Council of the European Union

Brussels, 14 June 2018
(OR. en)

9146/18

Interinstitutional Files:
2016/0408 (COD)
2016/0407 (COD)
2016/0409 (COD)

LIMITE

JAI 447
SIRIS 51
SCHENGEN 18
FRONT 145
ENFOPOL 258
COPEN 153
MIGR 68
COMIX 269
CODEC 816

NOTE

From:	Presidency
To:	Permanent Representatives Committee/ Mixed Committee at the level of Senior Officials (EU-Iceland/Norway and Switzerland/Liechtenstein)
Subject:	Schengen Information System (SIS) – Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) for the **return** of illegally staying third-country nationals (First reading) – Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of **border checks**, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006 (First reading) – 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 (First reading) *- Confirmation of the final compromise text with a view to agreement*

I. INTRODUCTION

1. On 22 December 2016 the Commission submitted to the Council a legislative package on the Schengen Information System (SIS). This package is composed of three separate proposals: a proposal for a Regulation of the European Parliament and of the Council on the use of the Schengen Information System for the return of illegally staying third-country nationals (hereinafter 'proposal on returns')[1]; a proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006 (hereinafter 'proposal on border checks')[2]; and a 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 (hereinafter 'proposal on police cooperation')[3].

   The reason the Commission tabled three different proposals was to respond to the different degrees of participation in the SIS of several groups of states ('variable geometry').

2. These proposals contain a series of measures aimed at maximising the effectiveness and efficiency of the SIS – the most widely used IT system in the area of freedom, justice and security in the EU – by technical enhancements, focusing on end-users and giving access to a greater number of national authorities and EU agencies. In particular, it is proposed that more categories of data, including biometrics, should be introduced, including for search purposes, and that new types of alert, including alerts on return decisions, should also be introduced.

3. The Working Party for Schengen Matters (Acquis) carried out a comprehensive examination of these proposals at numerous meetings from January to October 2017. The JHA Counsellors also examined the proposals on 26 and 29 September 2017 and on 5, 9 and 20 October 2017.

---

1 15812/16.
2 15813/16.
3 15814/16.

4. Taking into account the outcome of those meetings, on 8 November 2018 Coreper mandated the Presidency to start interinstitutional negotiations on the basis of the texts as set out in 14114/17 + COR 1 (proposal on returns), 14115/17 (proposal on border checks) and 14116/17 (proposal on police cooperation).

II. STATE OF PLAY

5. Trilogues took place on 16 November 2017, 13 December 2017, 7 February 2018, 22 March 2018, 12 April 2018, 24 April 2018, 22 May 2018 and 12 June 2018. Informal interinstitutional meetings, at technical and staff level, have taken place at quite an intensive pace since January 2018. The JHA Counsellors have met 14 times under the Bulgarian Presidency, to discuss compromise proposals resulting from and in preparation for the interinstitutional negotiations. During the last meeting, which was held on 8 June 2018, JHA Counsellors did not flag up any major issues to discuss further with the European Parliament.

6. During the last trilogue, which was held on 12 June 2018, a compromise was reached on the access to the SIS for state security services and on the issue of transferring personal data to third countries in the context of SIS return. In addition, all other compromise proposals agreed at technical level were confirmed at the trilogue.

7. During the interinstitutional negotiations that have taken place since January 2018, the Presidency has reached compromises that are compliant with the essential elements of the Council's negotiating mandate in relation to the most important issues: the technical architecture of the system; alerts for the purpose of entry and stay; alerts for discreet, inquiry and specific checks; alerts for missing and vulnerable persons; the entry into force and operation; the use of facial recognition technologies; access to the SIS for state security services; and implementing *versus* delegated acts. Therefore, the Presidency considers that the outcome of the negotiations provides a solid basis for an enhanced SIS which would be even more effective in helping to strengthen the security of the European Union.

III. CONCLUSION

8. Against this background, the Permanent Representatives Committee is invited to:

(a) approve the final compromise texts, as set out in annexes I to III to this note, as well as the draft statements related to the proposal on returns (on Ireland and on the synergies between the SIS and the Entry/Exit System), as set out in annexes IV and V to this note, and

(b) confirm that the Presidency can indicate to the European Parliament that, should the European Parliament adopt its position at first reading as regards the regulations as set out in annexes I to III to this note, subject to revision of those texts by the lawyer-linguists of both institutions, the Council would approve the European Parliament's position and the acts would be adopted with wording which corresponds to the European Parliament's position.

ANNEX I

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the use of the Schengen Information System for the return of illegally-staying third-country nationals

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 Article 79(2)(c) thereof,

Having regard to the proposal from the European Commission,

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

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The return of third-country nationals who do not fulfil or no longer fulfil the conditions for entry, stay or residence in the Member States, in full respect of fundamental rights and in particular the principle of non-refoulement, and in accordance with Directive 2008/115/EC of the European Parliament and of the Council, is an essential part of the comprehensive efforts to tackle irregular migration and increase the rate of return of irregular migrants.

(2) It is necessary to increase the effectiveness of the European system to return illegally staying third-country nationals. This is essential for maintaining public trust in the Union migration and asylum policy and providing support to persons in need of international protection.

