Council of the European Union

Brussels, 16 October 2017
(OR. en)

13163/17

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

**LIMITE**

**SIRIS 163**
**FRONT 422**
**SCHENGEN 65**
**COMIX 678**
**CODEC 1581**

**NOTE**

| | |
|---|---|
| From: | Presidency |
| To: | Delegations |
| Subject: | 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<br>- draft compromise text |

Delegations will find in the Annex a draft consolidated compromise version of the above-mentioned Regulation for meeting of the JHA Counsellors scheduled for 20 October 2017.

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

**ANNEX**

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 (EC) No 1987/2006**

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty the Functioning of the of the European Union, and in particular Articles 77(2)(b) and (d) and 79(2)(c) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Acting in accordance with the ordinary legislative procedure,

Whereas[1]:

(1) The Schengen Information System (SIS) constitutes an essential tool for the application of the provisions of the Schengen acquis as integrated into the framework of the European Union. SIS is one of the major compensatory measures **and law enforcement tools** contributing to maintaining a high level of security within the area of freedom, security and justice of the European Union by supporting operational cooperation between border guards, police, customs and other ~~law enforcement authorities, judicial~~ authorities **responsible for the prevention, the detection, investigation or prosecution of criminal ofences or the execution of** ~~in~~ criminal **penalties**~~matters~~ and immigration authorities. [2]

[1] **Scrutiny reservation pending from DE on the recitals.**
[2] **Wording in line with Article 43(1)(c).**

(2) SIS was **initially** set up pursuant to the provisions of Title IV of the Convention of 19 June 1990 implementing the Schengen Agreement of 14 June 1985 between the governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders[3] (the Schengen Convention). The development of the second generation of SIS (SIS II) was entrusted to the Commission pursuant to Council Regulation (EC) No 2424/2001[4] and Council Decision 2001/886/JHA (SIS)[5] and it was established by Regulation (EC) No 1987/2006[6] as well as by Council Decision 2007/533/JHA[7]. SIS II replaced SIS as created pursuant to the Schengen Convention.

(3) Three years after SIS II was brought into operation, the Commission carried out an evaluation of the system in accordance with Articles 24(5), 43(5) and 50(5) of Regulation (EC) No 1987/2006 and Articles 59 and 65(5) of Decision 2007/533/JHA. The evaluation report and the related Staff Working Document were adopted on 21 December 2016[8]. The recommendations set out in those documents **are** ~~should be~~ reflected, as appropriate, in this Regulation.

---

3 OJ L 239, 22.9.2000, p. 19. Convention as amended by Regulation (EC) No 1160/2005 of the European Parliament and of the Council (OJ L 191, 22.7.2005, p. 18).

4 OJ L 328, 13.12.2001, p. 4.

5 Council Decision 2001/886/JHA of 6 December 2001 on the development of the second generation Schengen Information System (SIS II ) (OJ L 328, 13.12.2001, p. 1).

6 Regulation (EC) No 1987/2006 of 20 December 2006 of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information system (SIS II) (OJ L181, 28.12.2006, p. 4).

7 Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information system (SIS II) (OJ L 205, 7.8.2007, p.63).

8 Report to the European Parliament and Council on the evaluation of the second generation Schengen Information System (SIS II) in accordance with Art. 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and Art. 59 (3) and 66(5) of Decision 2007/533/JHA and an accompanying Staff Working Document. **(OJ…).**

(4) This Regulation constitutes the necessary legislative basis for governing SIS in respect of matters falling within the scope of Chapter 2 of Title V of the Treaty on Functioning of the European Union. Regulation (EU) 2018/… 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[9] constitutes the necessary legislative basis for governing SIS in respect of matters falling within the scope of Chapters 4 and 5 of Title V of the Treaty on Functioning of the European Union.

(5) The fact that the legislative basis necessary for governing SIS consists of separate instruments does not affect the principle that SIS constitutes one single information system that should operate as such **and that should include a single network of SIRENE Bureaux for ensuring the exchange of supplementary information**. Certain provisions of these instruments should therefore be identical.

(6) It is necessary to specify the objectives of SIS, **certain elements of** its technical architecture**,** ~~, and~~ its financing, to lay down rules concerning its end-to-end operation and use and to define responsibilities, the categories of data to be entered into the system, the purposes for which the data are to be entered **and processed**, the criteria for their entry, the authorities authorised to access the data, the use of biometric ~~identifiers~~**data** and further rules on data processing.

