Council of the European Union

Brussels, 16 October 2017
(OR. en)

13162/17

Interinstitutional File:
2016/0409 (COD)

LIMITE

SIRIS 162
ENFOPOL 449
COPEN 298
SCHENGEN 64
COMIX 677
CODEC 1580

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 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 - 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 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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 82(1) second subparagraph point (d), 85(1), 87(2)(a) and 88(2)(a) 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 and judicial~~ authorities **responsible for the prevention, the detection, investigation or prosecution of criminal ofences or the execution of** ~~in~~ criminal **penalties and checks on third-country nationals**~~matters~~[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[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 Chapters 4 and 5 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 border checks[9] 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.

(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, 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 criminal offences, 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, in order to facilitate the identification of persons and to detect multiple identities, data categories relating to persons 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 **dactyloscopic**~~fingerprints~~ 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)[12] The introduction of an automated fingerprint identification service within SIS complements the existing Prüm mechanism on mutual cross-border online access to designated national DNA databases and automated fingerprint identification systems[13]. The Prüm mechanism enables interconnectivity of national fingerprint identification systems whereby a Member State can launch a request to ascertain if the perpetrator of a crime whose fingerprints have been found, is known in any other Member State. The Prüm mechanism verifies if the owner of the fingerprints are known in one point in time**. T**~~t~~herefore if the perpetrator becomes known in any of the Member States later on he or she will not necessarily be captured. The SIS fingerprint search allows an active search of the perpetrator. Therefore, it should be possible to upload the fingerprints of an unknown perpetrator into SIS, provided that the owner of the fingerprints can be identified to a high degree of probability as the perpetrator of a serious crime or act of terrorism. This is in particular the case if fingerprints are found on the weapon or on any object used for the offence. The mere presence of the fingerprints at the crime scene should not be considered as indicating a high degree of probability that the fingerprints are those of the perpetrator. A further precondition for the creation of such alert should be that the identity of the perpetrator cannot be established via any other national, European or international databases. Should such fingerprint search lead to a potential match the Member State should ~~should~~ carry out further checks with their fingerprints, possibly with the involvement of fingerprint experts to establish whether he or she is the owner of the prints stored in SIS, and should establish the identity of the person. The procedures should be subject of national law. An identification as the owner of an "unknown wanted person" in SIS may substantially contribute to the investigation and it may lead to an arrest provided that all conditions for an arrest are met.

---

12 EL entered a scrutiny reservation on this recital.

13 Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p.1); and Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 12).

(19) Fingerprints **or palmprints** found at a crime scene should be allowed to be checked against the **dactyloscopic data**~~fingerprints~~ 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[14] and 'terrorist offence' should be offences ~~under national law~~ **corresponding or equivalent to one of the offences** referred to in **Directive (EU) 2017/541**[15] ~~Council Framework Decision 2002/475/JHA~~[16].

(20) It should be possible to add a DNA profile in cases where ~~dactylographic~~**dactyloscopic** data**, photographs or facial images** are not available, and which should only be accessible to authorised users. DNA profiles should facilitate the identification of missing persons in need of protection and particularly missing children, including by allowing the use of DNA profiles of **ascendants, descendants** ~~parents~~ or siblings to enable identification. DNA data should not contain reference to racial origin.

(20A) 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.

(20B) DNA profiles should only be retrieved from SIS in case that an identification is necessary and proportionate for the purposes of Article 32(2)(a) and (c). DNA profiles should not be retrieved and processed for any other purpose than those for which they were entered in accordance with Article 32(2)(a) and (c). Applying the data protection and security rules laid down in this Regulation additional safeguards, if necessary, should be put in place when using DNA profiles in order to prevent any risks for false matches, hacking and unauthorised sharing with third parties.

---

14 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).

15 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.

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

(21) SIS should contain alerts on persons wanted for arrest for surrender purposes and wanted for arrest for extradition purposes. In addition to alerts, it is appropriate to provide for the exchange of supplementary information **via the SIRENE Bureaux** which is necessary for the surrender and extradition procedures. In particular, data referred to in Article 8 of the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant and the surrender procedures between Member States[17] should be processed in SIS. Due to operational reasons, it is appropriate for the issuing Member State to make an existing alert for arrest temporary unavailable upon the authorisation of the judicial authorities when a person subject of a European Arrest Warrant is intensively and actively searched and end-users not involved in the concrete search operation may jeopardise the successful outcome. The temporary unavailability of such alerts should **in principle** not exceed 48 hours.

(22) It should be possible to add to SIS a translation of the additional data entered for the purpose of surrender under the European Arrest Warrant and for the purpose of extradition.

(23) SIS should contain alerts on missing **or vulnerable** persons to ensure their protection or to prevent threats to public security. Issuing an alert in SIS for children at risk of abduction (*i.e.* in order to prevent a future harm that has not yet taken place as in the case of children who are at risk of parental abduction) should be limited, therefore it is appropriate to provide for ~~strict and~~ appropriate safeguards. In cases of children, these alerts and the corresponding procedures should serve the best interests of the child having regard to Article 24 of the Charter of Fundamental Rights of the European Union and the United Nations Convention on the Rights of the Child of 20 November 1989.

(23A) Alerts on children at risk of abduction should be entered to SIS at the request of competent authorities, including judicial authorities, having jurisdictions in matters of parental responsibility in accordance with national law.

[17] 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).

(23B)[18] **Alerts on vulnerable persons who need to be prevented from travelling for their own protection should be entered in particular with respect to whom it is believed that the travel would create a risk of forced mariage, female genital mutilation, trafficking of human beings or in the case of children, of joining armed conflicts, organised criminal groups or terrorist groups.**

(24)[19] A new action should be included for cases of suspected terrorism and serious crime, allowing for a person who is suspected to have committed a serious crime or where there is a reason to believe that he or she will commit a serious crime, to be ~~stopped and~~ **interviewed**~~questioned~~ **subject to national law** in order to supply the most detailed information to the issuing Member State. This new action **to be carried out during the police or border check** should not amount either to searching the person or to his or her arrest **and the procedural rights of the person should be preserved**. **It is also without prejudice to existing mutual legal assistance mechanisms.** It should supply, however, sufficient information to decide about further actions **between the alert issuing and executing authorities as much as possible in real time**. Serious crime should be the offences listed in Council Framework Decision 2002/584/JHA.

(24A) In case of alerts on objects for seizure or use as evidence in criminal proceedings, the objects should in principle be seized. However, national law determines if and in accordance with which conditions an object is seized if it is in the possession of its rightful owner.

(25) SIS should contain new categories of objects of high value, such as **information technology items**~~electronic and technical equipment~~ which can be identified and searched with a unique number.

---

18 EL entered scrutiny reservation on this recital.

19 LV entered scrutiny reservation on this recital.

(25A) As regards documents to be inserted for seizure or use as evidence in criminal proceedings, the term "false" should be construed as encompassing both falsified and counterfeit documents.

(26) It should be possible for a Member State to add an indication, called a flag, to an alert, to the effect that the action to be taken on the basis of the alert will not be taken on its territory. When alerts are issued for arrest for surrender purposes, nothing in this **Regulation** ~~Decision~~ should be construed so as to derogate from or prevent the application of the provisions contained in the Framework Decision 2002/584/JHA. The decision to add a flag to an alert **with a view to non-executing a European Arrest Warrant** should be based only on the grounds for refusal contained in that Framework Decision.

(27) When a flag has been added and the whereabouts of the person wanted for arrest for surrender becomes known, the whereabouts should always be communicated to the issuing judicial authority, which may decide to transmit a European Arrest Warrant to the competent judicial authority in accordance with the provisions of the Framework Decision 2002/584/JHA.

(28) 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.

(29) 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 retention period of alerts on persons with the retention periods envisaged for return and illegal stay purposes. Moreover, Member States regularly extend the expiry date of alerts on persons if the required action could not be taken within the original time period. 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, except for alerts issued for the purposes of discreet, specific and inquiry checks. These should be deleted after one year. Alerts on objects ~~entered for discreet checks, inquiry checks or specific checks should be automatically deleted from the SIS after a period of one year, as they are always related to persons. Alerts on objects for seizure or use as evidence in criminal proceedings~~ should be automatically deleted from SIS after a period of **ten**~~five~~ years, as after such a period the likelihood of finding them is very low and their economic value is significantly diminished. Alerts on **objects, where linked to alerts on persons** ~~issued and blank identification documents~~ should **not** be kept **longer than the linked alert on the person and in any case not exceeding five**~~for 10~~ years~~, as the validity period of documents is 10 years at the time of issuance~~. Decisions to keep alerts on persons should be based on a comprehensive individual assessment. Member States should review alerts on persons **and objects** within ~~the~~ **regular** ~~defined~~ period**s** and keep statistics about the number of alerts ~~on persons~~ for which the retention period has been extended.

(30) 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. Offences pursuant to Articles 1, 2, 3 and 4 of Council Framework Decision 2002/475/JHA on combating terrorism[20] constitute a very serious threat to public security and integrity of life of individuals and to society, and these offences are extremely difficult to prevent, detect and investigate in an area without internal border controls where potential offenders circulate freely. Where a person or object is sought in relation to these offences, it is ~~always~~ necessary to create the corresponding alert in SIS on persons sought for a criminal judicial procedure, on persons or objects subject to a discreet, inquiry**,** and specific check as well as on objects for seizure, as no other means would be as effective in relation to that purpose. **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.**

(31) It is necessary to provide clarity concerning the deletion of alerts. An alert should be kept only for the time required to achieve the purpose for which it was entered. Considering the diverging practices of Member States concerning the definition of the point in time when an alert fulfils its purpose, it is appropriate to set out detailed criteria for each alert category to determine when it should be deleted from SIS.

(32) 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 data processing should be bound by the security requirements of this Regulation and be subject to a uniform incident reporting procedure.