(3) Member States should take all necessary measures to return illegally staying third-country nationals in an effective and proportionate manner, in accordance with the provisions of Directive 2008/115/EC.

(4) A system for sharing information between Member States using the SIS, as established by the Regulation (EU) 2018/ xxx [Border checks] [1] on return decisions issued in respect of third-country nationals staying illegally on the territory of the Member States and for monitoring whether third-country nationals subject to those decisions have left the territory of the Member States should be established.

(4a) This Regulation does not affect the rights and obligations of the third-country nationals laid down in Directive 2008/115/EC. The alert in the SIS for the purpose of return does not, in itself, constitute a determination of the status of the third country national on the territory of Member States, especially in Member States other than the alert issuing Member State.

(5) Regulation (EU) 2018/xxx [border checks] and Regulation (EU) 2018/xxx [police and judicial cooperation][2] lay down the conditions for the establishment, operation and use of the Schengen Information System (SIS).

(6) SIS alerts on return and the exchange of supplementary information on these alerts should support competent authorities to take the necessary measures to enforce return decisions. SIS should contribute to the identification and the information sharing between Member States on third-country nationals who are the subject of such return decision, who have absconded and are apprehended in another Member State. These measures should help prevent and deter irregular migration, secondary movements, and enhance cooperation between Member States' authorities.

---

[1] Regulation (EU) 2018/… on the establishment, use and operation of the Schengen Information System for the purposes of border checks (OJ L …).

[2] Regulation (EU) 2018/… on the establishment, use and operation of the Schengen Information System for the purposes of police and judicial cooperation in criminal matters (OJ L…).

(7) To ensure the effectiveness of return and increase the added value of alerts on return, Member States should enter alerts in SIS in relation to return decisions they issue to illegally staying third-country nationals in accordance with provisions respecting Directive 2008/115/EC. For this purpose, Member States should enter an alert in SIS also when decisions imposing or stating an obligation to return are issued in the situations described in Article 2(2) of that Directive, notably to third-country nationals who are subject to a refusal of entry in accordance with the Schengen Borders Code, or who are apprehended or intercepted by the competent authorities in connection with the irregular crossing by land, sea or air of the external border of a Member State and who have not subsequently obtained an authorisation or a right to stay in that Member State, and to third-country nationals who are subject to return as a criminal law sanction or as a consequence of a criminal law sanction, according to national law, or who are the subject of extradition procedures. In certain circumstances, where the risk of the return decision not being complied with is low, namely during any period of detention or when the return decision is issued at the external border and is executed immediately, and in order to reduce the administrative burden, Member States may refrain from entering alerts on third-country nationals, subject to a return decision.

(8) This Regulation should set out common rules for entering alerts related to return in SIS as soon as the underlying return decisions are issued. The alert should indicate whether a period for voluntary departure has been granted to the third-country national concerned, including whether such period has been extended and whether the decision has been suspended or the removal has been postponed.

(9) It is necessary to specify the categories of data that can be entered in SIS in respect of third-country nationals who are the subject of a return decision. Alerts on return should contain only those data that are required in order to identify the data subjects, to allow the competent authorities to take informed decisions without losing time and to ensure, where necessary, their protection in relation to persons who are armed, violent, have escaped or are involved in an activity as referred to in Articles 3 to 14 of Directive (EU) 2017/541 on combating terrorism[3]. Furthermore, in order to facilitate identification and detect multiple identities, the alert should include also a reference to the personal identification document and a copy of such document, if available**.**

Given the reliability of identifying third-country nationals with fingerprints and photographs or facial images these should always be entered in the alerts on return. As these may not be available, for example, when a return decision is taken in absentia, it should be possible in these cases to exceptionally derogate from this requirement.

(10) The exchange of supplementary information, provided by the competent national authorities, should always be carried out through the SIRENE channel using the SIRENE Bureau as point of contact.

The SIRENE Bureau should ensure the exchange of all supplementary information on third-country nationals subject to alerts on return in accordance with Articles 7 and 8 of Regulation (EU) 2018/xxx [Border checks].

(11) Procedures should be established to enable Member States to verify that the obligation to return has been complied with and to confirm the departure of the third-country national concerned to the Member State that issued the alert on return. This information should contribute to a more comprehensive follow-up of the compliance with return decisions.

---

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

(12) Alerts on return should be deleted as soon as the Member State or competent authority that issued the return decision is informed that the return has taken place or if the competent authority has sufficient and convincing information that the third-country national has left the territory of the Member States. Where a return decision is accompanied by an entry ban, the latter should be entered in SIS in accordance with Article 24(1)(b) of Regulation (EU) 2018/xxx [border checks]. In such cases Member States should take all necessary measures to ensure that no time-gap exist between the moment in which the third-country national leaves the Schengen area and the activation of the alert on the entry ban in SIS. If the data of SIS shows that the return decision is accompanied by an entry ban, the enforceability of that entry ban should be ensured.

(13) SIS should contain a mechanism for notifying the Member States about the non-compliance of third-country nationals with an obligation to return within a given period of voluntary departure. The mechanism should support the Member States in fulfilling their obligations in accordance with Article 8(1) and their obligation to issue an entry ban in accordance with Article 11 of Directive 2008/115/EC with regard to third-country nationals who have not complied with an obligation to return.