[9] Regulation (EU) 2018/…

(7) SIS includes a central system (Central SIS) and national systems **that may contain** ~~with~~ a full or partial copy of the SIS database **which may be shared by two or more Member States**. Considering that SIS is the most important information exchange instrument in Europe **for ensuring security and an effective migration management**, it is necessary to ensure its uninterrupted operation at central as well as at national level. **The availability of the SIS should be subject to close monitoring at central and Member State level and any incident of unavailability for the end-users should be registered and reported to stakeholders at national and EU level.** ~~Therefore e~~**E**ach Member State should ~~establish a partial or full copy of the SIS database and should~~ set up **a** ~~its~~ backup **for its national** system. **Member States should also ensure uninterrupted connectivity with Central SIS by having duplicated, physically and geographically separated connection points. Central SIS should be operated to ensure its functioning 24 hours a day, 7 days a week. In order to achieve this, an active-active solution may be used.**

**(7A) The technical architecture of the SIS may be subject to change following technical developments while ensuring the highest degree of availability for end-users at central and national level, the fulfilment of all applicable data protection requirements, the services necessary for the entry and processing of SIS data including searches in the SIS database as well as an encrypted virtual communication network dedicated to SIS data and the exchange of data between SIRENE Bureaux. The changes should be decided based upon an impact and cost assessment and will be communicated to the European Parliament and the Council.**

(8) It is necessary to maintain a manual setting out the detailed rules for the exchange of ~~certain~~ supplementary information concerning the action called for by alerts. National authorities in each Member State (the SIRENE Bureaux), should ensure the exchange of this information.

(9) In order to maintain the efficient exchange of supplementary information ~~concerning the action to be taken specified in the alerts~~, it is appropriate to reinforce the functioning of the SIRENE Bureaux by specifying the requirements concerning **the** available resources, user training and the response time to the inquiries received from other SIRENE Bureaux.

(10) The operational management of the central components of SIS are exercised by the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice[10] (the Agency). In order to enable the Agency to dedicate the necessary financial and personal resources covering all aspects of the operational management of Central SIS **and the communication infrastructure**, this Regulation should set out its tasks in detail, in particular with regard to the technical aspects of the exchange of supplementary information.

(11) Without prejudice to the **primary** responsibility of Member States for the accuracy of data entered into SIS**, and the role of the SIRENE Bureaux as quality coordinators,** the Agency should become responsible for reinforcing data quality by introducing a central data quality monitoring tool, and for providing reports at regular intervals to **the Commission and** the Member States.

(12) In order to allow better monitoring of the use of SIS to analyse trends concerning migratory pressure and border management, the Agency should be able to develop a state-of-the-art capability for statistical reporting to the Member States, the Commission, Europol and the European Border and Cost Guard Agency without jeopardising data integrity. Therefore, a central statistical repository should be established. Any statistic produced should not contain personal data. **Member States should communicate statistics concerning the right of access, rectification of inaccurate data and erasure of unlawfully stored data to the cooperation mechanism.**

---

**10** Established by Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 286, 1.11.2011, p.1).

(13) SIS should contain further data categories to allow end-users to take informed decisions based upon an alert without losing time. Therefore alerts for the purpose of refusal of entry and stay should hold information concerning the decision on which the alert is based. Furthermore, in order to facilitate identification and detect multiple identities, the alert should include a reference to the personal identification document or number and a copy of such document~~,~~ where available.

**(13A) Where available, all the relevant data, in particular the forename, should be inserted when creating an alert, in order to minimize the risk of false hits and unnecessary operational activities.**

(14) SIS should not store any data used for search with the exception of keeping logs to verify if the search is lawful, for monitoring the lawfulness of data processing, for self-monitoring and for ensuring the proper functioning of N.SIS, as well as for data integrity and security.

(15) SIS should permit the processing of biometric data in order to assist in the reliable identification of the individuals concerned. In the same perspective, SIS should also allow for the processing of data concerning individuals whose identity has been misused (in order to avoid inconveniences caused by their misidentification), subject to suitable safeguards; in particular with the consent of the individual concerned and a strict limitation of the purposes for which such data can be lawfully processed.

(16) Member States should make the necessary technical arrangement so that each time the end-users are entitled to carry out a search in a national police or immigration database they also search SIS in parallel in accordance with Article 4 of Directive (EU) 2016/680 of the European Parliament and of the Council[11]. This should ensure that SIS functions as the main compensatory measure in the area without internal border controls and better address the cross-border dimension of criminality and the mobility of criminals.

(17) This Regulation should set out the conditions for use of ~~dactylographic~~**dactyloscopic** data and facial images for identification purposes. The use of facial images for identification purposes in SIS should **in particular**~~also~~ help **to** ensure consistency in border control procedures where **the** identification and the verification of identity are required by the use of dactylo**scopic**~~graphic data~~ and facial images. Searching with ~~dactylographic~~**dactyloscopic** data should be mandatory if there is any doubt concerning the identity of a person. ~~Facial images for identification purposes should only be used in the context of regular border controls in self-service kiosks and electronic gates.~~

[11] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 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 (OJ L 119, 4.5.2016, p. 89).

(18) Fingerprints **or palm prints** found at a crime scene should be allowed to be checked against the dactylo**scopic**~~graphic~~ data stored in SIS if it can be established to a high degree of probability that they belong to the perpetrator of the serious crime or terrorist offence. **Particular attention should be given to the establishement of quality standards appliable to the storage of biometric data, including latent dactyloscopic data.** Serious crime should be the offences listed in Council Framework Decision 2002/584/JHA[12] and 'terrorist offence' should be offences ~~under national law~~ **corresponding or equivalent to one of the offences** referred to in **Directive (EU) 2017/541**[13] ~~Council Framework Decision 2002/475/JHA~~[14].