---

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

(33) 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.~~

(34) It is appropriate to grant access to SIS to authorities responsible for registering vehicles, boats and aircraft in order to allow them to verify whether the conveyance is already searched for in a Member States for seizure or for check. ~~Direct access should be provided to authorities which are governmental services. This access should be limited to alerts concerning the respective conveyances and their registration document or number plate. Accordingly, the provisions of Regulation (EC) 1986/2006 of the European Parliament and of the Council~~[21] ~~should be included into this Regulation and that Regulation should be repealed.~~[22]

(34A) It is appropriate to grant access to SIS to authorities responsible for registering firearms in order to allow them to verify whether the firearm is already searched for in Member States for seizure or for check or whether there is an alert concerning the requesting person.

~~[21] Regulation (EC) 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (OJ L 381, 28.12.2006, p. 1).~~

[22] **Moved to recital (34B).**

(34B)[23] Direct access should be provided to competent authorities which are governmental services. This access should be limited to alerts concerning the respective conveyances and their registration document or number plate or firearms and requesting persons. Accordingly, the provisions of Regulation (EC) 1986/2006 of the European Parliament and of the Council[24] should be included into this Regulation and that Regulation should be repealed. Any hit in SIS must be reported by the above mentioned authorities to the police authorities for further procedures in line with the particular alert in SIS and for notifying the hit via the SIRENE Bureaux to the issuing Member State.

(35) For processing of data by competent national authorities for the purposes of the prevention, investigation, detection of serious crime or terrorist offences, or prosecution of criminal offences and the execution of criminal penalties including the safeguarding against the prevention of threat to public security, national provisions transposing Directive (EU) 2016/680 should apply. The provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council[25] and Directive (EU) 2016/680 should be further specified in this Regulation where necessary.

(36) Regulation (EU) 2016/679 should apply to the processing of personal data under this Regulation by national authorities when Directive (EU) 2016/680 does not apply. Regulation (EC) No 45/2001 of the European Parliament and of the Council[26] should apply to the processing of personal data by the institutions and bodies of the Union when carrying out their responsibilities under this Regulation.

---

23 **Partially moved from recital (34).**

24 **Regulation (EC) 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (OJ L 381, 28.12.2006, p. 1).**

25 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).

26 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).

(37) 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 (Europol Regulation)[27] applies. **With regard to processing of personal data by Eurojust, Decision 2002/187 applies.**

(38) The provisions of Decision 2002/187/JHA of 28 February 2002[28] setting up Eurojust with a view to reinforcing the fight against serious crime concerning data protection apply to the processing of SIS data by Eurojust, including the powers of the Joint Supervisory Body, set up under that Decision, to monitor the activities of Eurojust and liability for any unlawful processing of personal data by Eurojust. In cases when searches carried out by Eurojust in SIS reveal the existence of an alert issued by a Member State, Eurojust cannot take the required action. Therefore it should inform the Member State concerned allowing it to follow up the case.

(39) 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.

(40) 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.

(41) 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.

---

[27] 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).

[28] Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 63, 6.3.2002, p. 1).

(42) 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.

(43) 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. The extension of Europol's access rights to the SIS alerts on missing persons should further improve Europol's capacity to provide national law enforcement authorities with comprehensive operational and analytical products concerning trafficking in human beings and child sexual exploitation, including online. This would contribute to better prevention of these criminal offences, the protection of potential victims and to the investigation of perpetrators. Europol's European Cybercrime Centre would also benefit from new Europol access to SIS alerts on missing persons, including in cases of travelling sex offenders and child sexual abuse online, where perpetrators often claim that they have access to children or can get access to children who might have been registered as missing. ~~Furthermore, since 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 or stay within the territory of a Member State either on criminal grounds or because of non-compliance with visa and stay conditions.~~

(44)[29] 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.

(45) 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 the respective SIRENE Bureau** allowing it to follow up the case.

[29] UK entered a scrutiny reservation on this recital.

(46) Regulation (EU) 2016/1624 of the European Parliament and of the Council[30] provides for the purpose 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 team**s** 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 team**s** 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.**

[30] 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).

(47) 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)[31] 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 persons and alerts on blank and issued personal identification documents.

(48) 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, specifying new object categories within the technical and electronic equipment category, 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.

(49) 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[32]. The procedure for adopting implementing measures under this Regulation and Regulation (EU) 2018/xxx (border checks) should be the same.

---

31 COM (2016)731 final.

32 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).

(50) 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.

(51) 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 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.

(52) 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 special protection for children who could be victim of trafficking or parental abduction while fully respecting the protection of personal data.

(53) 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, 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.

(54) The United Kingdom is taking part in this Regulation in accordance with Article 5**(1)** of ~~the~~ Protocol **No 19** on the Schengen acquis integrated into the framework of the European Union annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union and Article 8(2) of Council Decision 2000/365/EC ~~of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis~~[33].

(55) Ireland is taking part in this Regulation in accordance with Article 5 of ~~the~~ Protocol **No 19** on the Schengen acquis integrated into the framework of the European Union annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union and Article 6(2) of Council Decision 2002/192/~~EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen acquis~~[34].

(56) 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[35], which fall within the area referred to in Article 1, point G of Council Decision 1999/437/EC[36]on certain arrangements for the application of that Agreement.

---

33 Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis (OJ L 131, 1.6.2000, p. 43).

34 Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen acquis (OJ L 64, 7.3.2002, p.20).

35 OJ L 176, 10.7.1999, p.36.

36 OJ L 176, 10.7.1999, p.31.

(57) 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[37] and 2004/860/EC[38]~~ **2008/149/JHA**[39].

~~[37] 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).~~

~~[38] 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).~~

[39] Council Decision 2008/149/JHA of 28 January 2008 on the conclusion on behalf of the European Union 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. 50).

(58) 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[40], 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[41] ~~and Article 3 of Council Decision 2011/350/EU[42]~~.

(59) 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[43] **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**.[44]

---

40 OJ L 160, 18.6.2011, p. 21.

41 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).

~~42 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).~~

43 OJ L 166, 1.7.2010, p. 17.

44 OJ L 108, 26.4.20017, p. 31.

(60) 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~~.

(61) This Regulation should apply to Ireland on dates determined in accordance with the procedures set out in the relevant instruments concerning the application of the Schengen acquis to this State.

~~(62) 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[45]. 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.~~

(63) Council Decision 2007/533/JHA and Commission Decision 2010/261/EU[46] should therefore be repealed.

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

~~[45] 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).~~

[46] 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).

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 4 and Chapter 5 of Title V of Part Three of the Treaty on the Functioning of the European Union relating to the movement of persons 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 on persons and objects, the exchange of supplementary information and additional data for the purpose of police and judicial cooperation in criminal matters.

2. This Regulation also lays down provisions on the technical architecture of SIS, the responsibilities of the Member States and of the European Agency 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 ~~identifiers~~ **data** as referred to in Article 22 and in Article 40, entered in SIS allowing the competent authorities to identify a person or an object 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) 'personal data' means any information relating to an identified or identifiable natural person ('data subject');

(e) '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;

(f) '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;

(g) 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 entered by another Member State in SIS; **and**

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

(ga) 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

(4**b**) further actions are requested.

(h) 'flag' means a suspension of validity of an alert at the national level that may be added to alerts for arrest, alerts for missing persons and alerts for discreet, inquiry and specific checks~~, where a Member State considers that to give effect to an alert is incompatible with its national law, its international obligations or essential national interests. Where the alert is flagged, the requested action on the basis of the alert shall not be taken on the territory of this Member State.~~**;**

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

(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;

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

(l) ‘dactylo~~graphies~~**scopic**data’ means ~~data on~~ fingerprints **images, images of fingerprint latents** ~~and~~ palm prints**, palm prints latents and templates of such images (coded minutiae)** [47] which due to their unique character and the reference points contained therein enable accurate and conclusive comparisons on a person's identity;

(la) 'facial image' means digital images of the face with sufficient image resolution and quality to be used in automated biometric matching; [48]

(lb) 'DNA profile' means a letter or number code which represents a set of identification characteristics of the noncoding part of an analysed human DNA sample, i.e. the particular molecular structure at the various DNA locations (loci) [49]**;**

(m) ‘serious crime’ means offences listed in Article 2(1) and (2) of Framework Decision 2002/584/JHA of 13 June 2002; [50]

(n) ‘terrorist offences’ means **an** offence~~s~~ under national law **which corresponds or is equivalent to one of the offences** referred to in ~~Articles 1-4of Framework Decision 2002/475/JHA of 13 June 2002~~[51] **Directive (EU) 2017/541**[52].

---

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

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

49 Same definition as in Article 2(c) of Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 12).

50 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).

~~51 Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ L 164, 22.6.2002, p. 3).~~

52 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.

(o) 'vulnerable persons' means persons who, due to their age, physical or mental state, or due to their social or family circumstances, require protection.

(p) 'threat to public health' means threat to public health as defined by Regulation (EU) 2016/399[53].

Article 4[54]

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)[55] a national system (N.SIS) in each of the Member States, consisting of the national data systems which communicate with Central SIS. An N.SIS ~~shall~~**may** 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**

---

53 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);

54 SI entered a scrutiny reservation on this Article.

55 FI, supported by IS and NO, opposed the obligation for the Member States to have a national copy and entered a reservation on this provision.

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

2. ~~SIS data~~**Member States** shall ~~be~~ entere~~d~~, update~~d~~, delete~~d~~ and search~~ed~~ **SIS data** via the various N.SIS. A partial or a full national **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) concerning objects and the data listed in Article 20(3) (a) to (v) **and (z)** of this Regulation concerning alerts on persons. 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[56]

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[57].

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

[57] 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.~~[58]

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 ~~I~~ **O**ffice and of their SIRENE Bureau. The Agency shall publish the list of them together with the list referred to in Article 53(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 Communication Infrastructure is unavailable, Member States may use other adequately secured technical means to exchange supplementary information.

---

[58] 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 61 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[59] 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 72(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 72(2).~~[60]

2. Member States shall ensure, by means of the services provided by CS-SIS, that data stored in the national **or shared** copy are, by means of automatic updates referred to in Article 4(4), identical to and consistent with the SIS database, and that a search in its national **or shared** copy produces a result equivalent to that of a search in the SIS database. End-users shall receive the data required to perform their tasks, in particular all data required for the identification of the data subject and to take the required action.

---

[59] DE, EL, ES, HU, LT, SE and SK expressed concerns regarding this provision. UK entered a reservation, as it opposed the insertion of the 12-hour period into the Regulation.