(14) This Regulation should establish mandatory rules for the consultation between national authorities to solve possible conflicting instructions. Consultations should be carried out where third-country nationals who hold, or are being granted, a valid residence permit or a long-stay visa by a Member State are subject to an alert on return issued by another Member State if the return decision is accompanied by a refusal of entry and stay, or cases where conflicting situations may arise at entry in the territories of the Member States.

(15) Alerts should be kept in SIS only for the time required to fulfil the purposes for which they were entered. Article 34 of Regulation (EU) 2018/xxx [border checks] on review periods should apply.

Alerts on return should be automatically deleted as soon as the alert expires, in accordance with the review procedure.

(16) Personal data obtained by a Member State pursuant to this Regulation should not be transferred or made available to any third country. As a derogation to that rule, it should be possible to transfer such personal data to a third country where such a transfer is subject to strict conditions and is necessary in individual cases in order to assist with the identification of a third-country national in relation to his or her return. The transfer of any personal data to third countries should be carried out in accordance with the provisions of Regulation (EU) 2016/679 and be conducted with the agreement of the Member State that issued the alert. The third countries of return are often not subject to adequacy decisions adopted by the Commission under Article 45 of Regulation (EU) 2016/679. Furthermore, the extensive efforts of the Union in cooperating with the main countries of origin of illegally staying third-country nationals subject to an obligation to return has not been able to ensure the systematic fulfilment by such third countries of the obligation established by international law to readmit their own nationals. Readmission agreements, concluded or being negotiated by the Union or the Member States and providing for appropriate safeguards for the transfer of data to third countries pursuant to Article 46 of Regulation (EU) 2016/679 cover a limited number of such third countries and conclusion of any new agreement remains uncertain. In such situations, and as an exception to the requirement of an adequacy decision or appropriate safeguards, transfer of personal data to third-country authorities pursuant to this Regulation should be allowed for the purposes of implementing the return policy of the Union, the derogation provided for in Article 49 of Regulation (EU) 2016/679 may be used, provided that the conditions laid down in that Article are met. According to its Article 57, implementation of Regulation (EU) 2016/679, including with regard to transfers of personal data to third countries pursuant to this Regulation, should be subject to monitoring by the national independent supervisory authority.

(17) National authorities responsible for return may differ significantly among Member States, and such authorities may also vary within a Member State depending on the reasons for illegal stay. Judicial authorities may also issue return decisions, for instance as result of appeals against a refusal of granting an authorisation or right to stay, or as a criminal sanction. All national authorities in charge of issuing and enforcing return decisions in accordance with Directive 2008/115/EC should be entitled to access SIS in order to enter, update, delete and search alerts on return.

(18) Access to alerts on return should be granted to national authorities referred to in Article 29(1), (1a) and in Article 29(2) of Regulation (EU) 2018/xxx [border checks] for the purpose of identification and return of third-country nationals.

(19) Regulation (EU) 2016/794 on the European Union Agency for Law Enforcement cooperation (Europol Regulation) provides that Europol supports and strengthens actions carried out by the competent authorities of Member States and their cooperation in combating terrorism and serious crime and provides analysis and threat assessments. In order to facilitate Europol in carrying out its tasks, in particular within the European Migrant Smuggling Centre, it is appropriate to allow Europol access to the alert category defined in this Regulation.

(20) Regulation (EU) 2016/1624 provides that the host Member State shall authorise the members of the teams as defined in Article 2(8) of Regulation (EU) 2016/1624, 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. The objective of the deployment of the teams as defined in Article 2(8) and (9) of Regulation (EU) 2016/1624 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 teams as defined in Article 2(8) and (9) of Regulation (EU) 2016/1624 necessitates access to alerts on return SIS via a technical interface of European Border and Coast Gard Agency connecting to Central SIS.

(21) The provisions on responsibilities of the Member States and the European Agency on the operational management of large-scale IT systems in the area of freedom, security and justice, the entry and processing of alerts, the conditions to access and retention of alerts, data processing, data protection, liability and monitoring and statistics as included in Regulation (EU) 2018/xxx [Border checks] should also apply to data entered and processed in SIS in accordance with this Regulation.

(21a) This Regulation respects fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the European Union.

(21b) The application of this Regulation is without prejudice to the obligations deriving from the Geneva Convention relating to the Status of Refugees of 28 July 1951, as supplemented by the New York Protocol of 31 January 1967.

(21c) Member States should implement this Regulation in full respect of fundamental rights, including the respect of the principle of *non-refoulement*, and should always take into consideration the best interests of the child, family life, and the state of health or condition of vulnerability of the individuals concerned.

(22) 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 Treaty on 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.

(23) This Regulation constitutes a development of provisions of the Schengen *acquis* in which the United Kingdom does not take part, in accordance with Council Decision 2000/365/EC[4]; the United Kingdom is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(24) This Regulation constitutes a development of the provisions of the Schengen *acquis* in which Ireland does not take part, in accordance with Council Decision 2002/192/EC[6]; Ireland is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

---

4 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).

(25) As regards Iceland and Norway, this Regulation constitutes a development of the 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 latters' association with the implementation, application and development of the Schengen *acquis*[5], which fall within the area referred to in Article 1, point C of Council Decision 1999/437/EC[6].