**(18A) It should be possible in all cases to identify a person by using dactyloscopic data. Wherever the identity of the person cannot be ascertained by any other means, dactyloscopic data should be used to attempt to ascertain the identity.**

(19) It should be possible for Member States to establish links between alerts in SIS. The establishment by a Member State of links between two or more alerts should have no impact on the action to be taken, their retention period or the access rights to the alerts.

---

12 Council Framework Decision (2002/584/JHA) of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (0J L 190, 18.07.2002, p. 1).

13 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.

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

(20) A greater level of effectiveness, harmonisation and consistency can be achieved by making it mandatory to enter in SIS all entry bans issued by the competent authorities of the Member States in accordance with procedures respecting Directive 2008/115/EC[15], and by setting common rules for entering such alerts following the return of the illegally staying third country national. Member States should take all necessary measures to ensure that no time-gap exist between the moment in which the third-country national leaves the Schengen area and the activation of the alert in SIS. This should ensure the successful enforcement of entry bans at external border crossing points, effectively preventing re-entry into the Schengen area.

(21) This Regulation should set mandatory rules for the consultation **and notification** of national authorities in case a third country national holds or may obtain a valid residence permit or ~~other authorisation or right to stay~~ **long-stay visa** granted in one Member State, and another Member State intends to issue or already entered an alert for refusal of entry and stay to the third country national concerned. Such situations create serious uncertainties for border guards, police and immigration authorities. Therefore, it is appropriate to provide for a mandatory timeframe for rapid consultation with a definite result in order to avoid that persons representing a threat may enter to the Schengen area. **Furthermore statistics on the reasons for which the deadline was not met should be collected.**

**(21A) When deleting an alert in SIS following a consultation between Member States, the issuing Member State may keep the third-country national concerned on their national list of alerts.**

[15] Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals (OJ L 348, 24.12.2008, p. 98).

(22) This Regulation should be without prejudice to the application of Directive 2004/38[16].

(23) Alerts should not be kept in SIS longer than the time required to fulfil the purposes for which they were issued. In order **to** reduce the administrative burden on the **different** authorities involved in processing data on individuals for different purposes, it is appropriate to align the maximum retention period of refusal of entry and stay alerts with the possible maximum length of entry bans issued in accordance with procedures respecting Directive 2008/115/EC. Therefore, the retention period for alerts on persons should be a maximum of five years. As a general principle, alerts on persons should be automatically deleted from SIS after a period of five years. Decisions to keep alerts on persons should be based on a comprehensive individual assessment. Member States should review alerts on persons within the defined period and keep statistics about the number of alerts on persons for which the retention period has been extended.

(24) Entering and extending the expiry date of a SIS alert should be subject to the necessary proportionality requirement, examining whether a concrete case is adequate, relevant and important enough to insert an alert in SIS. In cases of offences pursuant Articles ~~1, 2,~~ 3 **to**~~and~~ **1**4 **Directive (EU) 2017/541,** ~~of Council Framework Decision 2002/475/JHA on combating terrorism~~[17] an alert should ~~always~~ be created on third country nationals for the purposes of refusal of entry and stay taking into account the high level of threat and overall negative impact such activity may result in. **Exceptionally, 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.**

---

16 Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States (OJ L 158, 30.4.2004, p.77).

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

(25) The integrity of SIS data is of primary importance. Therefore, appropriate safeguards should be provided to process SIS data at central as well as at national level to ensure the end-to-end security of data. The authorities involved in ~~the~~ data processing should be bound by the security requirements of this Regulation and be subject to a uniform incident reporting procedure.

(26) Data processed in SIS in application of this Regulation should not be transferred or made available to third countries or to international organisations. ~~However, it is appropriate to strengthen cooperation between the European Union and Interpol by promoting an efficient exchange of passport data. Where personal data is transferred from SIS to Interpol, these personal data should be subject to an adequate level of protection, guaranteed by an agreement, providing strict safeguards and conditions.~~

(27) To enhance the efficiency of the work of the immigration authorities when deciding about the right of third country nationals to enter and stay in the territories of the Member States, as well as about the return of illegally staying third country nationals, it is appropriate to grant them access to SIS under this Regulation.

(28) Regulation (EU) 2016/679[18] should apply to the processing of personal data under this Regulation by Member States authorities when Directive (EU) 2016/680[19] does not apply. Regulation (EC) No 45/2001 of the European Parliament and of the Council[20] should apply to the processing of personal data by the institutions and bodies of the Union**, in particular the Agency and the European Border and Cost Guard Agency,** when carrying out their responsibilities under this Regulation. The provisions of Directive (EU) 2016/680, Regulation (EU) 2016/679 and Regulation (EC) No 45/2001 should be further specified in this Regulation where necessary. With regard to processing of personal data by Europol, Regulation (EU) 2016/794 on the European Union Agency for Law Enforcement cooperation[21] (Europol Regulation) applies.

(29) In so far as confidentiality is concerned, the relevant provisions of the Staff Regulations of officials and the Conditions of Employment of other servants of the European Union should apply to officials or other servants employed and working in connection with SIS.