[60] Moved to paragraph 3.

3.[61] 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 72(2).

Article 10

Security – Member States

1. Each Member State shall[62], 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**[63] and confidential access modes only (data access control);

---

61 Moved from paragraph 1, *in fine*.
62 eu-LISA proposes to insert the words: "in consultation with the Agency".
63 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 6~~6~~**7** 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 43.

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

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 ~~records~~ **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 ~~names~~ **individual and unique user identifiers**[64] 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~~s 40, 41 and~~ 42 the logs shall show, in particular, the type of data used to perform a search, a reference to the type of data transmitted and the ~~names~~ **individual and unique user identifiers**[65] 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.

---

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

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

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

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

7. Where Member States carry out automated scanned searches of the number plates of motor vehicles, using Automatic Number Plate Recognition systems, Member States shall maintain a log of the search in accordance with national law. ~~The content of this log shall be established by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).~~[66]~~. Where a positive match is achieved against data stored in SIS, or a national or technical copy of SIS data, a full search shall be carried out in SIS in order to verify that a match has indeed been achieved. The provisions of paragraphs 1 to 6 of this Article shall apply to this full search.~~

8.[67] **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 72(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.

---

66 Text moved to new paragraph 8.

67 Text moved from paragraph 7.

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.

CHAPTER III
RESPONSIBILITIES OF THE AGENCY[68]

Article 15

Operational management

1. The Agency shall be responsible for the operational management of Central SIS. The Agency shall, 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;

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

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.

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

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

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

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[69]. The Agency shall provide a regular report to the Commission covering the issues encountered and the Member States concerned. ~~This mechanism, procedures and the interpretation of data quality compliance shall be established by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).~~[70]

[69] eu-LISA would prefer more clear provision on its competences regarding access to data.
[70] Text moved to new paragraph 7.

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

7.[71] **The Commission shall adopt implementing acts to set out the technical requirements of the Communication Infrastructure referred to in paragraph 2, and to establish the mechanism and procedures for the quality checks on the data in CS-SIS referred to in paragraph 5 and for the interpretation of data quality compliance. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72(2).**

Article 16

Security ***- Agency***

1. The Agency shall adopt the necessary measures[72], 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);

[71] Text moved from paragraph 5.
[72] eu-LISA asked to include in recital 40 a reference to Commission Decision 2017/46.

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

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

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

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

(g) create profiles describing the functions and responsibilities for persons who are authorised to access the data or the data processing facilities and make these profiles available to the European Data Protection Supervisor referred to in Article 64 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 – ~~The~~ 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 **C**ommunication **I**nfrastructure.

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**[73], 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**[74] of the competent authority responsible for processing the data.

[73] Singular, as in Article 12(2).
[74] Same wording as in Articles 10(1)(f) and 12(2) and (3).

3. If the search is carried out with dactylo~~graphies~~**scopic** data or facial image in accordance with Articles 40, 41 and **42** 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.

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[75]

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.

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

CHAPTER V
CATEGORIES OF DATA AND FLAGGING

Article 20

Categories of data

1. Without prejudice to Article 8(1) or the provisions of this Regulation providing for the storage of additional data, SIS shall contain only those categories of data which are supplied by each of the Member States, as required for the purposes laid down in Articles 26, 32, 34, 36**,** ~~and~~ 38 **and 40**.

2. The categories of data shall be as follows:

   (a) information on persons in relation to whom an alert has been issued;

   (b) information on objects referred to in Articles 32, **34,** 36 and 38.

3. **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) ~~sex~~**gender**;

(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** ~~risk~~ **threat to public health; or**

vi. ~~or~~ is involved in a **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 ~~53~~**60**;

(p) the type of offence for which the alert was issued;

(q) the person's registration number in a national register**;**

(r) a categorisation of the type of missing person case (only for alerts referred to in Article 32);

(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) relevant DNA profiles subject to Article 22(1)(b) of this Regulation;

(y) dactylo~~graphic~~**scopic** data;

(z) a ~~colour~~ copy**, whenever possible in colour,** of the identification document**s**.

4. The technical rules necessary for entering, updating, deleting and searching the data referred to in paragraphs 2 and 3 shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).

5. ~~The technical rules necessary for searching data referred to in paragraph 3 shall be laid down and developed in accordance with the examination procedure referred to in Article 72(2).~~[76]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 53(2) 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 72(2).

[76] Redundant with paragraph 4.

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.[77] Where a person or an object is sought by a Member State in relation to an offence that falls under Articles ~~1~~**3** to **1**4 of **Directive 2017/541 or is equivalent to those offences** ~~of the European Parliamenent and of the Council on combating terrorism and replacing CouncilFramework Decision 2002/475/JHA on combating terrorism~~[78], the Member State shall~~,in all circumstances,~~ create a~~the~~ corresponding alert,~~under either Article 34, 36 or 38 as appropriate,~~ **. 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**.[79]

Article 22[80]

~~*Specific rules for entering photographs, facial images, dactyloscopic data and DNA profiles*~~

~~1. The entering into SIS of data referred to in Article 20(3)(w), (x) and (y) shall be subject to the following provisions:~~

~~(a) Photographs, facial images, dactylographic data and DNA profiles shall only be entered following a quality check to ascertain the fulfilment of a minimum data quality standard.~~

[77] UK entered a reservation on this paragraph.
[78] ~~OJ L 88, 31.3.2017, p. 6.~~
[79] ES and SE entered a reservation on this paragraph.
[80] Article moved to new Chapter XIa, as Article 41A.

~~(b) A DNA profile may only be added to alerts provided for in Article 32(2)(a) and (c) and only where photographs, facial images or dactylographic data suitable for identification are not available. The DNA profiles of persons who are direct ascendants, descendants or siblings of the alert subject may be added to the alert provided that those persons concerned gives explicit consent. The racial origin of the person shall not be included in the DNA profile.~~

~~2. Quality standards shall be established for the storage of the data referred to under paragraph 1(a) of this Article and Article 40. 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 72(2).~~

Article 23

Requirement for an alert to be entered

1. ~~An alert on a person may not be entered without the data referred to in Article 20(3)(a), (g), (k), (m), (n) as well as, where applicable, (p), except for in the situations referred to in Article 40.~~[81] **All data listed in Article 20(3) shall be entered, where available.**[82]

2. ~~Where available, all other data listed in Article 20(3) shall also be entered.~~[83] An alert on a person may not be entered without the data referred to in Article 20(3)(a), (g), (k), ~~(m),~~ (n) ~~as well as, where applicable,~~ ~~(p)~~, except for in the situations referred to in Article 40.[84]

---

81 Partially moved to paragraph 2.
82 Partially moved from paragraph 2.
83 Partially moved to paragraph 1.
84 Partially moved from paragraph 1.

Article 24

General provisions on flagging

1. Where a Member State considers that to give effect to an alert entered in accordance with Articles 26, 32 **or**~~and~~ 36 is incompatible with its national law, its international obligations or essential national interests, it may subsequently require that a flag be added to the alert to the effect that the action to be taken on the basis of the alert will not be taken in its territory. The flag shall be added by the SIRENE Bureau of the issuing Member State.

2. In order to enable Member States to require that a flag be added to an alert issued in accordance with Article 26, all Member States shall be notified automatically about any new alert of that category by the exchange of supplementary information.

3. If in particularly urgent and serious cases, an issuing Member State requests the execution of the action, the Member State executing the alert shall examine whether it is able to allow the flag added at its behest to be withdrawn. If the executing Member State is able to do so, it shall take the necessary steps to ensure that the action to be taken can be carried out immediately.

Article 25

Flagging related to alerts for arrest for surrender purposes

1. Where Framework Decision 2002/584/JHA applies, a flag preventing arrest shall ~~only~~ be added to an alert for arrest for surrender purposes where the competent judicial authority under national law for the execution of a European Arrest Warrant has refused its execution on the basis of a ground for non-execution and where the addition of the flag has been required.

A Member State may also require that a flag be added to the alert if its competent judicial authority releases the subject of the alert during the surrender process.

2. However, at the behest of a competent judicial authority under national law, either on the basis of a general instruction or in a specific case, a flag may also be required to be added to an alert for arrest for surrender purposes if it is obvious that the execution of the European Arrest Warrant will have to be refused.

CHAPTER VI

ALERTS IN RESPECT OF PERSONS WANTED FOR ARREST FOR SURRENDER OR EXTRADITION PURPOSES

Article 26

Objectives and conditions for issuing alerts

1. Data on persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant or wanted for arrest for extradition purposes shall be entered at the request of the judicial authority of the issuing Member State.

2. Data on persons wanted for arrest for surrender purposes shall also be entered on the basis of arrest warrants issued in accordance with Agreements concluded between the Union and third countries on the basis of Article 37 of the Treaty on the European Union for the purpose of surrender of persons on the basis of an arrest warrant, which provide for the transmission of such an arrest warrant via the SIS.

3. Any reference in this Regulation to provisions of the Framework Decision 2002/584/JHA shall be construed as including the corresponding provisions of Agreements concluded between the European Union and third countries on the basis of Article 37 the Treaty on the European Union for the purpose of surrender of persons on the basis of an arrest warrant which provide for the transmission of such an arrest warrant via SIS.

4.[85] ~~The issuing Member State may, i~~**I**n the case of an ongoing ~~search~~ operation**, the issuing Member State may temporarily make an existing alert for arrest issued under Article 26 unavailable for searching to the effect that the alert shall not be searchable by the end-user in the Member States involved in the operation and will only be accessible to the SIRENE Bureaux, where the following conditions are met:**

(a) ~~where~~ **the purpose of the operation cannot be achieved by other measures;**

(b) ~~and following the~~ **a prior** authorisation ~~of~~ **as been granted by** the relevant judicial authority of the issuing Member State**; and**

(c) all Member States involved in the operation have been informed through the exchange of supplementary information.

~~, temporarily make an existing alert for arrest issued under Article 26 of this Regulation unavailable for searching to the effect that the alert shall not be searchable by the end-user and will only be accessible to the SIRENE Bureaux.~~

The~~is~~ functionality **provided for in the first subparagraph** shall **only** be used for a period not exceeding 48 hours ~~with the authorisation of the relevant judicial authority of the issuing Member State after informing all Member States involved in the operation, through the exchange of supplementary information~~. **However, i**f operationally necessary, ~~however,~~ it may be extended by further periods of 48 hours. Member States shall keep statistics about the number of alerts where this functionality has been used.