(26) As regards Switzerland, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning 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*[7], which fall within the area referred to in Article 1, point C of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/146/EC[8].

---

5 OJ L 176, 10.7.1999, p. 36.

6 Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application 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 (OJ L 176, 10.7.1999, p. 31).

7 OJ L 53, 27.2.2008, p. 52.

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

(27) As regards Liechtenstein, this Regulation 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*[9], which fall within the area referred to in Article 1, point C of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU[10].

(27a) As regards Bulgaria, Romania and Croatia, this Regulation constitutes an act building upon, or otherwise relating to, the Schengen *acquis* within, respectively the meaning of 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[11] 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[12].

(27b) Concerning Cyprus this Regulation constitutes an act building upon, or otherwise relating to, the Schengen *acquis* within the meaning of Article 3(2) of the 2003 Act of Accession.

(28) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 3 May 2017,

---

9 OJ L 160, 18.6.2011, p. 21.

10 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).

11 OJ L 166, 1.7.2010, p. 17. To be updated in case decision on BG RO in SIS is adopted before the SIS.

12 OJ L 108, 26.4.2017, p. 31

HAVE ADOPTED THIS REGULATION:

Article 1

Subject matter and scope

This Regulation lays down the conditions and procedures for the entry and processing in the Schengen Information System (SIS), as established by Regulation (EU) 2018/xxx [border checks], of alerts in respect of third-country nationals subject to return decisions issued by the Member States, as well as for exchanging supplementary information on such alerts.

Article 2

Definitions

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

(a) 'return' means return as defined in Article 3(3) of Directive 2008/115/EC;

(b) 'third-country national' means third-country nationals as defined in Article 3(1) of Directive 2008/115/EC;

(c) (deleted)

(d) 'return decision' means an administrative or judicial decision or act, stating or declaring the stay of a third-country national to be illegal and imposing or stating an obligation to return that respects Directive 2008/115/EC;

(da) 'alert' means alert as defined in point (a) of Article 3(1) of Regulation (EU) No …/… [Border Checks]

(db) 'supplementary information' means supplementary information as defined in point (b) of Article 3(1) of Regulation (EU) No …/… [Border Checks];

(dc) 'removal' means removal as defined in Article 3(5) of Directive 2008/115/EC;

(e) 'voluntary departure' means voluntary departure as defined in Article 3(8) of Directive 2008/115/EC;

(ea) 'issuing Member State' means the Member State as defined in point (i) of Article 3(1) of Regulation (EU) No …/… [Border Checks];

(eb) 'granting Member State' means the Member State as defined in point (ia) of Article 3(1) of Regulation (EU) No …/… [Border Checks]

(ec) 'personal data' means data as defined in point (e) of Article 3(1) of Regulation (EU) No …/… [Border Checks];

(ed) "executing Member State" means the Member State as defined in point (j) of Article 3(1) of Regulation (EU) No …/… [Border Checks];

(f) 'CS-SIS' means the technical support function of the Central SIS as referred to in Article 4(1)(a) of Regulation (EU) 2018/xxx [border checks];

(g) 'residence permit' means residence permit as defined in Article 2(16) of Regulation (EU) 2016/399);

(h) 'long-stay visa' means long-stay visa as defined in Article 1(1) of the Regulation (EU) No 265/2010[13].

(i) a 'match' means match as defined in point (h) of Article 3(1) of Regulation (EU) No …/… [Border Checks]

(ia) a 'hit' means hit as defined in point (ha) of Article 3(1) of Regulation (EU) No …/… [Border Checks]

(j) 'end-users' mean end users as defined in point (k) of Article 3(1) of Regulation (EU) No …/… [Border Checks];

(k) 'threat to public health' means to threat to public health as defined in Article 2(21) of Regulation (EU) 2016/399;

(l) 'external borders' means external borders as defined in Article 2(2) of Regulation (EU) 2016/399.

---

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

Article 3

Entry of data in SIS

1. Data on third-country nationals subject to a return decision shall be entered in SIS for the purpose of verifying that the obligation to return has been complied with and for supporting the enforcement of the decision. An alert shall be entered in SIS without delay when the return decision is issued.

1a. Member States may refrain from entering data in SIS on third-country nationals subject to a return decision when that decision concerns third-country nationals who are detained pending removal. When the third-country nationals concerned are released from detention without being removed, data on the third-country nationals subject to a return decision shall be entered in SIS without delay.

1b. Member States may also refrain from entering data on third-country nationals subject to a return decision in SIS when the decision is issued at the external border of a Member State and is executed immediately.

2. The period for voluntary departure granted in accordance with Article 7 of Directive 2008/115/EC shall be recorded in the alert immediately. Any prolongation of such a period shall be recorded in the alert without delay.

3. The suspension and the postponement of the enforcement of the return decision including as a result of the lodging of an appeal, shall be immediately recorded in the alert.