(30) Both the Member States and the Agency should maintain security plans in order to facilitate the implementation of security obligations and should cooperate with each other in order to address security issues from a common perspective.

---

18 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation (OJ L 119, 4.5.2016, p. 1).

19 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 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 (OJ L 119, 4.5.2016, p.89).

20 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p.1).

21 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 25.5.2016, p. 53).

(31) The national independent supervisory authorities should monitor the lawfulness of the processing of personal data by the Member States in relation to this Regulation. The rights of data subjects for access, rectification and erasure of their personal data stored in SIS, and subsequent remedies before national courts as well as the mutual recognition of judgments should be set out. Therefore, it is appropriate to require annual statistics from Member States.

(32) The supervisory authorities should ensure that an audit of the data processing operations in **their**~~its~~ N.SIS is carried out in accordance with international auditing standards at least every four years. The audit should either be carried out by the supervisory authorities, or the national supervisory authorities should directly order the audit from an independent data protection auditor. The independent auditor should remain under the control and responsibility of the national supervisory authority or authorities which therefore should order the audit itself and provide a clearly defined purpose, scope and methodology of the audit as well as guidance and supervision concerning the audit and its final results.

(33) Regulation (EU) 2016/794 (Europol Regulation) provides that Europol supports and strengthens actions carried out by the competent authorities of Member States and their cooperation in combating terrorism and serious crime and provides analysis and threat assessments. In order to facilitate Europol in carrying out its tasks, in particular within the European Migrant Smuggling Centre, it is appropriate to allow Europol access to the alert categories defined in this Regulation. Europol's European Migrant Smuggling Centre plays a major strategic role in countering the facilitation of irregular migration, it should obtain access to alerts on persons who are refused entry and stay within the territory of a Member State either on criminal grounds or because of non-compliance with entry and stay conditions.

(34) In order to bridge the gap in information sharing on terrorism, in particular on foreign terrorist fighters – where monitoring of their movement is crucial – Member States should share information on terrorism-related activity with Europol **when** ~~in parallel to~~ introducing an alert in SIS, as well as hits and related information. **This information sharing should be carried out by the exchange of supplementary information with Europol on corresponding alerts. For this purpose Europol should set up a connection with the SIRENE communication infrastructure.** This should allow Europol's European Counter Terrorism Centre to verify if there is any additional contextual information available in Europol's databases and to deliver high quality analysis contributing to disrupting terrorism networks and, where possible, preventing their attacks.

(35) It is also necessary to set out clear rules for Europol on the processing and downloading of SIS data to allow the most comprehensive use of SIS provided that data protection standards are respected as provided in this Regulation and Regulation (EU) 2016/794. In cases where searches carried out by Europol in SIS reveal the existence of an alert issued by a Member State, Europol cannot take the required action. Therefore it should inform the Member State concerned **via the exchange of supplementary information with SIRENE Bureau** allowing it to follow up the case.

(36) Regulation (EU) 2016/1624 of the European Parliament and of the Council[22] provides for the **purpose**~~purposes~~ of this Regulation, that the host Member State is to authorise the members of the European Border and Coast Guard teams or teams of staff involved in return-related tasks, deployed by the European Border and Coast Guard Agency, to consult European databases, where this consultation is necessary for fulfilling operational aims specified in the operational plan on border checks, border surveillance and return. Other relevant Union agencies, in particular the European Asylum Support Office and Europol, may also deploy experts as part of migration management support teams, who are not members of the staff of those Union agencies. The objective of the deployment of the European Border and Coast Guard teams, teams of staff involved in return-related tasks and the migration management support teams is to provide for technical and operational reinforcement to the requesting Member States, especially to those facing disproportionate migratory challenges. Fulfilling the tasks assigned to the European Border and Coast Guard teams, teams of staff involved in return-related tasks and ~~to~~ the migration management support teams, necessitates access to SIS via a technical interface of the European Border and Coast Guard Agency connecting to Central SIS. In cases where searches carried out by the team or the teams of staff in SIS reveal the existence of an alert issued by a Member State, the member of the team or the staff cannot take the required action unless authorised to do so by the host Member State. Therefore it should inform the **host** Member States ~~concerned~~ allowing for follow up of the case. **The host Member State should notify the hit to the issuing Member State through the exchange of supplementary information.**

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

(37) In accordance with Regulation (EU) 2016/1624 the European Border and Coast Guard Agency ~~shall~~ prepare**s** risk analyses. These risk analyses ~~shall~~ cover all aspects relevant to European integrated border management, notably threats that may affect the functioning or security of the external borders. Alerts introduced in the SIS in accordance with this Regulation, notably the alerts on refusal of entry and stay are relevant information for assessing possible threats that may affect the external borders and should thus be available in view of the risk analysis which must be prepared by the European Border and Coast Guard Agency. Fulfilling the tasks assigned to the European Border and Coast Guard Agency in relation to risk analysis, necessitates access to SIS. Furthermore, in accordance with Commission proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS)[23] the ETIAS Central Unit of the European Border and Coast Guard Agency will perform verifications in SIS via ETIAS in order to perform the assessment of the applications for travel authorisation which require, inter alia, to ascertain if the third country national applying for a travel authorisation is subject of a SIS alert. To this end the ETIAS Central Unit within **the** European Border and Coast Guard Agency should also have access to SIS to the extent necessary to carry out its mandate, namely to all alert categories on third country nationals in respect of whom an alert has been issued for the purposes of entry and stay, and those who are subject to restrictive measure intended to prevent entry or transit through Member States.

