** 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.

3.¹² 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).

*Article 10**

Security – Member States

1. Each Member State shall, in relation to its N.SIS, adopt the necessary measures, including a security plan, a business continuity plan and a disaster recovery plan in order to:
 - (a) physically protect data, including by making contingency plans for the protection of critical infrastructure;
 - (b) deny unauthorised persons access to data-processing facilities used for processing personal data (facilities access control);
 - (c) prevent the unauthorised reading, copying, modification or removal of data media (data media control);
 - (d) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);

¹² Moved from paragraph 1, *in fine*.

- (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~~identifiers¹³ 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);
 - (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); **and**
 - (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.

¹³ Same wording as in Article 12(2) and (3) and Article 18(2) and (3).

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 of this Article and its applicability to the SIS shall be clearly identifiable in and ensured by that plan.**

CHAPTER II

RESPONSIBILITIES OF THE MEMBER STATES¹⁴

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**¹⁵ of both the competent authority and the person responsible for processing the data.

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

¹⁵ Same wording as in paragraph 3 and Article 10(1)(f).

3. If the search is carried out with dactylographic scopic data or facial image in accordance with Article ~~22~~⁸ 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}¹⁶ 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.

CHAPTER III

RESPONSIBILITIES OF THE AGENCY¹⁷

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}most appropriate technology, using a cost-benefit analysis, is used for Central SIS.

¹⁶ Same wording as in paragraph 2 and Article 10(1)(f).

¹⁷ Articles 15 –18 are also applicable to the proposal on Returns by virtue of Article 13 of the Returns Proposal.

[2. ¹⁸ The Agency shall also be responsible for the following **all** tasks relating to the Communication Infrastructure, **in particular**:-

- (a) supervision;
- (b) security;
- (c) the coordination of relations between the Member States and the provider;

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

- ~~(da) tasks relating to implementation of the budget;~~
- ~~(eb) acquisition and renewal; **and**~~
- ~~(fe) contractual matters.]~~

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**;
- (b) the maintenance and update of technical specifications for the exchange of supplementary information between SIRENE Bureaux and the Communication Infrastructure and managing the impact of technical changes where it affects both SIS and the exchange of supplementary information between SIRENE Bureaux.

¹⁸ The content and or the insertion of these provisions depend on the final text of the proposal for a Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011 (see 11164/17), and its date of entry into force.

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 States¹⁹. 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 and developed by means of implementing measures in accordance with the examination procedure referred to in Article 55(2).~~²⁰
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.

7.²¹ The Commission shall adopt implementing acts to set out the technical requirements of the Communication Infrastructure referred to in paragraph 2, and to establish the mechanism and procedures for the quality checks on the data in CS-SIS, referred to in paragraph 5, and for the interpretation of data quality compliance. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 55(2).

*Article 16**

*Security – **The Agency***

1. The Agency shall adopt the necessary measures²², including of a security plan, a business continuity plan and a disaster recovery plan for Central SIS and the Communication Infrastructure in order to:

¹⁹ eu-LISA would prefer more clear provisions on its competences regarding access to data.

²⁰ Text moved to new paragraph 7.

²¹ Text moved from paragraph 5.

²² eu-LISA asked to include in recital 40 a reference to Commission Decision 2017/46.

- (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);
- (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 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**²³, 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**²⁴ of the competent authority responsible for processing the data.
3. If the search is carried out with dactylographic~~ic~~**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 ~~the 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.

²³ Singular, as in Article 12(2).

²⁴ Same wording as in Articles 10(1)(f) and 12(2) and (3).

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.

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 Articles 24 and 24A7.
2. Any alert in SIS which includes~~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);

- (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 an **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 ~~43~~**43**;

- (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 illegally 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) of this Regulation~~);
- (s) the category of the person's identification documents;
- (t) the country of issue of the person's identification documents;
- (u) the number(s) of the person's identification documents;
- (v) the date of issue of the person's identification documents;
- (w) photographs and facial images;
- (x) dactyloscopic data;
- (y) a colour copy, **whenever possible in colour**, of the identification documents.
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).~~²⁵ These technical rules shall be similar for searches in CS-SIS, in national **or shared** 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**²⁶. ~~Exceptionally~~ ~~1 4 of Council Framework Decision 2002/475/JHA on combating terrorism~~²⁷, **Member States may refrain from creating the alert when it is likely to obstruct official or legal inquiries, investigations or procedures related to public or national security**²⁸.

²⁵ Redundant with previous paragraph.

²⁶ **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.**

²⁷ ~~Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ L 164, 22.6.2002, p. 3).~~

²⁸ DE, NL and UK entered a reservation on this paragraph.