Article 4

Categories of data

Data entered in SIS in accordance with Article 3 of this Regulation shall contain only the following:

(a) surnames;

(b) forenames;

(c) names at birth;

(d) previously used names and aliases;

(e) (deleted)

(f) place of birth;

(g) date of birth;

(h) 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 threat to public health; or

vi. is involved in an activity as referred to in Articles 3 to 14 of Directive (EU) 2017/541;

(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) links to other alerts issued in SIS;

(oa) whether the return decision is issued in relation to a third-country national who poses a threat to public policy, public security or national security;

(ob) type of offence;

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

(q) the country of issue of the person's identification document(s);

(r) the number(s) of the person's identification document(s);

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

(t) photographs and facial images;

(u) dactyloscopic data;

(v) a copy of the identification document(s), whenever possible in colour;

(w) last date of the period for voluntary departure, if granted;

(x) whether the return decision has been suspended or the enforcement of the decision has been postponed, including as a result of the lodging of an appeal.

(y) whether the return decision is accompanied by an entry ban constituting the basis for an alert for refusal of entry and stay pursuant to Article 24(1)(b) of Regulation xxx [Border Checks].

The minimum set of data necessary in order to enter an alert in SIS shall be the data as referred to in points (a), (g), (k), (m), (n), (w) and (y) of the first paragraph. The other data listed in that paragraph shall also be entered in SIS, if available.

Dactyloscopic data referred to in point (u) of the first paragraph may consist of one to ten flat fingerprints and one to ten rolled fingerprints of the third country national concerned; it may consist of up to two palm prints in respect of third-country nationals for whom the collection of fingerprints is impossible; it may include up to two palm prints in respect of third-country nationals who are subject to return as a criminal law penalty or who have committed a criminal offence on the territory of the Member State issuing the return decision.

Article 5

Authority responsible for the exchange of supplementary information

The SIRENE Bureau shall ensure the exchange of all supplementary information on third-country nationals subject to return in accordance with Articles 7 and 8 of Regulation (EU) 2018/xxx [Border checks].

Article 6

Hits at the external borders at exit - Confirmation of return

1. In the event of a hit on an alert on return concerning a third country national who is exiting the territory of the Member States through the external borders of a Member State, the executing Member State shall communicate the following information to the issuing Member State through the exchange of supplementary information:

   (a) the fact that the third-country national has been identified;

   (b) the location and time of the check;

   (c) the fact that the third-country national has left the territory of the Member States;

   (d) the fact that the third-country national was subject to removal.

   (e) (deleted)

   Where a third-country national, who is the subject of an alert on return, exits the territory of the Member States through the external border of the issuing Member State, the confirmation of return shall be sent to the competent authority of that Member State in accordance with national procedures.

2. The issuing Member State shall delete the alert without delay following the receipt of the confirmation of return. Where applicable, an alert for refusal of entry or stay shall be issued without delay pursuant to Article 24(1)(b) of Regulation (EU) 2018/xxx [border checks].

3. The Member States shall provide on a quarterly basis statistics to 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 of the European Parliament and of the Council ('the Agency') on the number of confirmed returns and on the number of those confirmed returns where the third-country national was subject to removal. The Agency shall compile the quarterly statistics into the annual report referred to in Article 11. Those statistics shall not contain personal data.

Article 7

Non-compliance with return decisions

1. CS-SIS shall automatically notify the issuing Member States about their alerts on return for which the period for voluntary departure including any possible extensions has expired.

2. Without prejudice to the procedure referred to in Article 6(1), 8A and 8E, in the event of a hit on an alert on return the executing Member State shall contact immediately the issuing Member State through the exchange of supplementary information in order to determine the measures to be taken.

Article 8

(deleted)

Article 8A

Hits at the external borders at entry

In the event of a hit on an alert on return concerning a third-country national who is entering the territory of the Member States through the external borders the following procedure shall apply:

(a) Where the return decision is accompanied by an entry ban, the executing Member State shall immediately inform the issuing Member State, through the exchange of supplementary information. The issuing Member State shall immediately delete the alert on return and issue a refusal of entry and stay alert pursuant to Article 24(1)(b) of Regulation xxx [Border Checks];

(b) Where the return decision is not accompanied by an entry ban, the executing Member State shall immediately inform the issuing Member State, through the exchange of supplementary information, in order to delete without delay the alert on return.

The decision on the entry of the third-country national shall be taken by the executing Member State in accordance with the Schengen Borders Code.

Article 8B

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

1. Where a Member State considers granting or extending a residence permit or long-stay visa to a third-country national who is the subject of an alert on return, accompanied by an entry ban, entered by another Member State, the Member States involved shall consult each other, through the exchange of supplementary information, according to the following rules:

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

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

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

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

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

   (f) where the granting Member State notifies the issuing Member State that it intends to grant or extend the residence permit or long-stay visa or that it decided to do so, the issuing Member State shall delete the alert on return.

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

2. Where a Member State considers granting or extending a residence permit or long-stay visa to a third-country national who is the subject of an alert on return, which is not accompanied by an entry ban, entered by another Member State, the granting Member State shall inform without delay the issuing Member State that it intends to grant or has granted a residence permit or a long-stay visa. The issuing Member State shall without delay delete the alert on return.