(38) Owing to their technical nature, level of detail and need for regular updating, certain aspects of SIS cannot be covered exhaustively by the provisions of this Regulation. These include, for example, technical rules on entering data, updating, deleting and searching data, data quality and search rules related to biometric ~~identifiers~~**data**, rules on compatibility and priority of alerts, ~~the adding of flags,~~ links between alerts, setting the expiry date of alerts within the maximum time limit and the exchange of supplementary information. Implementing powers in respect of those aspects should therefore be conferred to the Commission. Technical rules on searching alerts should take into account the smooth operation of national applications.

---

**23** COM (2016)731 final.

(39) In order to ensure uniform conditions for the implementation of this Regulation**,** implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with **Article 5 of** Regulation (EU) No 182/2011[24]. The procedure for adopting implementing measures under this Regulation and Regulation (EU) 2018/xxx (police and judicial cooperation) should be the same.

(40) In order to ensure transparency, a report on the technical functioning of Central SIS and the communication infrastructure, including its security, and on the **bilateral and multilateral** exchange of supplementary information should be produced every two years by the Agency. An overall evaluation should be issued by the Commission every four years.

(41) Since the objectives of this Regulation, namely the establishment and regulation of a joint information system and the exchange of related supplementary information, cannot, by **its**~~their~~ very nature, be sufficiently achieved by the Member States and can therefore be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity, as set out in Article 5 of the Treaty of the European Union. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.

(42) This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. In particular, this Regulation seeks to ensure a safe environment for all persons residing on the territory of the European Union and a protection of irregular migrants from exploitation and trafficking by allowing their identification while fully respecting the protection of personal data.

---

[24] Regulation (EU) No182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

(43) In accordance with Articles 1 and 2 of Protocol No 22 on the Position of Denmark annexed to the Treaty on European Union and to the **Functioning of the European Union**~~TFEU~~, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Given that this Regulation builds upon the Schengen *acquis*, Denmark shall, in accordance with Article 4 of that Protocol, decide within a period of six months after the Council has decided on this Regulation whether it will implement it in its national law.

(44) This Regulation constitutes a development of provisions of the Schengen *acquis* in which the United Kingdom does not take part, in accordance with Council Decision 2000/365/EC[25]; the United Kingdom is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(45) This Regulation constitutes a development of the provisions of the Schengen *acquis* in which Ireland does not take part, in accordance with Council Decision 2002/192/EC[26]; Ireland is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(46) As regards Iceland and Norway, this Regulation constitutes a development of provisions of the Schengen acquis within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis[27], which fall within the area referred to in Article 1, point G of Council Decision 1999/437/EC[28]on certain arrangements for the application of that Agreement.

---

25 OJ L 131, 1.6.2000, p. 43.
26 OJ L 64, 7.3.2002, p.20.
27 OJ L 176, 10.7.1999, p.36.
28 OJ L 176, 10.7.1999, p.31.

(47) As regards Switzerland, this Regulation constitutes a development of provisions of the Schengen acquis within the meaning of the Agreement signed between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis, which fall within the area referred to in Article 1, point G, of Decision 1999/437/EC read in conjunction with Article ~~4(1)~~**3** of Council Decision~~s~~ ~~2004/849/EC[29] and 2004/860/EC[30]~~ **2008/146/EC**[31].

~~[29] Council Decision 2004/849/EC of 25 October 2004 on the signing, on behalf of the European Union, and on the provisional application of certain provisions of the Agreement between the European Union, the European Community and the Swiss Confederation concerning the Swiss Confederation's association with the implementation, application and development of the Schengen acquis (OJ L 368, 15.12.2004, p. 26).~~

~~[30] Council Decision 2004/860/EC of 25 October 2004 on the signing, on behalf of the European Community, and on the provisional application of certain provisions of the Agreement between the European Union, the European Community and the Swiss Confederation, concerning the Swiss Confederation's association with the implementation, application and development of the Schengen acquis (OJ L 370, 17.12.2004, p. 78).~~

[31] Council Decision 2008/146/EC of 28 January 2008 on the conclusion, on behalf of the European Community, of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis (OJ L 53, 27.2.2008, p. 1).

(48) As regards Liechtenstein, this Decision constitutes a development of the provisions of the Schengen acquis within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis[32], which fall within the area referred to in Article 1, point G, of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/349/EU[33] and Article 3 of Council Decision 2011/350/EU[34].