5. Where there is a clear indication that the object referred to in Article 38 (2)(a), (b), (c), (e), (g), (h) and (k) are connected with a person who is the subject of an alert pursuant to paragraph 1 and 2, alerts on those objects may be issued in order to locate the person. In those cases the alert on the person and the alert on the object shall be linked in accordance with Article 60.

[85] UK entered a reservation on this Paragraph.

Article 27

Additional data on persons wanted for arrest for surrender purposes

1. Where a person is wanted for arrest for surrender purposes on the basis of a European Arrest Warrant the issuing Member State shall enter in SIS a copy of the original of the European Arrest Warrant.

2. The issuing Member State may enter a copy of a translation of the European Arrest Warrant in one or more other official languages of the institutions of the European Union.

Article 28

Supplementary information on persons wanted for arrest for surrender purposes

The Member State which entered the alert in SIS for arrest for surrender purposes shall communicate the information referred to in Article 8(1) of Framework Decision 2002/584/JHA to the other Member States through the exchange of supplementary information.

Article 29

Supplementary information on persons wanted for arrest for extradition purposes

1. The Member State which entered the alert into SIS for extradition purposes shall communicate the following data to the other Member States through the exchange of supplementary information to all Member States:

   (a) the authority which issued the request for arrest;

   (b) whether there is an arrest warrant or a document having the same legal effect, or an enforceable judgment;

   (c) the nature and legal classification of the offence;

   (d) a description of the circumstances in which the offence was committed, including the time, place and the degree of participation in the offence by the person for whom the alert has been issued;

(e) in so far as possible, the consequences of the offence;

(f) any other information useful or necessary for the execution of the alert.

2. The data listed in paragraph 1 shall not be communicated where the data referred to in Articles 27 or 28 have already been provided and are considered sufficient for the execution of the alert by the Member State concerned.

Article 30

Conversion of alerts on persons wanted for arrest for surrender purposes or extradition purposes

Where an arrest cannot be made, either because a requested Member State refuses to do so, in accordance with the procedures on flagging set out in Articles 24 or 25, or because, in the case of an alert for arrest for extradition purposes, an investigation has not been completed, the requested Member State shall consider the alert ~~as being an alert~~ for the purposes of communicating the whereabouts of the person concerned.

Article 31

Execution of action based on an alert on a person wanted for arrest with a view to surrender or extradition

1. An alert entered in SIS in accordance with Article 26 together with the additional data referred to in Article 27, shall constitute and have the same effect as a European Arrest Warrant issued in accordance with Framework Decision 2002/584/JHA where this Framework Decision applies.

2. Where Framework Decision 2002/584/JHA does not apply, an alert entered in SIS in accordance with Articles 26 and 29 shall have the same legal force as a request for provisional arrest under Article 16 of the European Convention on Extradition of 13 December 1957 or Article 15 of the Benelux Treaty concerning Extradition and Mutual Assistance in Criminal Matters of 27 June 1962.

CHAPTER VII

ALERTS ON MISSING OR VULNERABLE PERSONS

Article 32[86]

Objectives and conditions for issuing alerts

1. ~~Data on missing persons or other persons who need to be placed under protection or whose whereabouts need to be ascertained shall be entered in SIS at the request of the competent authority of the Member State issuing the alert.~~

2. The following categories of ~~missing~~ persons **shall**~~may~~ be entered **in SIS at the request of a competent authority of the Member State issuing the alert**:

   (a) missing persons who need to be placed under protection

      (i) for their own protection;

      (ii) in order to prevent threats;

   (b) missing persons who do not need to be placed under protection;

   (c) children at risk of abduction in accordance with paragraph 4 **who need to be prevented from travelling; or**

   (d) vulnerable persons who need to be prevented from travelling for their own protection in accordance with paragraph 4(a).

3. **Points (a) and (d) of** ~~P~~**p**aragraph 2~~(a)~~ shall apply in particular to children**,** and to **those** persons **in respect of whom** a decision **has been made** by a competent authority~~ies~~.

[86] AT, EL, SI and UK entered a scrutiny reservation on this Article.

4. An alert on a child referred to in paragraph 2(c) shall be entered at the request of the competent ~~judicial~~ authorit**iesy**~~,~~**including judicial authorities of the Member States having jurisdiction in matters of parental responsibility,** ~~of the Member State that has jurisdiction in matters of parental responsibility in accordance with Council Regulation No 2201/2003[87]~~where a concrete and apparent risk exists that the child may be unlawfully ~~and imminently~~ removed from the Member State where th~~at~~**e** competent ~~judicial~~ authorit**iesy** **are**~~is~~ situated. ~~In Member States which are party to the Hague Convention of 19 October 1996 on Jurisdiction, Applicable law, Recognition, Enforcement and Cooperation in Respect of Parental Responsibility and Measures for the Protection of Children and where Council Regulation No 2201/2003 does not apply, the provisions of the Hague Convention are applicable.~~

The competent authority shall regularly review the need to retain the alert.

4a. An alert on vulnerable persons referred to in paragraph 2(d) shall be entered at the request of the competent authorities, where it is considered that a concrete and apparent risk exists to that person should they travel from that Member State. ~~This shall apply in particular to vulnerable persons in relation to whom it is believed that the travel would create a risk of forced mariage, female genital mutilation, or in the case of minors, of joining armed conflicts, organised criminal groups or terrorist groups.~~

The competent authority shall regularly review the need to retain the alert.

~~[87] Council Regulation (EC) No 2201/2003 of 27 November 2003 concerning jurisdiction and the recognition and enforcement of judgments in matrimonial matters and the matters of parental responsibility, repealing Regulation (EC) No 1347/2000 (OJ L 338, 23.12.2003, p. 1).~~

5. Member States shall ensure that the data entered in SIS indicate which of the categories referred to in paragraph 2 the ~~missing~~ person falls into. Further, Member States shall also ensure that the data entered in SIS indicate which type of ~~missing or vulnerable person~~ case is involved **and that, in relation to alerts issued pursuant to points (c) and (d) of paragraph 2, all relevant information is made available at the SIRENE Bureau of the issuing Member State at the time of the alert creation**. ~~The rules on the categorisation of the types of cases and the entering of such data shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).~~[88]

6. Four months before a child who is the subject of an alert under this Article reaches **the age of majority in accordance with the national law of the issuing Member State**~~adulthood~~, CS-SIS shall automatically notify the issuing Member State that the reason for request and the action to be taken have to be updated or the alert has to be deleted.

7. Where there is a clear indication that vehicles, boats or aircraft are connected with a person who is the subject of an alert pursuant to paragraph 2, alerts on those vehicles, boats and aircraft may be issued in order to locate the person. In those cases the alert on the ~~missing~~ person and the alert on the object shall be linked in accordance with Article 60. ~~The technical rules necessary for entering, updating, deleting and searching the data referred to in this paragraph shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).~~[89]

8.[90] **The Commission shall adopt implementing acts to lay down and develop rules on the categorisation of the types of cases and the entering of data referred to in paragraph 5 and technical rules necessary for entering, updating, deleting and searching the data referred to in paragraph 7. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72(2).**

---

88 Moved to paragraph 8.
89 Moved to paragraph 8.
90 Moved from paragraph 5 *in fine* and paragraph 7 *in fine*.

Article 33[91]

Execution of action based on an alert

1. Where a person as referred to in Article 32 is located, the competent authorities shall, subject to paragraph 2, communicate his or her whereabouts to the Member State issuing the alert.

1a. In the case of **persons** ~~missing children or children~~ who need to be placed under protection **as referred to in Article 32(2)(a), (c) and (d),** the executing Member State shall ~~consult~~ immediately **consult its own competent authorities and those in** the issuing Member State **through the exchange of supplementary information** in order to agree without delay on the measures to be taken ~~in order to safeguard the best interest of the child~~. The competent authorities **in the executing Member State** may**, in accordance with national law,** ~~, in the cases referred to in Article 32(2)(a) and (c),~~ move the person to a safe place in order to prevent him or her from continuing his journey~~, if so authorised by national law~~.

2. The communication, other than between the competent authorities, of data on a missing person who has been located and who is of age shall be subject to that person's consent. The competent authorities may, however, communicate the fact that the alert has been erased because the missing person has been located to the person who reported the person missing.

[91] UK entered a scrutiny reservation on this Article.

CHAPTER VIII

ALERTS ON PERSONS SOUGHT TO ASSIST WITH A JUDICIAL PROCEDURE

Article 34

Objectives and conditions for issuing alerts

1. For the purposes of communicating the place of residence or domicile of persons, Member States shall, at the request of a competent authority, enter in SIS data on:

   (a) witnesses;

   (b) persons summoned or persons sought to be summoned to appear before the judicial authorities in connection with criminal proceedings in order to account for acts for which they are being prosecuted;

   (c) persons who are to be served with a criminal judgment or other documents in connection with criminal proceedings in order to account for acts for which they are being prosecuted;

   (d) persons who are to be served with a summons to report in order to serve a penalty involving deprivation of liberty.

2. Where there is a clear indication that vehicles, boat**s** or aircraft are connected with a person subject of an alert pursuant to paragraph 1, alerts on those vehicles, boats and aircraft may be issued in order to locate the person. In such cases the alerts on the person and the alert on the object shall be linked in accordance with Article 60. ~~The technical rules necessary for entering, updating, deleting and searching the data referred to in this paragraph shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2)~~[92].

[92] Moved to paragraph 3.

3.[93] The Commission shall adopt implementing acts to lay down and develop technical rules necessary for entering, updating, deleting and searching the data referred to in paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72(2).

Article 35

Execution of the action based on an alert

Requested information shall be communicated to the requesting Member State through the exchange of supplementary information.