Article 8C

Prior consultation before entering an alert on return concerning a third country national holding a valid residence permit or long-stay visa

Where a Member State has issued a return decision in accordance with Article 6(2) of Directive 2008/115/EC and it considers entering an alert for return concerning a third-country national who is the holder of a valid residence permit or a long-stay visa granted by another Member State, the involved Member States shall exchange supplementary information according to the following rules:

(a) the Member State that has taken the return decision shall inform the granting Member State about the decision;

(b) the exchange of information referred to in point a) shall contain sufficient information about the reasons for the return decision;

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

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

(e) within fourteen calendar days after the receipt of the information request the granting Member State shall notify the Member State that has taken the return decision about its decision or where it was impossible to take a decision within that period shall make a reasoned request to prolong the time period for the response. The period may exceptionally be extended for a maximum of further twelve calendar days.

(f) where the granting Member State notifies the Member State that has taken the return decision that it maintains the residence permit or long-stay visa the Member State that has taken the return decision shall not enter the alert on return.

Article 8D

A posteriori consultation procedure after entering an alert on return

Where it emerges that an alert on return has been issued for a third-country national who holds a valid residence permit or long-stay visa granted by another Member State, the issuing Member State may decide to withdraw the return decision. In the case of such withdrawal it shall immediately delete the alert on return. However, where the issuing Member State decides to maintain the return decision issued in accordance with Article 6(2) of Directive 2008/115/EC, the involved Member States shall exchange supplementary information according to the following rules:

(a) the issuing Member State shall inform the granting Member State about the return decision;

(b) the exchange of information referred to in point (a) shall contain sufficient information about the reasons for the alert on return;

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

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

(e) within fourteen calendar days after the receipt of the information request the granting Member State shall notify the issuing Member State about its decision or where it was impossible to take a decision within that period shall make a reasoned request to prolong the time period for the response. The period may exceptionally be extended for a maximum of further twelve calendar days.

(f) where the granting Member State notifies the issuing Member State that it maintains the residence permit or long-stay visa the issuing Member State shall immediately delete the alert on return.

Article 8E

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

Where a Member State encounters a hit on an alert on return entered by a Member State in respect of a third-country national who is the holder of a valid residence permit or long-stay visa granted by another Member State, the involved Member States shall exchange supplementary information, according to the following rules:

(a) the executing Member State shall inform the issuing Member State about the situation and the issuing Member State shall initiate the procedure laid down in Article 8D;

(b) the issuing Member State shall notify the executing Member State about the final outcome of the exchange of information.

Article 8F

Statistics of exchange of information

Member States shall provide on an annual basis statistics to the Agency about the exchanges of information carried out in accordance with Articles 8 A to 8E and the instances in which the deadlines were not met.

Article 9

Deletion of alerts

1. In addition to Articles 6 and 8 A-E, alerts on return shall be deleted when the decision upon which the alert was based has been withdrawn or annulled by the competent authority. Alerts on return shall also be deleted when the third-country national concerned can demonstrate that they have left the territory of the Member States in compliance with the respective return decision.

2. Alerts on return entered in respect of a person who has acquired citizenship of a Member State or of any State whose nationals are beneficiaries of the right of free movement under Union law shall be deleted as soon as the issuing Member State becomes aware, or is informed pursuant to Article 39 of Regulation (EU) 2018/xxx [border checks], that the person in question has acquired such citizenship.

Article 10

Transfer of personal data to third countries for the purpose of return

1. By way of derogation from Article 45 of Regulation (EU) 2018/ xxx [border checks], the data referred to in Article 4 (a), (b), (c), (d), (f), (g), (h), (i), (p), (q), (r), (s), (t), (u) and (v) and the related supplementary information may be transferred or made available to a third country with the agreement of the issuing Member State.

2. The transfer of the data to a third country shall be carried out in accordance with the relevant provisions of Union law, in particular provisions on data protection, including Chapter V of Regulation (EU) 2016/679, and, where applicable, readmission agreements, and the national law of the Member State transferring the data.

3. The transfers of data to a third country shall take place only when the following conditions are met:

   (a) the data is transferred or made available solely for the purpose of identification of, and issuance of an identification or travel document to, an illegally staying third-country national in view of return;

   (b) the third-country national concerned has been informed that his or her personal data and supplementary information may be shared with the authorities of a third country.

4. Transfers of personal data to third countries pursuant to this Article shall not prejudice the rights of applicants for and beneficiaries of international protection, in particular as regards *non-refoulement*, and the prohibition to disclose or obtain information in accordance with Article 30 of Directive 2013/32/EU.

5. Data processed in SIS and the related supplementary information exchanged pursuant to this Regulation shall not be made available to a third country where the enforcement of the return decision was suspended or postponed including as a result of the lodging of an appeal because such return would have violated the principle of *non-refoulement*.

6. Implementation of Regulation (EU) 2016/679, including with regard to the transfer of personal data to third countries pursuant to this Article, and in particular the use, proportionality and necessity of transfers based on Article 49(1)(d) of that Regulation, shall be subject to monitoring by the national independent supervisory authority set up pursuant to Chapter VI of Regulation (EU) 2016/679.

Article 11

Statistics

The Agency shall produce daily, monthly and annual statistics, both in total number and per each Member State on the number of alerts on return entered in SIS , including on the data referred to in Article 4(x) of this Regulation, on the notifications referred to in Article 7(1) of this Regulation and the number of alerts on return deleted. The Agency shall produce statistics about the data provided by the Member States in accordance with Article 6(3) and Article 8F of this Regulation. Those statistics shall not contain personal data.