Article 22²⁹

~~Specific rules for entering photographs, facial images and dactyloscographic 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

- 1³⁰. ~~Where available, a~~ All other data listed in Article 20(2) shall also be entered, **where available**.
- 2³¹. 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 24³²

Conditions for issuing alerts ~~for~~ 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.

²⁹ Moved to Article 27A.

³⁰ Moved from paragraph 2.

³¹ Moved from paragraph 1.

³² LU entered a scrutiny reservation.

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.
- 3.³³ 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 or the alert-issuing Member State has obtained clear indications that the third-country national 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 274A³⁴³⁵

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.

³³ BE and FR entered a scrutiny reservation on this paragraph.

³⁴ Moved from Article 27.

³⁵ LU entered a scrutiny reservation on this Article.

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 25³⁶

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 Council³⁷ **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~~ **implementation of** that Directive **or that agreement**.
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.

³⁶ LU entered a scrutiny reservation on this Article.

³⁷ OJ L 158, 30.4.2004, p.77.

CHAPTER Va

CONSULTATION PROCEDURE

Article 26³⁸

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, 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 seven³⁹ 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]⁴⁰.

³⁸ AT ~~and FR~~ **and LU** entered a scrutiny reservation on this Article.

³⁹ 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.

⁴⁰ Paragraph moved to new Article 26A.

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 an 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].⁴¹~~

⁴¹ Paragraph moved to new Article 26B.

~~2a.⁴² 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].⁴³~~

~~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~~

⁴² Based on Article 25(2) of the Convention Implementing the Schengen Agreement (CISA), (OJ L 239, 22.9.2000, p.19).

⁴³ Paragraph moved to new Article 26C.

⁴⁴ Paragraph moved to new Article 26D.

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.~~⁴⁵

Article 26A

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

Where a Member State considers granting or extending a residence permit or ~~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, the Member States involved shall consult each other, through the exchange of supplementary information, according to the following rules:

- (a) the granting Member State shall transmit a consultation request to the issuing Member State prior to granting or extending the residence permit or long-stay visa;
- (b) the issuing Member State shall reply to the consultation request within ~~seventen~~⁴⁶ calendar days;
- (c) the absence of a reply by the deadline referred to in point b) shall mean that the issuing Member State does not object to the granting of the residence permit or long-stay visa;
- (d) when making the relevant decision, the granting Member State shall take into account the interests of the issuing Member State and shall consider any threat to public policy or public security which the presence of the third country national in question on the territory of the Member States may pose;
- (e) the granting Member State shall notify the issuing Member State about its final decision; and

⁴⁵ Paragraph moved to new Article 26E

⁴⁶ AT, EL, ES, HU, LU, PT and SI considered seven days too short. HU entered a reservation on this delay.

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

Article 26B

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

Where a Member State **has taken a decision referred to in Article 24(1) and it** considers entering an alert for refusal of entry and stay **in respect of** ~~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~~ issued by another Member State, the involved Member States shall consult each other, ~~through the exchange of supplementary information,~~ according to the following rules:

- (a) the Member State that has taken the decision referred to in Article 24(1) shall transmit a consultation request to the granting Member State prior to entering the alert on refusal of entry and stay;**
- (b) the consultation request referred to in point a) shall contain substantial information about the reasons for the decision referred to in Article 24(1);**
- (c) the granting Member State shall consider on the basis of the information in the consultation request whether there are reasons for withdrawing the residence permit or long-stay visa;**
- (d) when making the relevant decision, the granting Member State shall take into account the interests of the Member State that has taken the decision referred to in Article 24(1) and shall consider any threat to public policy or public security which the presence of the third country national in question on the territory of the Member States may pose;**

- (e) the granting Member State shall notify the Member State that has taken the decision referred to in Article 24(1) within ⁴⁷seventen calendar days after the receipt of the consultation request about its final decision; the deadline may be extended upon the reasoned request of the granting Member State; and**
- (f) where the granting Member State notifies the Member State that has taken the decision referred to in Article 24(1) that it decides to maintain the residence permit or long-stay visa, the latter shall not enter the refusal of entry and stay alert in the SIS.**

Article 26C

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

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

- (a) the issuing Member State shall transmit a consultation request to the granting Member State;**
- (b) the consultation request referred to in point a) shall contain substantial information about the reasons for the refusal of entry and stay alert;**
- (c) the granting Member State shall consider on the basis of the information in the consultation request whether there are reasons for withdrawing the residence permit or long-stay visa;**

⁴⁷ AT, EL, ES, HU, LU, PT and SI considered seven days too short. HU entered a reservation on this delay.