CHAPTER IX
ALERTS ON PERSONS AND OBJECTS FOR DISCREET CHECKS, INQUIRY CHECKS OR SPECIFIC CHECKS

Article 36[94]

Objectives and conditions for issuing alerts

1. Data on persons or **the objects referred to in Article 38(2)(a), (b), (c), (e), (g), (h), (j), (k) and non-cash means of payment** shall be entered in accordance with the national law of the Member State issuing the alert, for the purposes of discreet checks, inquiry checks or specific checks in accordance with Article 37**(3),** (4) **and (5)**.

1a. When issuing alerts for the purposes of discreet checks, inquiry checks or specific checks and where the information sought by the issuing Member State is additional to that provided for in Article 37(1), the issuing Member State shall add to the alert all information being sought.[95]

---

93 Moved from paragraph 2, *in fine*.

94 DE, FR, HU, IE, IT, LV (on inquiry checks only), PL, PT, SI, RO and UK have entered a reservation on this Article.

95 FR and PL entered a scrutiny reservation on this paragraph.

2. The alert may be issued for the purposes of **preventing, detecting, investigating or** prosecuting criminal offences, executing a criminal sentence and for the prevention of threats to public security:

   (a) where there is a clear indication that a person intends to commit or is committing a serious crime, in particular the offences referred to in Article 2(2) of the Framework Decision 2002/584/JHA; **or**

   (b) where the information referred to in Article 37(1) is necessary for the execution of a criminal ~~sentence~~ **penalty** of a person convicted of a serious crime, in particular the offences referred to in Article 2(2) of the Framework Decision 2002/584/JHA[96]; or

   (c) where an overall assessment of a person, in particular on the basis of past criminal offences, gives reason to believe that that person may also commit serious crimes in the future, in particular the offences referred to in Article 2(2) of the Framework Decision 2002/584/JHA.

3. In addition, an alert may be issued in accordance with national law, at the request of the authorities responsible for national security, where ~~there is a concrete indication that~~ the information referred to in Article 37(1) is necessary in order to prevent a serious threat by the person concerned or other serious threats to internal or external national security. The Member State issuing the alert pursuant to this paragraph shall inform the other Member States thereof. Each Member State shall determine to which authorities this information shall be transmitted **via its SIRENE Bureau**.

4. Where there is a clear indication that **the objects referred to in Article 38(2)(a), (b), (c), (e), (g), (h), (j), (k) or non-cash means of payment**~~vehicles, boats, aircraft and containers~~ are connected with the serious crimes referred to in paragraph 2 or the serious threats referred to in paragraph 3, alerts on those **objects** ~~vehicles, boats, aircraft and containers~~ may be issued **and linked to the alerts inserted pursuant to paragraphs 2 and 3**.

---

96 FI entered a scrutiny reservation on this point.

5. ~~Where there is a clear indication that blank official documents or isued identity documents are connected with the serious crimes referred to in paragraph 2 or the serious threats referred to in paragraph 3, alerts on those documents, regardless of the identity of the original holder of the identity document, if any, may be issued. The technical rules necessary for entering, updating, deleting and searching the data referred to in this paragraph shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).~~ **[97]**

6.[98] The technical rules necessary for entering, updating, deleting and searching the data referred to in paragraph (4) as well as the additional information referred to in paragraph 1a shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).

Article 37 **[99]**

Execution of the action based on an alert

1. For the purposes of discreet checks, inquiry checks or specific checks, all or some of the following information shall be collected and communicated to the ~~authority~~ issuing ~~the alert when border control checks, police and customs checks or other law enforcement activities are carried out within a~~ Member State:

   (a) the fact that the person for whom, or the **objects referred to in Article**~~vehicle, boat, aircraft, container, blank official document or issued identity paper~~ **38(2)(a), (b), (c), (e), (g), (h), (j), (k) or non-cash means of payment** for which an alert has been issued, has **or have** been located;

   (b) the place, time and reason for the check;

---

97 Moved to paragraph 6.

98 Moved from paragraph 5 *in fine*.

99 AT, FR, IT, LV (on inquiry checks only), PL and SI have entered a reservation on this Article.

(c) the route of the journey and destination ;

(d) the persons accompanying the person concerned or the occupants of the vehicle, boat or aircraft or accompanying the holder of the blank official document or issued identity document who can reasonably be expected to be associated with the persons concerned;

(e) the identity revealed and personal description of the person using the blank official document or issued identity paper subject of the alert;

(f) **objects referred to in Article 38(2)(a), (b), (c), (e), (g), (h), (j), (k) or non-cash means of payment** ~~the vehicle, boat, aircraft or container~~ used;

(g) objects carried, including travel documents;

(h) the circumstances under which the person or the **motor** vehicle, **trailer, caravan,** boat, **container,** aircraft, ~~container,~~ blank official document or issued identity ~~paper~~**documents or non-cash means of payment** was located**;**

(i) other information, the collection of which may have been requested by the issuing Member State in accordance with Article 36(1a).

2. The information referred to in paragraph 1 shall be communicated through the exchange of supplementary information.

3. ~~Depending on the operational circumstances and in accordance with national law, a~~**A** discreet check shall comprise **the discreet collection of as much information described in paragraph 1 as possible during routine activities carried out by the competent national authorities**. **The collection of this information shall not jeopardise the discreet nature of the checks and the subject of the alert shall in no way be made aware as to the existence of the alert.**

4. ~~Depending on the operational circumstances and in accordance with national law~~**A**n inquiry check shall comprise **the** ~~a more in-depth check and a questioning~~ **interviewing** of the person~~. Where inquiry checks are not authorised by the law of a Member State, they shall be replaced by discreet checks in that Member State~~[100]**, including on the basis of information or specific questions added to the alert by the issuing Member State. The interview shall be carried out in accordance with the national law of the executing Member State.** ~~The person may be informed about the alert or the issuing authority.~~

5. During specific checks, persons, vehicles, boats, aircraft, containers and objects carried, may be searched ~~in accordance with national law~~ for the purposes referred to in Article 36. Searches shall be carried out in accordance with national law. ~~Where specific checks are not authorised by the law of a Member State, they shall be replaced by inquiry checks in that Member State.~~[101]

6. Where specific checks are not authorised by ~~the~~ **national** law ~~of a Member State~~, they shall be replaced by inquiry checks in that Member State[102]**. Where inquiry checks are not authorised by national law, they shall be replaced by discreet checks in that Member State**[103]**.**

7. Paragraph 6 is without prejudice to the obligation of Member States to make available to the end-users all additional information referred to in Article 36(1a) and to ensure that this information is collected and communicated to the issuing Member State through the exchange of supplementary information.

---

100 Moved to new paragraph 6.
101 Moved to new paragraph 6.
102 Moved from paragraph 5.
103 Moved from paragraph 4.

CHAPTER X

ALERTS ON OBJECTS FOR SEIZURE OR USE AS EVIDENCE IN CRIMINAL PROCEEDINGS

Article 38

Objectives and conditions for issuing alerts

1. Data on objects sought for the purposes of seizure ~~for law enforcement purposes~~ or **for** use as evidence in criminal proceedings shall be entered in SIS.

2. The following categories of readily identifiable objects shall be entered:

   (a) motor vehicles~~, as defined by national law,~~ regardless of the propulsion system;

   (b) trailers with an unladen weight exceeding 750 kg;

   (c) caravans;

   (d) industrial equipment;

   (e) boats;

   (f) boat engines;

   (g) containers;

   (h) aircraft;

   (ha) aircraft engines;

   (i) firearms;

   (j) blank official documents which have been stolen, misappropriated**,** ~~or~~ lost **or purport to be such a document but are false**;

(k) issued identity documents such as passports, identity cards, ~~driving licenses,~~ residence permits**,** ~~and~~ travel documents and **as well as driving licenses** which have been stolen, misappropriated, lost or, invalidated or purport to be such a document but are fals~~ified~~;

(l) vehicle registration certificates and vehicle number plates which have been stolen, misappropriated, lost, or invalidated or purport to be such a document or plate but are fals~~ified~~;

(m) banknotes (registered notes) and fals~~ified~~ banknotes;

(n) ~~technical equipment,~~information technology items ~~and other high-value readily identifiable objects~~[104];

(o) identifiable component parts of motor vehicles;

(p) identifiable component parts of industrial equipment**;**

(q) other identifiable objects of high-value[105], as defined in accordance with paragraph 3.

With regard to the documents referred to in paragraphs 2(j), (k) and (l), the issuing Member State may specify whether such documents are stolen, misappropriated, lost, invalidated or false.

3. The definition of new sub-categories of object**s** under paragraph 2(n)**, (o), (p) and (q)** and 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 72(2).

---

104 Moved to new point (q).
105 Moved from point (n).

Article 39

Execution of the action based on an alert

1. Where a search brings to light an alert for an object which has been located, the authority which matched the two items of data shall in accordance with national law seize the object and contact the authority which issued the alert in order to agree on the measures to be taken. For this purpose, personal data may also be communicated in accordance with this Regulation.[106]

2. The information referred to in paragraph 1 shall be communicated through the exchange of supplementary information.

3. The Member State which located the object shall take the requested measures in accordance with national law.

[106] NL entered a scrutiny reservation on this paragraph.

CHAPTER XI

ALERTS ON UNKNOWN WANTED PERSONS FOR IDENTIFICATION ACCORDING TO NATIONAL LAW ~~AND SEARCH WITH BIOMETRIC DATA~~[107]

Article 40[108]

*Alerts on unknown wanted person for ~~apprehension~~ **identification** under national law*

Dactylo**sco**graph~~h~~ic data may be entered in SIS, not related to persons who are subject of the alerts. These dactylo**sco**graph~~h~~ic data shall be either complete or incomplete sets of fingerprints or palm prints **that are** discovered at the scenes of **serious** crimes **or terrorist offences** under investigation, ~~of serious crime and terrorist offence~~ and where it can be established to a high degree of probability that they belong to ~~the~~ **a** perpetrator of the offence.

The dactylo**sco**graph~~h~~ic data in this category shall be stored as "unknown suspect or wanted person" **and shall only be stored where**~~provided that~~ the competent authorities **of the issuing Member State** cannot establish the identity of the person by using any other national, European or international database.