Those statistics shall be included in the annual report provided for in Article 54 of Regulation (EU) 2018/ xxx [border checks].

Article 12

Right to access data in SIS

1. Access to data entered in SIS and the right to search such data shall be reserved to the national authorities referred to in Article 29(1), (1a) and (2) of Regulation (EU) 2018/ xxx [Border checks].

2. Europol shall have within their mandate the right to access and search data entered in SIS for the purpose of supporting and strengthening action by the competent authorities of the Member States and their mutual cooperation in preventing and combating migrant smuggling and facilitation of irregular migration in accordance with the conditions laid down in Article 30 of Regulation (EU) 2018/ xxx [Border checks].

3. Members of the teams as defined in Article 2(8) and (9) of Regulation (EU) 2016/1624 shall have within their mandate the right to access and search data entered in SIS for the purpose of carrying out border checks, border surveillance and return operations via the technical interface set up and maintained by the European Border and Coast Guard Agency as referred to and in accordance with the conditions laid down in Articles 31 of Regulation (EU) 2018/ xxx [Border checks].

Article 12 A

Evaluation

The Commission shall evaluate the application of this Regulation within two years from the date of the start of its application. This evaluation shall include an assessment of the possible synergies between this Regulation and the Regulation (EU) 2017/2226 establishing an Entry-Exit System.

Article 13

Applicability of the provisions of Regulation (EU) 2018/xxx [Border checks]

As far as not established in this Regulation, the entry, processing and updating of alerts, the provisions on responsibilities of the Member States and the Agency, the conditions to access and retention of alerts, data processing, data protection, liability and monitoring and statistics laid down in Articles 6 to 19, Article 20(3) and (4) as well as in Articles 21, 22, 23a, 28, 29(4) and 33 to 54 of Regulation (EU) 2018/ xxx [Border checks] shall apply to data entered and processed in SIS in accordance with this Regulation.

Article 14

Entry into force

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

It shall apply from the date fixed by the Commission in accordance with Article 58(2) of Regulation (EU) 2018/xxx [border checks].

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

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

ANNEX II

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) 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 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 competent national authorities, in particular border guards, police, customs, authorities responsible for prevention, detection, investigation or prosecution of criminal offences or execution of criminal penalties and immigration authorities.

(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[1] (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[2] and Council Decision 2001/886/JHA (SIS)[3] and it was established by Regulation (EC) No 1987/2006[4] as well as by Council Decision 2007/533/JHA[5]. 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[6]. The recommendations set out in those documents should be reflected, as appropriate, in this Regulation.

---

1 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).

2 OJ L 328, 13.12.2001, p. 4.

3 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).

4 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).

5 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).

6 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.

(4) This Regulation constitutes the necessary legislative basis for governing SIS in respect of matters falling within the scope of Chapter 2 of Title V of the Treaty on Functioning of the European Union. Regulation (EU) 2018/… of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters[7] constitutes the necessary legislative basis for governing SIS in respect of matters falling within the scope of Chapters 4 and 5 of Title V of the Treaty on Functioning of the European Union.

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

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

(6a) SIS alerts contain only the information necessary for the identification of a person and the action to be taken. Therefore, Member States should exchange supplementary information related to alerts where required.

[7] Regulation (EU) 2018/…

(7) SIS includes a central system (Central SIS) and national systems that may contain 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 border 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. Each Member State should set up a 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 and the Communication Infrastructure should be operated to ensure its functioning 24 hours a day, 7 days a week. For this reason the Agency should implement technical solutions to reinforce the uninterrupted availability of SIS, subject to an independent impact assessment and cost-benefit analysis.

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

(9) In order to ensure the efficient exchange of supplementary information, including on 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.

(9a) Member States should ensure that the staff of the SIRENE Bureau have the necessary linguistic skills and knowledge in relevant legislation and rules of procedure to perform their tasks.

(9b) In order to be able to fully exploit the functionalities of SIS, Member States should ensure that end-users and the staff of the SIRENE Bureaux regularly receive training, including on data security and protection, as well as on data quality. SIRENE Bureaux should be involved in the development of training programs. To the extent possible, SIRENE Bureaux should also provide for staff exchanges with other SIRENE Bureaux at least once a year. Member States are encouraged to take appropriate measures to avoid the loss of skills and experience through staff turnover.

(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[8] (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 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. The Commission should report to the European Parliament and the Council on data quality issues encountered. To further increase the quality of data in SIS, the Agency should also offer training on the use of SIS to national training bodies and, insofar as possible, to SIRENE Bureaux and to end-users.

[8] Established by [Regulation (EU) No …./2018 new eu-LISA]

(12) In order to allow better monitoring of the use of SIS to analyse trends concerning migratory pressure and border management, the Agency should be able to develop a state-of-the-art capability for statistical reporting to the Member States, the European Parliament, the Council, the Commission, Europol and the European Border and Cost Guard Agency without jeopardising data integrity. Therefore, a central statistical repository should be established. Any statistics retained in the repository or produced by the repository should not contain personal data as defined in [new Regulation (EC) No 45/2001[9]] of the European Parliament and of the Council. Member States should communicate statistics concerning the right of access, rectification of inaccurate data and erasure of unlawfully stored data to the cooperation mechanism.