(49) As regards Bulgaria**,** ~~and~~ Romania **and Croatia**, this Regulation constitutes an act building upon, or otherwise relating to, the Schengen acquis within**, respectively,** the meaning of Article Article 4(2) of the 2005 Act of Accession **and Article 4(2) of the 2011 Act of Accession, and** should be read in conjunction with**, respectively,** Council Decision 2010/365/EU on the application of the provisions of the Schengen acquis relating to the Schengen Information System in the Republic of Bulgaria and Romania[35] **and Council Decision 2017/733 on the application of the provisions of the Schengen acquis relating to the Schengen Information System in the Republic of Croatia.**[36]

---

32 OJ L 160, 18.6.2011, p. 21.

33 Council Decision 2011/349/EU of 7 March 2011 on the conclusion on behalf of the European Union of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis,* relating in particular to judicial cooperation in criminal matters and police cooperation (OJ L 160, 18.6.2011, p. 1).

34 Council Decision 2011/350/EU of 7 March 2011 on the conclusion, on behalf of the European Union, of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*, relating to the abolition of checks at internal borders and movement of persons (OJ L 160, 18.6.2011, p. 19).

35 OJ L 166, 1.7.2010, p. 17.

36 OJ L 108, 26.4.20017, p. 31.

(50) Concerning Cyprus ~~and Croatia~~ this Regulation constitutes an act building upon, or otherwise relating to, the Schengen acquis within~~, respectively,~~ the meaning of Article 3(2) of the 2003 Act of Accession ~~and Article 4(2) of the 2011 Act of Accession~~.

(51) The estimated costs of the upgrade of the SIS national systems and of the implementation of the new functionalities, envisaged in this Regulation are lower than the remaining amount in the budget line for Smart Borders in Regulation (EU) No 515/2014 of the European Parliament and the Council[37]. Therefore, this Regulation should re-allocate the amount, attributed for developing IT systems supporting the management of migration flows across the external borders.in accordance with Article 5(5)(b) of Regulation (EU) No 515/2014**.** **The financial costs of upgrading the SIS as well as the implementation of the this Regulation should be monitored. In case of higher estimated costs EU funding should be made available to support Member States in conformity with the Multiannual Financial Framework**.

(52) Regulation (EC) No 1987/2006 should therefore be repealed.

(53) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on …,

---

[37] 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).

# 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**, where applicable,** biometric **data**~~identifiers~~ as referred to in Article 2**7A**~~2~~, 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 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)[38] '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'~~ **'match'** ~~in SIS~~ means **the occurrence of the following steps**:

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

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

(3) data concerning the alert in SIS match~~es~~ the search data~~, and~~**.**

~~(4) further actions are requested as a result of the hit~~[39]

[38] 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.

[39] Moved to point (b) of subparagraph (ha).

**(ha) a 'hit' means any match which fulfils the following criteria:**

**(a) it has been confirmed:**

**(i) by the end-user; or**

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

**and**

**(b) further actions are requested.**[40]

(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 biometric data as defined in Article 3(13) of Directive (EU) 2016/680;**

[40] Moved from point (4) of subparagraph (h).

(n) 'dactylo~~graphic~~**scopic** data' means ~~data on~~ fingerprints **images, images of fingerprint latents,** ~~and~~ palm prints**, palm prints latents and templates of such images (coded minutiae)**[41] 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;**[42]

(o) 'serious crime' means offences listed in Article 2(1) and (2) of Framework Decision 2002/584/JHA of 13 June 2002;[43]

(p) 'terrorist offences' means **an** offence~~s~~ under national law **which corresponds or is equivalent to one of the offences** referred to in ~~Articles 1-4 of Framework Decision 2002/475/JHA of 13 June 2002~~[44] **Directive (EU) 2017/541**[45]**.**

**(q) 'residence permit' means residence permit as defined in Article 2(16) of Regulation (EU) 2016/399**[46]**;**

**(r) 'long-stay visa' means long-stays visa as defined in Article 1(1) of the Regulation (EU) No 265/2010**[47]**;**

**(s) 'threat to public health' means threat to public health as defined by Regulation (EU) 2016/399**[46]**.**

---

41 Same definition as in Council Decision 2008/616/JHA.

42 Same definition as in the EES proposal (see Article 3(16) in 11037/17 + ADD 1 +ADD 2).

43 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).

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

45 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.

46 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);

47 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*[48]

*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) 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 **may**~~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~~. **Two or more Member States may establish in one of their N.SIS a shared copy which may be used jointly by these Member States. Such shared copy shall be considered as the national copy of each of the participating Member States;**

**(ba) at least one national or shared backup site in each N.SIS. A shared backup N.SIS may be used jointly by two or more Member States and shall be considered as the back-up N.SIS of each of the participating Member States.** The N.SIS and its backup may be used simultaneously to ensure uninterrupted availability to end-users; **and**

(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).

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

2. ~~SIS data~~ **Member States** shall ~~be~~ entere~~d~~, update~~d~~, delete~~d~~ and searche~~d~~ **SIS data** via the various N.SIS. A partial or a full national **or shared** 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 **or shared** 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.

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; **and**

   (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[49]

*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.**[50]

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

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

*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.~~[51]

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.

---

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

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).~~[52]

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.

[52] Moved to paragraph 3.

**3.[53] 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[54], 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**[55] and confidential access modes only (data access control);

---

53 Moved from paragraph 1, *in fine*.

54 eu-LISA proposes to insert the words: "in consultation with the Agency".