Article 41[109]

Execution of the action based on an alert

In the event of a hit ~~or a potential match~~ with the data stored pursuant to Article 40, the identity of the person shall be established in accordance with national law, together with **expert** verification that the dactylo**sco**graph~~h~~ic data stored in SIS belong to the person. Member States shall communicate **information about the identity and the whereabouts of the person** ~~by using~~**through the exchange of** supplementary information in order to facilitate timely investigation of the case.

---

[107] Moved to new Chapter XIa.

[108] BE, DE, FR, EL, IE, PT and UK entered a scrutiny reservation on this paragraph.

[109] EL entered a scrutiny reservation on this Article.

CHAPTER XIa
SPECIFIC RULES FOR BIOMETRIC DATA

*Article **41A (ex-Article** 22**)***

*Specific rules for entering photographs, facial images, dactylo~~graphic~~**scopic** data and DNA profiles*

1. The entering into SIS of data referred to in Article 20(3)(w), (x) and (y) shall be subject to the following provisions:

   (a) Photographs, facial images, dactylo~~graphic~~**scopic** data and DNA profiles shall only be entered following a quality check to ascertain the fulfilment of a minimum data quality standard.

   (b) A DNA profile may only be added to alerts provided for in Article 32(2)(a) and (c) and only where photographs, facial images or dactylo~~graphic~~**scopic** data suitable for identification are not available **or not sufficient**. The DNA profiles of persons who are direct ascendants, descendants or siblings of the alert subject may be added to the alert provided that those persons concerned give~~s~~ explicit consent. ~~The racial origin of the person shall not be included in the DNA profile.~~

2. Quality standards shall be established for the storage of the data referred to under paragraph 1(a) of this Article and Article 40. 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 72(2).

Article 42

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

1. Photographs, facial images, dactylo**sco**~~graph~~ic data and DNA profiles 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.[110] ~~Dactylographic data stored in SIS shall be searched for identification purposes i~~**I**f the identity of the person cannot be ascertained by other means **dactyloscopic data shall be** ~~used~~ **searched for identification purposes**. Dactylo**sco**~~graph~~ic data may ~~also~~ be ~~used~~ **searched in all cases** to identify a person.

3. Dactyloscopic data stored in SIS in relation to alerts issued pursuant to Articles 26, **32,** 34~~(1) b) and d)~~**, 36** and ~~Article 36~~ **40** may also be searched by using complete or incomplete sets of fingerprints or palm prints discovered at the scenes of **serious** crimes **or terrorist offences**[111] 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 the functionality is implemented, the Commission shall present a report on the availability and readiness of the required technology, on which the European Parliament shall be consulted.**[58] Identification based on photographs or facial images shall ~~only~~ be used **subject to national law** ~~at regular border crossing points where self-service systems and automated border control systems are in use~~.

---

[110] A new corresponding recital would be inserted with the following text: *Member States may choose to use dactyloscopic data in all cases, to identify a person. Wherever the identity of the person cannot be ascertained by any other means, Member States shall use dactyloscopic data in order to attempt to ascertain the identity*.

[111] In line with Article 40.

CHAPTER XII

RIGHT TO ACCESS AND RETENTION OF ALERTS

Article 43[112]

Authorities having a right to access alerts

1. **National competent authorities shall have access 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 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;[59]

   (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) 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;

---

112 In line with Article 29 of the proposal for Border Checks (see 9593/17).

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 naturalization, in the performance of their tasks, as provided for in national law, and by their coordinating authorities.**

2. 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 law, and by their coordinating authorities.

3. The right to access data entered in SIS and to search such data directly may be exercised by the authorities competent to carry out the tasks referred to in paragraph 1(c) in the performance of these tasks. The access 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 53(8).

Article 44[113]

Vehicle registration authorities

1. The services in the Member States responsible for issuing registration certificates for vehicles, as referred to in Council Directive 1999/37/EC[114], shall have access to ~~the following~~ data entered into SIS in accordance with Article 38(2)(a), (b), (c)**,** ~~, and~~ (l) **and (o)** of this Regulation for the sole purpose of checking whether **motor** vehicles **and accompanying vehicle registration certificates and vehicle number plates** presented to them for registration have been stolen, misappropriated or lost **or purport to be such a document but are false** or are sought as evidence in criminal proceedings~~:~~**.**

[113] PL entered a scrutiny reservation on this Article

[114] Council Directive 1999/37 of 29 April 1999 on the registration of documents for vehicles (OJ L 138, 1.6.1999, p. 57).

~~(a) data on motor vehicles, as defined by national law, regardless of the propulsion system;~~

~~(b) data on trailers with an unladen weight exceeding 750 kg and caravans;~~

~~(c) data concerning vehicle registration certificates and vehicle number plates which have been stolen, misappropriated, lost or invalidated.~~

Access to those data by the services responsible for issuing registration certificates for vehicles shall be governed by the national law of that Member State.

2. Services as referred to in paragraph 1 that are government services shall have the right to access directly the data entered in SIS.

3. Services as referred to in paragraph 1 that are non-government services shall have access to data entered in SIS only through the intermediary of an authority as referred to in Article 43 of this Regulation. That authority shall have the right to access those data directly and to pass them on to the service concerned. The Member State concerned shall ensure that the service in question and its employees are required to respect any limitations on the permissible use of data passed on to them by the authority.

4. Article 39 of this Regulation shall not apply to access gained in accordance with this Article. The communication to the police or judicial authorities by services as referred to in paragraph 1 of any information brought to light by access to SIS ~~which gives rise to suspicion of the commission of a criminal offence~~ shall be governed by national law.

Article 45

Registration authorities for boats and aircraft

1. The services in the Member States responsible for issuing registration certificates or ensuring traffic management for boats, including boat engines and aircraft shall have access to the following data entered into SIS in accordance with Article 38(2) of this Regulation for the sole purpose of checking whether boats, including boat engines; aircraft or containers presented to them for registration or subject of traffic management have been stolen, misappropriated or lost or are sought as evidence in criminal proceedings:

(a) data on boats;

(b) data on boat engines;

(c) data on aircraft.

Subject to paragraph 2, the law of each Member State shall govern access to those data by those services in that Member State. Access to the data listed (a) to (c) above shall be limited to the specific competence of the services concerned.

2. Services as referred to in paragraph 1 that are government services shall have the right to access directly the data entered in SIS.

3. Services referred to in paragraph 1 that are non-government services shall have access to data entered in SIS only through the intermediary of an authority as referred to in Article 43 of this Regulation. That authority shall have the right to access the data directly and to pass those data on to the service concerned. The Member State concerned shall ensure that the service in question and its employees are required to respect any limitations on the permissible use of data conveyed to them by the authority.

4. Article 39 of this Regulation shall not apply to access gained in accordance with this Article. The communication to the police or judicial authorities by services as referred to in paragraph 1 of any information brought to light by access to SIS which gives rise to suspicion of a criminal offence shall be governed by national law.

Article 45A[115]

Registration authorities for firearms

1. The services in the Member States responsible for issuing registration certificates for firearms, shall have access to data on persons subject to an alert under Article 26 or 36 and firearms entered into SIS in accordance with Article 38(2) of this Regulation for the purpose of checking whether the person requesting registration represents a threat to public or national security or whether firearms presented to them for registration are sought for seizure or for use as evidence in criminal proceedings.

2. Access to those data by those services shall be governed by the national law of that Member State.[116] Access to those data shall be limited to the specific competence of the services concerned.

3. Services as referred to in paragraph 1 that are competent authorities may have the right to access directly the data entered in SIS.

4. Services as referred to in paragraph 1 that are not competent authorities shall have access to data entered in SIS through intermediation by an authority referred to in Article 43 of this Regulation. The intermediating authority shall have the right to access the data directly and shall inform the service concerned if the firearm can be registered or not. The Member State shall ensure that the service in question and its employees are required to respect any limitations o the permissible use of data conveyed to them by the intermediating authority.

5. Article 39 shall not apply to access gained in accordance with this Article. The communication to the police or the judicial authorities by services as referred to in paragraph 1 of any information brought to light by access to SIS shall be governed by national law.

---

115 AT entered a scrutiny reservation on this Article.

116 Wording in line with Article 44(1), last subparagraph.

Article 46

Access to SIS data by Europol

1. The European Union Agency for Law Enforcement Cooperation (Europol) shall have, within its mandate, 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**.[117]

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 the 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.

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 operational analyses as defined in points (a) 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 ~~concerned~~. 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.~~ [118]

---

117 SK entered a scrutiny reservation on this paragraph.

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

5. Europol shall:

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

(aa) notwithstanding Article 31(1) of Regulation (EU) 2016/794, delete supplementary information containing personal data at the latest one year after the related alert has been deleted from SIS, unless the continued storage of the data is deemed necessary, on the basis of information that is more extensive than that possessed by the data provider, in order for Europol to perform its tasks. Europol shall inform the data provider of the continued storage of such data and present a justification of such continued storage;

(b) limit access to data entered in SIS**, including supplementary information,** to specifically authorised staff of Europol;

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

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

6. Data may only be copied for technical purposes, provided that such copying is necessary in order for duly authorised Europol staff to carry out a direct search. The provisions of this Regulation shall apply to such copies. The technical copy shall be used for the purpose of storing SIS data whilst those data are searched. Once the data have been searched they shall be deleted. Such uses shall not be construed to be an unlawful downloading or copying of SIS data. Europol shall not copy alert data or additional data issued by Member States or from CS-SIS into other Europol systems.

7. ~~Any copies, as referred to in paragraph 6, which lead to off-line databases may be retained for a period not exceeding 48 hours. That period may be extended in an emergency until the emergency comes to an end. Europol shall report any such extensions to the European Data Protection Supervisor.~~

8. ~~Europol may receive and process supplementary information on corresponding SIS alerts provided that the data processing rules referred to in paragraphs 2~~**5** ~~to 7 are applied as appropriate.~~

9. For the purpose of verifying the lawfulness of data processing, self-monitoring and ensuring proper data security and integrity Europol ~~should~~ **shall** keep log**s** 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 47

Access to SIS data by Eurojust

1. The national members of Eurojust and their assistants shall, within their mandate, have the right to access and search data entered in SIS within their mandate, in accordance with Articles 26, 32, 34 38 and 40.