- (d) when making the relevant decision, the granting Member State shall take into account the interests of the issuing Member State and shall consider any threat to public policy or public security which the presence of the third country national in question on the territory of the Member States may pose;**
- (e) the granting Member State shall notify the issuing Member State within seven calendar days after the receipt of the consultation request about its final decision; the deadline may be extended upon the reasoned request of the granting Member State; and**
- (f) where the granting Member State notifies the issuing Member State that it decides to maintain the residence permit or long-stay visa, the issuing Member State shall delete the alert for refusal of entry and stay.**

Article 26D

Consultation in case of a hit

Where a Member State has encountered~~In the event of a hit on an alert for refusal of entry and stay entered by a Member State in respect of~~one 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 **granted** the residence permit and the **by another** 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. If it is decided to maintain the residence permit, the alert shall be deleted. **the involved Member States shall consult each other, through the exchange of supplementary information, according to the following rules:**~~

- (a) the executing Member State shall inform the issuing Member State that has entered the alert ("the second Member State") about the situation;**
- (b) the issuing Member State shall transmit a consultation request to the granting Member State;**
- (c) the consultation request referred to in point b) shall contain substantial information about the reasons for the refusal of entry and stay alert;**

- (d) the granting Member State shall consider on the basis of the information in the consultation request whether there are reasons for withdrawing the residence permit or long-stay visa;**
- (e) when making the relevant decision, the granting Member State shall take into account the interests of the issuing Member State and shall consider any threat to public policy or public security which the presence of the third country national in question on the territory of the Member States may pose;**
- (f) the granting Member State shall notify the issuing Member State within ~~seventeen~~ calendar days after the receipt of the consultation request about its final decision; the deadline may be extended upon the reasoned request of the granting Member State;**
- (g) where the granting Member State notifies the issuing Member State that it decides to maintain the residence permit or long-stay visa, the issuing Member State shall delete the alert for refusal of entry and stay; and**
- (h) the issuing Member State shall notify the executing Member State about the final outcome of the consultation.**

Article 26E

Statistics⁴⁸

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 26A to Article 26D and the instances in which the consultation deadline was not met.**

⁴⁸ Moved from Article 26(4).

CHAPTER VI

SEARCH WITH BIOMETRIC DATA⁴⁹

Article 27A^{*50}

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).~~

Specific rules for entering photographs, facial images and dactyloscographic 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).

⁴⁹ Moved from before Article 28.

⁵⁰ Moved from Article 22.

CHAPTER VI

SEARCH WITH BIOMETRIC DATA⁵¹

Article 28

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

1. Photographs, facial images ~~and/or~~ dactyloscographic 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. Dactyloscographic data may also be used **in all cases** to identify a person. ~~Dactyloscographic data stored in SIS shall be used~~ **searched** ~~for identification purposes~~ ~~– If the identity of the person cannot be ascertained by other means,~~ **dactyloscopic data shall be used for identification purposes.**
3. Dactyloscographic data stored in SIS in relation to alerts issued under Articles 24 **and 24A7** may also be searched with complete or incomplete sets of fingerprints or palm prints discovered at the scenes of **serious crimes or terrorist offences** 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. **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.**⁵² Identification based on photographs or facial images shall ~~only~~ be used **subject to national law** ~~in the context of regular border crossing points where self service systems and automated border control systems are in use.~~

⁵¹ Moved to before Article 27A.

⁵² 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** Access 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 or national security** within the Member State concerned;⁵³
 - (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.⁵⁴

⁵³ In line with text of Article 3(7) of Directive 2016/680.

⁵⁴ 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 illegally 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;

- 1a. The right to access data entered in SIS and the right to search such data directly may also be exercised by national competent authorities responsible for naturalisation, in the performance of their tasks, as provided for in national law, and by their coordinating authorities.**
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(~~de~~). 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 30⁵⁵

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 **and may exchange and process supplementary information in accordance with the provisions of the SIRENE Manual laid down in Article 8**⁵⁶.
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 to exchange supplementary information, it shall inform the issuing Member State via the** channels defined by Regulation (EU) 2016/794.
 - 2a. **Europol may process the supplementary information that has been provided to it by Member States for the purposes of cross-checking, aimed at identifying connections or other relevant links and for strategic, thematic or operational analyses as defined in points (a), (b) and (c) of Article 18(2) of Regulation (EU) 2016/794 . Any processing by Europol of supplementary information shall be carried out in accordance with Regulation (EU) 2016/794.**
3. The use of information obtained from a search in ~~the~~-SIS **or from the processing of supplementary information** 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.~~⁵⁷

⁵⁵ DE entered a scrutiny reservation on this Article.