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

(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.

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**[56] 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**[57] 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.

---

[56] Same wording as in paragraph 3 and Article 10(1)(f).
[57] Same wording as in paragraph 2 and Article 10(1)(f).

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.

**7.[58] 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.

[58] Text moved from paragraph 7.

# CHAPTER III

## RESPONSIBILITIES OF THE AGENCY[59]

*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.

2. 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. 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.

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

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**;[60]

   (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[61]. 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).~~[62]

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.

---

60 PT, RO, eu-LISA expressed concerns on this provision.
61 eu-LISA would prefer more clear provisions on its competences regarding access to data.
62 Text moved to new paragraph 7.

**7.[63] 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 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 –**Agency***

1. The Agency shall adopt the necessary measures[64], 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);

[63] Text moved from paragraph 5.

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

(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 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**[65], 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**[66] 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 Article~~s 22 and~~ 28 the logs shall show, in particular, the type of data used to perform **the** 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.

---

[65] Singular, as in Article 12(2).

[66] 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 IV

### INFORMATION TO THE PUBLIC[67]

*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.

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

# 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 24A**.

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 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**3~~8~~;

(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) 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**, whenever possible in colour,** 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).~~[68] 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**[69]**, or is equivalent to those. Exceptionally** ~~1-4 of Council Framework Decision 2002/475/JHA on combating terrorism~~[70]**, 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**[71].

---

[68] Redundant with previous paragraph.

[69] **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.**

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

[71] DE and UK entered a reservation on this paragraph.

*Article 22*

*~~Specific rules for entering photographs, facial images and dactylographic 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[72]. ~~Where available, a~~**A**ll ~~other~~ data listed in Article 20(2) shall ~~also~~ be entered**, where available**.

2[73]. An alert may not be entered without the data referred to in Article 20(2) (a), (g), (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.

[72] Moved from paragraph 2.
[73] 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.[74] 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 takes effect 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.**~~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 ~~27~~4A*[75]

*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.

---

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

75 Moved from Article 27.

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 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[76] **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**.

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.

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

# CHAPTER Va

## CONSULTATION PROCEDURE

*Article 26**A***[77]

~~*Consultation procedure*~~ ***Prior consultation before granting or extending a residence permit or long-stay visa***

~~1.~~ Where a Member State considers granting **or extending** a residence permit or ~~other authorisation offering a right to~~ **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** ~~it~~ shall ~~first~~ consult **each other,** ~~the issuing Member State~~ 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** ~~and shall take account of the interests of that Member State. The issuing Member State shall provide a definite reply~~ within **fourteen**~~seven~~ **calendar** days. ~~Where the Member State considering granting a permit or other authorisation offering a right to stay decides to grant it, the alert for refusal of entry and stay shall be deleted.~~

**(c) the absence of a reply by the deadline referred to in paragraph (b) shall mean that the issuing Member State does not object to the granting of the residence permit or long-stay visa;** [78]

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

---

77 PT entered a scrutiny reservation on this Article.

78 LU entered a scrutiny reservation on this paragraph.

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

**(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***

~~2.~~ 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, **and is aware that he or she** ~~who~~ is the holder of a valid residence permit or **long-stay visa**~~other authorisation offering a right to stay~~ ~~issued~~ **granted** by another Member State, ~~it shal first consult~~ the **involved** Member State ~~that issued the permit~~ **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 sufficient 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 reasons for the decision of the Member State that has taken the decision referred to in Article 24(1) and shall consider, in accordance with national law, any threat to public policy or public security which the presence of the third country national in question on the territory of the Member States may pose;**

**(e) the granting** ~~considers entering an 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 consult the Member State that issued the permit through the exchange of supplementary information and shall take account of the interests of that Member State. The~~ Member State ~~that issued the permit~~ shall **notify the Member State that has taken the decision referred to in Article 24(1)** ~~provide a definite reply~~ within **fourteen** ~~seven~~ **calendar** days **after the receipt of the consultation request about its decision; the deadline may be extended upon the reasoned request of the granting**~~. If the~~ 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** ~~issued the permit~~ decides to maintain ~~it, the alert for refusal of entry and stay shall not be entered.~~ **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***

~~3.~~ **Where it emerges that a Member State has entered** ~~In the event of a hit on~~ an alert for refusal of entry and stay ~~concerning~~**in respect of** a third-country national who is the holder of a valid residence permit or ~~other authorisation offering a right to~~ **a long-**stay **visa granted by another**~~, the executing~~ Member State**, the involved Member States** shall consult **each other, through** ~~immediately the Member State that issued the residence permit and the Member State that entered the alert, respectively, via~~ 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 sufficient 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;**

**(d) when making the relevant decision, the granting Member State shall take into account the reasons for the decision of the issuing Member State and shall consider, in accordance with national law, any threat to public policy or 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 fourteen calendar days after the receipt of the consultation request about its 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** ~~in order to~~ decide**s to maintain the residence permit or long-stay visa, the issuing Member State** ~~without delay if the action may be taken. If it is decided to maintain the residence permit, the alert shall be~~ delete~~d~~ **the alert for refusal of entry and stay**.