2. Where a search by a national member of Eurojust reveals the existence of an alert in SIS, he or she shall inform the issuing Member State **thereof**. **Any communication of information obtained from such a search may only be communicated to third countries and third bodies with the consent of the issuing Member State.**

3. Nothing in this Article shall be interpreted as affecting the provisions of Decision 2002/187/JHA concerning data protection and the liability for any unauthorised or incorrect processing of such data by national members of Eurojust or their assistants, or as affecting the powers of the Joint Supervisory Body set up pursuant to that Decision.

4. Every access and search made by a national member of Eurojust or an assistant shall be logged in accordance with the provisions of Article 12 and every use made by them of data accessed by them shall be logged.

5. No parts of SIS shall be connected to any computer system for data collection and processing operated by or at Eurojust nor shall the data contained in SIS to which the national members or their assistants have access be transferred to such a computer system. No part of SIS shall be downloaded. The logging of access and searches shall not be construed to be an unlawful download or copying of SIS data.

6. Access to data entered in SIS shall be limited to the national members and their assistants and shall not be extended to Eurojust staff.

7. Measures to ensure security and confidentiality as provided for in Articles 10 and 11 shall be adopted and applied.

Article 48[119]

*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 team***s**

1. ~~In accordance with Article 40(8) of Regulation (EU) 2016/1624,~~ **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**, 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 43**, 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.** [120]

[119] NL entered a scrutiny reservation with respect to the provisions regarding ETIAS.
[120] Text moved from paragraph 5.

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 49(1).

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 team**s** reveals the existence of an alert in SIS, the issuing Member State shall be informed thereof. In accordance with Article 40 of Regulation (EU) 2016/1624, members of the teams may only act in response to an alert in SIS under instructions from and, as a general rule, in the presence of border guards or staff involved in return-related tasks of the host Member State in which they are operating. The host Member State may authorise members of the teams to act on its behalf.

4. Every instance of access and every search made by a member of the European Border and Coast Guard teams or teams of staff involved in return-related tasks or by a member of the migration management support team**s** shall be logged in accordance with the provisions of Article 12 and every use made by them of data accessed by them shall be 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 team and shall not be extended to any other team members.~~[121]

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**easures to ensure security and confidentiality as provided for in Articles 10 and 11 ~~shall be adopted and applied.~~

[121] Merged with paragraph 1.

Article 49[122]

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

1. For the purposes of Article 48(1) **[**and ~~paragraph 2 of this~~ Article **49A]** the European Border and Coast Guard Agency shall set up and maintain a technical interface which allows a direct connection to Central SIS.

2.[123] ~~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 26, 32, 34, 36 and 38(2) (j) and (k).~~

3.[124] ~~Where a verification by the European Border and Coast Guard Agency reveals the existence of an alert in SIS the procedure set out in Article 22 of Regulation establishing a European Travel Information and Authorisation System (ETIAS) applies.~~

4. 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.

5. 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 each use made of data accessed by them shall be ~~registered~~ **logged**.

6. **Except in cases where paragraph 1 of this Article applies**, 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.

---

122 NL entered a reservation on this Article.
123 Paragraph moved to Article 49A(1).
124 Paragraph moved to Article 49A(2).

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

[Article 49A[125]

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 26, 32, 34, 36 and 38(2)(j) and (k).

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 20A and 22 of Regulation establishing a European Travel Information and Authorisation System (ETIAS) applies.][126]

Article 49B

Evaluation of the use of SIS by Europol, Eurojust and the European Border and Coast 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, Eurojust and the European Border and Coast 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.

---

125 Provisions moved from Article 49(2) and (3).

126 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), and its date of entry into force.

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, Eurojust 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.

6. In light of the findings and the assessments contained in that evaluation report, the Commission shall draft recommendations for remedial action aimed at addressing any deficiencies identified during the evaluation and give an indication of the priorities for implementing them, as well as, where appropriate, examples of good practices.

7. Following an evaluation, Europol, Eurojust and the European Border and Coast Guard Agency shall provide the Commission with an action plan to remedy any deficiencies identified in the evaluation report and shall thereafter continue to report on progress every three months until the action plan is fully implemented.

Article 50

Scope of access

End-users, including Europol, the national members of Eurojust and their assistants**,** ~~as well as~~ 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 51[127]

Retention period of alerts ***- persons***[128]

1. Alerts **on persons** 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. **Concerning alerts on persons:**

   (a) A Member State may issue an alert for a period of five years.

   (b) ~~A~~ **The issuing** Member State ~~issuing an alert~~ shall, within five years of **the alert's** ~~its~~ entry into SIS, review the need to retain it. ~~Alerts issued for the purposes of Article 36 of this Regulation shall be kept for a maximum period of one year.~~[129]

---

127 FI and UK entered a scrutiny reservation on this Article.

128 A new Article 51A was incorporated to rule the retention period of alerts on objects.

129 Moved to paragraph 3.

3. ~~Alerts on blank official documents, and issued identity documents entered in accordance with Article 38 shall be kept for a maximum of 10 years.Shorter retention periods for categories of object alerts may be established by means of implementing measures adopted in accordance with the examination procedure referred to in Article 72(2).~~

By way of derogation to paragraph 2, concerning alerts issued for the purposes of **Article 32 (2)(c) and (d) and** Article 36 of this Regulation[130]**:**

(a) A Member State may issue an alert for a period of one year.

(b) The issuing Member State shall, within one year of the alert's entry into SIS, review the need to retain it.

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

5. **Within the review period, the issuing Member State 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 on a person was issued. In such a case paragraph 2(a) or paragraph 3(a) as appropriate, shall apply also to the extension. Any extension of an alert shall be communicated to CS-SIS.**[131]132

130 Text partially moved from paragraph 2.
131 Moved from paragraph 2a.
132 HU entered a scrutiny reservation on this paragraph

~~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 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 be deleted by the staff of the SIRENE Bureau. SIRENE Bureaux shall report any recurring issues in this area to their national supervisory authority.~~[133]

6. ~~Within the review period, the Member State issuing the alert may, following a comprehensive individual assessment, which shall be logged, 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.~~[134]

Alerts shall automatically be ~~erased~~**deleted** after the review period referred to in paragraphs 2**(b) and 3(b)** except where the **issuing** Member has informed CS-SIS about the extension of the alert **on a person** 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.[135]

[133] Moved to paragraph 8.
[134] Moved to paragraph 2a.
[135] Moved from paragraph 7.

7. ~~Alerts shall automatically be erased after the review period referred to in paragraph 2 except where the Member State issuing the alert has informed CS-SIS about the extension of the alert pursuant to paragraph 6. CS-SIS shall automatically inform the Member States of the scheduled deletion of data from the system four months in advance.~~[136]

   Member States shall keep statistics about the number of alerts **on persons** for which the retention period has been extended in accordance with paragraph ~~6~~**5**.[137]

8. ~~Member States shall keep statistics about the number of alerts for which the retention period has been extended in accordance with paragraph 6.~~[138]

   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 issue 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[139]. SIRENE Bureaux shall report any recurring issues in this area to their national supervisory authority.[140]

---

136 Moved to paragraph 6.
137 Moved from paragraph 8.
138 Moved to paragraph 7.
139 AT, DE, PL, SI and CH expressed concerns regarding the deletion of alerts by the SIRENE Bureaux.
140 Moved from paragraph 5.

Article 51A[141][142]

Retention period of alerts - objects

1. Alerts on objects 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. Concerning alerts on objects:

(a) a Member State may issue an alert for objects for a period of 10 years.

(b) A Member State may issue an alert for other objects in accordance with Articles 26, 32, 34, 36 or 38 for a period of five years if they are linked to alerts on persons.

(c) The retention periods referred to in paragraphs 2(a) and (b) may be extended should this prove necessary for the purposes for which the alert was issued. In such cases paragraphs (2)(a) and (b) shall also apply to the extension.

(d) Shorter retention periods for categories of object alerts may be established by means of implementing measures adopted in accordance with the examination procedure referred to in Article 72(2).

3. Member States shall keep statistics about the number of alerts on objects for which the retention period has been extended in accordance with paragraph 2(c).

[141] This new Article regards specifically the retention period for alerts on objects, and mirrors, mutatis mutandis, the provisions on retention period of alerts on persons (Article 51).

[142] A recital would be added concerning the obligation of MS to review the alerts regularly.

CHAPTER XIII
DELETION OF ALERTS

Article 52[143]

Deletion of alerts

1. Alerts for arrest for surrender or extradition purposes pursuant to Article 26 shall be deleted once the person has been surrendered or extradited to the competent authorities of the issuing Member State. They **shall**~~may~~ also be deleted where the judicial decision on which the alert was based has been revoked by the competent judicial authority according to national law.

2. Alerts for missing **persons, children at risk of abduction or vulnerable** persons **pursuant to Article 32** shall be deleted in accordance with the following rules:

   (a) Concerning missing children~~,~~ **and children at risk of abduction** ~~pursuant to Article 32~~, an alert shall be deleted upon:

   – the resolution of the case, such as when the child has been repatriated or the competent authorities in the executing Member State have taken a decision on the care of the child);

   – the expiry of the alert in accordance with Article 51;

   – a decision by the competent authority of the issuing Member State; or

   – ~~the location of the child.~~

   – **when the risk of abduction is no longer present.**

[143] UK entered a scrutiny reservation on this Article.

(b) Concerning missing adults ~~pursuant to Article 32~~, where no protective measures are requested, an alert shall be deleted upon:

– the execution of the action to be taken (whereabouts ascertained by the executing Member State);

– the expiry of the alert in accordance with Article 51; or

– a decision by the competent authority of the issuing Member State.

(c) Concerning missing adults where protective measures are requested~~, pursuant to Article 32,~~ an alert shall be deleted upon:

– the carrying out of the action to be taken (person placed under protection);

– the expiry of the alert in accordance with Article 51; or

– a decision by the competent authority of the issuing Member State.

(d) Concerning vulnerable persons who need to be prevented from travel for their own potection an alert shall be deleted upon:

– **the carrying out of the action to be taken (person placed under protection);**

– **the expiry of the alert in accordance with Article 51; or**

– **a decision by the competent authority of the issuing Member State.**[144]

Subject to national law, where a person has been interned following a decision by a competent authority an alert may be retained until that person has been repatriated.