⁵⁶ SK entered a scrutiny reservation on this paragraph.

⁵⁷ In accordance with Regulation 2016/794, Europol may in any event request information related to mandated offences from the Member States. Paragraph 4 may therefore be considered superfluous.

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;
 - (aa) notwithstanding Article 31(1) of Regulation (EU) 2016/794, delete supplementary information containing personal data at the latest one year after the related alert has been deleted from SIS, unless the continued storage of the data is deemed necessary, on the basis of information that is more extensive than that possessed by the data provider, in order for Europol to perform its tasks. Europol shall inform the data provider of the continued storage of such data and present a justification of such continued storage;**
 - (b) limit access to data entered in SIS, **including supplementary information** to specifically authorised staff of Europol;
 - (c) adopt and apply measures provided for in Articles 10 and 11; **and**
 - (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 **and the exchange and processing of supplementary information.**
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 ~~shall~~^{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 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 24A7.
2. For the purposes of Article 31(2) and paragraphs 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.
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. ~~Whenever 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.~~⁵⁸

⁵⁸ Same provisions as in Article 31(3).

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.~~⁵⁹
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.~~⁶⁰
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**.
8. Except **in cases** where **paragraph 2 applies** ~~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 Mm** measures to ensure security and confidentiality as provided for in Articles 10 and 11 ~~shall be adopted and applied~~.

⁵⁹ Moved to Article 32A(1).

⁶⁰ Moved to Article 32A(2).

*[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 24A7.
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 Articles 18, 20A and 22 of Regulation establishing a European Travel Information and Authorisation System (ETIAS) applies.]⁶¹

*Article 32B**

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

1. 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 ~~five~~ years.
2. A team responsible for ~~To~~ this on-site evaluation shall consist of a maximum of two ~~and~~ the Commission representatives, ~~shall be assisted by a maximum of eight~~ ~~four~~ experts designated by Member States.
3. -The Commission shall draw up an evaluation report following each evaluation, in consultation with the designated Member State experts. The evaluation report shall be based on the findings of the on-site evaluation team and shall analyse the qualitative, quantitative, operational, administrative and organisational aspects of the operation and use of SIS, as appropriate, and shall list any deficiencies identified during the evaluation.

⁶¹ The content and or the insertion of these provisions depend on the final text of the proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624 (see 10017/17 + ADD 1), and its date of entry into force.

4. Europol and the European Border and Coast Guard Agency respectively, shall be given the opportunity to make comments prior to the adoption of the report.
5. 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.
6. In light of the findings and the assessments contained in that evaluation report, the Commission shall draft recommendations for remedial action aimed at addressing any deficiencies identified during the evaluation and give an indication of the priorities for implementing them, as well as, where appropriate, examples of good practices.
7. Following an evaluation, Europol, Eurojust and the European Border and Coast Guard Agency shall provide the Commission with an action plan to remedy any deficiencies identified in the evaluation report and shall thereafter continue to report on progress every three months until the action plan is fully implemented.

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 **intended to prevent entry into or transit through the territory of Member States** as referred to in ~~Article 27~~ shall be deleted when the **restrictive** 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 39

Quality of the data processed in SIS

1. An **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 **or to the supplementary information** 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, **Europol, Eurojust and the European Border and Coast Guard Agency** shall notify the Commission, the Agency and the European Data Protection Supervisor of security incidents. The Agency shall notify the Commission and the European Data 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 **or supplementary information exchanged** by other Member States, shall be provided to **all** 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; **and**
- (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) **dactyloscopic data**~~fingerprints~~;
 - (k) nationality/**nationalit**(ies);
 - (l) the category of the person's ~~identity~~**identification** documents;
 - (m) the country of issue of the person's ~~identity~~**identification** documents;
 - (n) the number(s) of the person's ~~identity~~**identification** documents;
 - (o) the date of issue of a person's ~~identity~~**identification** documents;
 - (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 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 PROTECTION⁶²

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.⁶³
3. **National provisions transposing Directive (EU) 2016/680 shall apply** for 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 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.~~

⁶² Articles 46 to 52 are also applicable to Returns by virtue of Article 13 of the Returns Proposal.

⁶³ Reworded taking into account COM and CLS suggestions. Should be also reflected in recital 28.

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, the 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.~~ ⁶⁴.
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.~~ ⁶⁵

⁶⁴ Paragraph merged with paragraph 6.

⁶⁵ Merged with paragraph 5.

CHAPTER XI

FINAL PROVISIONS⁶⁶

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 annual 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 1053/2013⁶⁷**, 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~~ **Every** 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~~ **Every** 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.

*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.

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

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.
-