***Article 26D***

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

**Where a Member State has encountered a hit on an alert for refusal of entry and stay entered by a Member State in respect of a third-country national who is the holder of a valid residence permit or long-stay visa granted by another Member State the executing Member State shall consult immediately, via the exchange of supplementary information, the issuing Member State and the granting Member State in order to determine the measures to be taken. The decision on the entry of the third-country national shall be taken by the executing Member State in accordance with the Schengen Borders Code. In addition, the issuing Member State and granting Member State shall carry out a consultation as referred to in Article 26C.**

**The issuing Member State shall notify the executing Member State about the final outcome of the consultation.**

***Article 26E***

***Statistics***

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

## CHAPTER VI

## SEARCH WITH BIOMETRIC DATA[79]

***Article 27A***

**Specific rules for entering photographs, facial images and dactyloscopic 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).**

[79] Moved from before Article 28.

## ~~CHAPTER VI~~

## ~~SEARCH WITH BIOMETRIC DATA~~[80]

*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, **whenever it is necessary,** from SIS to verify the identity of a person who has been located as a result of an alphanumeric search made in SIS.

2. ~~Dactylographic data may also be used to identify a person. Dactylographic data stored in SIS shall be used for identification purposes i~~**I**f the identity of the person cannot be ascertained by other means**, dactyloscopic data shall be searched for identification purposes. Dactyloscopic data may be searched in all cases to identify a person**.

3. Dactylo**sco**~~graph~~ic data stored in SIS in relation to alerts issued under Article**s** 24 **and 24A** 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~~**a** 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 this functionality is 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.**[81] 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~~.

---

**80** Moved to before Article 27A.

**81** 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).

*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 or national security** within the Member State concerned;[82]

   (d) examining the conditions and taking decisions related to the entry and stay of third-country nationals on the territory of the Member States, ~~including~~ on residence permits**,** ~~and~~ long-stay visas, and to the return of third-country nationals;

   (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.[83]

   **(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;**

---

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

[83] 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).

**1a. The right to access data entered in SIS and the right to search such data directly may 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 t~~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 **national** 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*[84]

*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**[85].

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 the functionality to exchange supplementary information, it shall inform the issuing Member State via the** channels defined by Regulation (EU) 2016/794.

---

84 DE entered a scrutiny reservation on this Article.

85 SK entered a scrutiny reservation on this paragraph.

**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.~~[86]

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;

---

[86] 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.

(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 sh**al**~~ould~~ 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*[87]

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**.[88]

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).

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.

---

87 It should be plural ("team**s**") in both instruments.

88 Text moved from paragraph 5.

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.~~[89]

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 2**4A**~~7~~.

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.

~~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.~~

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.~~[90]

---

**89** Merged with paragraph 1.
**90** Moved to Article 32A(1).

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.~~[91]

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** ~~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 24A.**

[91] Moved to Article 32A(2).

**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.]** [92]

***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 this on-site evaluation shall consist of a maximum of two Commission representatives, assisted by a maximum of eight 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.**

**4. 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.**

**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.**

---

92 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.

**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 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 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[93]. 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.

---

[93] 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 **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 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**.

# CHAPTER VIII

## GENERAL DATA PROCESSING RULES

*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 **exchange supplementary information** ~~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~~**or** 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 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 **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 **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** 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[94]

*Article 46*

*Applicable legislation*

1. Regulation (EC) No 45/2001 shall apply to the processing of personal data by the Agency **and by the European Border and Coast Guard Agency** under this Regulation. **Regulation (EU) 2016/794 (Europol Regulation) shall apply to the processing of personal data by Europol under this Regulation.**

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

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 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.~~

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

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 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~~.[95].

[95] Paragraph merged with paragraph 6.

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.~~[96]

*Article 48*[97]

*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.~~

[96] Merged with paragraph 5.
[97] Moved to Article 46A.

*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.

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)[98] the number of cases **in** which **a final court decision was handed down**~~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)[99] 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.

---

[98] SI, SK, NL suggested the deletion of this point. COM opposed.

[99] NL suggested the deletion of this point.

*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**.

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 AND PENALTIES[100][101]

*Article 53*

*Liability*

1. Each Member State shall be liable**, in accordance with the national law,** 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~~ **other** Member States participating in SIS failed to take reasonable steps to prevent the damage from occurring or to minimise its impact.

***Article 53A***

***Penalties[102]***

**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.**

---

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

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

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

# CHAPTER XI

## FINAL PROVISIONS[103]

*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, **data quality 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.

---

**103** 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**[104]**,** 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).~~[105]

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.

---

[104] 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).

[105] 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.**[106] **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.

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

*Article 56*

*Amendments to Regulation (EU) 515/2014*[107]

Regulation (EU) 515/2014[108] 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 …)~~".

---

**107** UK is not participating in this Regulation.

**108** 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 provisions 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.[109]

Article 25 of the Convention implementing the Schengen Agreement.[110]

*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 Treat**ies**~~y on the Functioning of the European Union~~.

---

[109] 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).

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