[144] Text similar to that of point (c).

3. ~~Alerts on persons sought for a judicial procedure shall be deleted in accordance with the following rules:~~

Concerning alerts on persons sought for a judicial procedure pursuant to Article 34 an alert shall be deleted upon:

(a) the communication of the whereabouts of the person to the competent authority of the issuing Member State. Where the information forwarded cannot be acted upon the SIRENE Bureau of the issuing Member State shall inform the SIRENE Bureau of the executing Member State in order to resolve the problem;

(b) the expiry of the alert in accordance with Article 51; or

(c) a decision by the competent authority of the issuing Member State.

Where a hit has been achieved in a Member State and the address details were forwarded to the issuing Member State and a subsequent hit in that Member State reveals the same address details the hit shall be ~~logged~~ **recorded** in the executing Member State but neither the address details nor supplementary **information** shall be resent to the issuing Member State. In such cases the executing Member State shall inform the issuing Member State of the repeated hits and the issuing Member State shall consider the need to maintain the alert.

4. ~~Alerts on discreet, inquiry and specific checks shall be deleted in accordance with the following rules:~~

Concerning alerts on discreet, inquiry and specific checks, pursuant to Article 36, an alert shall be deleted upon:

(a) the expiry of the alert in accordance with Article 51;

(b) a decision to delete by the competent authority of the issuing Member State.

5. ~~Alerts on objects for seizure or use as evidence shall be deleted in accordance with the following rules:~~

Concerning deletion of alerts on objects for seizure or use as evidence in criminal proceedings pursuant to Article 38 an alert shall be deleted upon:

(a) the seizure of the object or equivalent measure once the necessary follow-up exchange of supplementary information has taken place between SIRENE Bureaux or the object becomes subject of another judicial or administrative procedure;

(b) the expiry of the alert; or

(c) a decision to delete by the competent authority of the issuing Member State.

6. Alerts on unknown wanted persons pursuant to Article 40 shall be deleted in accordance with the following rules:

~~7.~~ (a) the identification of the person; or

~~8.~~ (b) the expiry of the alert.

CHAPTER XIV
GENERAL DATA PROCESSING RULES

Article 53

Processing of SIS data

1. The Member States may process the data referred to in Article 20 only for the purposes laid down for each category of alert referred to in Articles 26, 32, 34, 36, 38 and 40.

2. Data may only be copied for technical purposes, provided that such copying is necessary in order for the authorities referred to in Article 43 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.

4. 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.

5. Access to data shall only be authorised within the limits of the competence of the national authorities referred to in Article 43 and to duly authorised staff.

6.[145] With regard to the alerts laid down in Articles 26, 32, 34, 36, 38 and 40 of this Regulation, any processing of information contained therein 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 Member State issuing the alert shall be obtained for this purpose.

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 54

SIS data and national files

1. Article 53(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 53(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.

[145] UK entered a scrutiny reservation on this paragraph.

Article 55

Information in case of non-execution of alert

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

Article 56

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**[146].

146 Text inspired on Article 49(4) of Council Decision 2007/533/JHA.

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 59.

6. Where a person is already the subject of an alert in SIS, a Member State which enters a further alert shall **observe the compatability and priority of alerts and, where necessary, 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 57

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, Eurojust and the European Border and Coast Guard Agency** shall notify the Commission, the Agency and the national supervisory authority of security incidents. The Agency shall notify the Commission and the European ~~d~~**D**ata Protection Supervisor of security incidents.

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

Article 58

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 56(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 59

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),~~**;**

(d) name~~(s)~~ at birth**;**

(e) previously used names and any aliases possibly entered separately;

(f) any specific objective**,** ~~and~~ physical characteristic not subject to change;

(g) place of birth;

(h) date of birth;

(i) ~~sex~~**gender**;

(j) photographs and facial images;

(k) ~~fingerprints~~**dactyloscopic data**;

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

(m) the category of the person's identi**fication**~~ty~~ document**s;**

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

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

(p) the date of issue of a person's i~~dentity~~**identification** document**s;**

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

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

(s) **person**~~victim~~'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 72(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 60

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 referred to in Article 72(2).

Article 61

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 62

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.

Article 63

~~*Exchange of data on stolen, misappropriated, lost or invalidated passports with Interpol*~~

~~1. By way of derogation from Article 62, the passport number, country of issuance and the document type of stolen, misappropriated, lost or invalidated passports entered in SIS may be exchanged with members of Interpol by establishing a connection between SIS and the Interpol database on stolen or missing travel documents, subject to the conclusion of an Agreement between Interpol and the European Union. The Agreement shall provide that the transmission of data entered by a Member State shall be subject to the consent of that Member State.~~

~~2. The Agreement referred to in paragraph 1 shall foresee that the data shared shall only be accessible to members of Interpol from countries that ensure an adequate level of protection of personal data. Before concluding this Agreement, the Council shall seek the opinion of the Commission on the adequacy of the level of protection of personal data and respect of fundamental rights and liberties regarding the automatic processing of personal data by Interpol and by countries which have delegated members to Interpol.~~

~~3. The Agreement referred to in paragraph 1 may also provide for access through SIS for the Member States to data from the Interpol database on stolen or missing travel documents, in accordance with the relevant provisions of this Decision governing alerts on stolen, misappropriated, lost and invalidated passports entered in SIS.~~

CHAPTER XV
DATA PROTECTION[147]

Article 64[148]

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. Decision 2002/187 (Eurojust) shall apply to the processing of personal data by Eurojust under this Regulation.**

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

---

147 Articles 46 to 52 (Proposal on Border Checks) are also applicable to Returns by virtue of Article 13 of the Returns Proposal.

148 DE entered a scrutiny reservation on this Article, in particular with regard to the relation between the different instruments.

3. **National provisions transposing Directive (EU) 2016/680 shall apply** ~~F~~**f**or processing of data by competent national authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences o**r**~~f~~ 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 65

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 ~~erasure~~**erased** shall be exercised in accordance with the law of the Member State before which they invoke that right.

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

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

4. [149] 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:

[149] SE entered a scrutiny reservation on this paragraph.

(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. ~~Any person has the right to have factually inaccurate data relating to him rectified or unlawfully stored data relating to him erased.~~

6. ~~The person concerned~~ **Following an application for access, rectification or erasure, the data subject** shall be informed as soon as possible ~~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~~**of application, as to the follow-up given to the exercise of these rights**[150].

7. ~~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.~~[151]

Article 66

Remedies

1. Any person may bring an action before the courts or **any competent** ~~the~~ authority ~~any competent authorities, including courts,~~ under the **national** law ~~of any Member State~~ to access, rectify, 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 70.

---

150 Paragraph merged with paragraph 7.

151 Merged with paragraph 6.

3. ~~In order to gain a consistent overview of the functioning of remedies~~ **T**he national authorities shall ~~develop a standard statistical system for reporting~~**(…) report** 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 rectified or 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) [152][153] the number of cases **in which a final court decision was handed down**[154] ~~which are heard before the courts;~~

~~(f)~~[155] ~~the number of cases where the court ruled in favour of the applicant in any aspect of the case~~; **and**

(g) [156] 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 69.

---

152 AT entered a scrutiny reservation on this paragraph.
153 SI, NL and LT suggested the deletion of this point. COM opposed.
154 Text from point (f).
155 Merged with point (e).
156 NL suggested the deletion of this point.

Article 67

Supervision of N.SIS

1. Each Member State shall ensure that the national supervisory authorit**y**~~(ies)~~ 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 authority, or the national supervisory authorit**y**~~(ies)~~ 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 68

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 69

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 XVI

LIABILITY ***AND PENALTIES***[157][158]

Article 70

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 70A

Penalties[159]

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.

---

157 Article 53 (Proposal on Border Checks) is also applicable to the Returns Proposal by virtue of Article 13 of the Returns Proposal.

158 "And Penalties" has been added, due to the inclusion of new Article 53A / 70A.

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

CHAPTER XVII

FINAL PROVISIONS[160]

Article 71

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 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. The statistics produced shall not contain any personal data. The annual statistical report shall be published. The Agency shall also provide annual statistics on the use of the functionality on making an alert issued ~~under~~ pursuant to Article 26 of this Regulation temporarily non-searchable, in total and for each Member State, including any extensions to the ~~retention~~**initial non-searchable** period of 48 hours.

4. Member States as well as Europol, Eurojust 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[161]**.**

---

160 Article 54 (Proposal on Border Checks) is also applicable to the Returns Proposal by virtue of Article 13 of the Returns Proposal.

161 Text moved to paragraph 4a.

4a.[162] This information shall include separate statistics on the number of searches carried out by, or on behalf of, by the services in the Member States responsible for issuing vehicle registration certificates and the services in the Member States responsible for issuing registration certificates or ensuring traffic management for boats, including boat engines; aircraft and containers. The statistics shall also show the number of hits per category of alert.

5. The Agency shall provide the Member States, the Commission, Europol, Eurojust 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**[163]**,** 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 ~~and~~**or** 5 of this Article and of 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, Eurojust 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.[164]

~~Detailed rules on the operation of the central repository and the data protection and security rules applicable to the repository shall be adopted by means of implementing measures adopted in accordance with the examination procedure referred to in Article 72(2).~~

---

162 Moved from paragraph 4.

163 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).

164 Text moved to paragraph 9.

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.

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.[165] **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 security rules applicable to **that repository. Those** implementing **acts shall be** adopted in accordance with the examination procedure referred to in Article 72(2).

Article 72

Committee procedure

1. The Commission shall be assisted by 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.

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

Article 73

Amendments to Regulation (EU) 515/2014[166]

~~Regulation (EU) 515/2014~~[167] ~~is amended as follows:~~

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

~~"6. 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 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 …)".~~[168]

Article 74

Repeal

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

Regulation (EC) No 1986/2006 of 20 December 2006 of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates;

---

166 UK is not participating in this Regulation.

167 ~~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).~~

168 Article removed, as this instrument does not amend Regulation (EU) 515/2014.

Council Decision ~~533/~~2007/**533**/JHA of 12 July 2007 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[169].

Article 75

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~~.

---

[169] 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).