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

(13a) Competent authorities should be able, where strictly necessary, to enter into SIS specific information relating to any specific, objective, physical characteristics of a person not subject to change, such as tattoos, marks or scars.

(13b) 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.

[9] Regulation (EC)… (OJ…)

(15) SIS should permit the processing of biometric data in order to assist in the reliable identification of the individuals concerned. Any entry and use of photographs, facial images or dactyloscopic data should not exceed what is necessary for the objectives pursued, should be authorised by Union law, respect fundamental rights, including the best interests of the child, and be in accordance with relevant provisions on data protection laid down in this Regulation and Union data protection legislation. 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, with the consent for each data category, and in particular palm prints, of the individual concerned and a strict limitation of the purposes for which such personal 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 subject to the principles set out in Article 4 of Directive (EU) 2016/680 of the European Parliament and of the Council[10] and Article 5 of Regulation (EU) 2016/679. 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 dactyloscopic data, photographs and facial images for identification and verification purposes. Facial images and photographs for identification purposes should initially only be used in the context of regular border crossing points, subject to a report by the Commission confirming the availability, reliability and readiness of the technology.

---

[10] 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) Complete or incomplete sets of fingerprints or palm prints found at a crime scene should be allowed to be checked against the dactyloscopic data stored in SIS if it can be established to a high degree of probability that they belong to the perpetrator of the serious crime or terrorist offence provided that the search is carried out simultaneously in the relevant national fingerprint databases. Particular attention should be given to the establishement of quality standards applicable to the storage of biometric data.

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

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

(20) A greater level of effectiveness, harmonisation and consistency can be achieved by making it mandatory to enter in SIS all entry bans issued by the competent authorities of the Member States in accordance with procedures respecting Directive 2008/115/EC[11], and by setting common rules for entering such alerts following the return of the illegally staying third country national. Member States should take all necessary measures to ensure that no time-gap exist between the moment in which the third-country national leaves the Schengen area and the activation of the alert in SIS. This should ensure the enforcement of entry bans at external border crossing points, effectively preventing re-entry into the Schengen area.

(20a) Persons in respect of whom a decision for refusal of entry and stay is taken should have the right to appeal against those decisions. The right of appeal should comply with Directive 2008/115/EC where decisions are related to return.

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

(21) This Regulation should set mandatory rules for the consultation and notification of national authorities in case a third country national holds or may obtain a valid residence permit or long-stay visa granted in one Member State, and another Member State intends to issue or already entered an alert for refusal of entry and stay to the third country national concerned. Such situations create serious uncertainties for border guards, police and immigration authorities. Therefore, it is appropriate to provide for a mandatory timeframe for rapid consultation with a definite result in order to ensure that those third country nationals entitled to reside lawfully in the territory of the Member States are entitled to enter that territory without difficulty and that those who are not entitled to enter are prevented from doing so.

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

(22) This Regulation should be without prejudice to the application of Directive 2004/38[12].

(23) Alerts should not be kept in SIS longer than the time required to fulfil the specific purposes for which they were issued. An issuing Member State should within three years of entry of an alert into SIS, review the need to retain it. If the national decision on which the alert is based provides for a longer period of validity than three years, the alert should be reviewed within five years. Decisions to keep alerts on persons should be based on a comprehensive individual assessment. Member States should review alerts on persons within the defined period and keep statistics about the number of alerts on persons for which the retention period has been extended.

---

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

(24) Entering and extending the expiry date of a SIS alert should be subject to the necessary proportionality requirement, examining whether a concrete case is adequate, relevant and important enough to insert an alert in SIS. In cases of terrorist offences the case should be considered adequate, relevant and important enough to warrant the existence of an alert in SIS. For public or national security reasons Member States should be allowed exceptionally to refrain from creating an alert, when it is likely to obstruct official or legal inquiries, investigations or procedures.

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

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

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

(28) Without prejudice to more specific rules laid down in this Regulation for the processing of personal data, Regulation (EU) 2016/679 of the European Parliament and of the Council[13] should apply to the processing of personal data by the Member States in application of this Regulation unless such processing is carried out by the competent authorities of the Member States for the purposes of prevention, investigation, detection or prosecution of terrorist offences or of other serious criminal offences.

[13] Add OJ reference

(28a) Without prejudice to more specific rules laid down in this Regulation, the national laws, regulations and administrative provisions adopted pursuant to Directive (EU) 2016/680 should apply to the processing of personal data by the competent authorities of Member States for the purposes of prevention, detection, investigation or prosecution of terrorist offences or other serious criminal offences or the execution of criminal penalties pursuant to this Regulation. Access to data entered into SIS and the right to search such data by national competent authorities which are responsible for the prevention, detection, investigation or prosecution of terrorist offences or other serious criminal offences or the execution of criminal penalties are to be subject to all the relevant provisions of this Regulation and those of Directive (EU) 2016/680 as transposed into national law, in particular the monitoring by the supervisory authorities established in accordance with Article 41(1) of Directive (EU) 2016/680.

(28b) [new Regulation (EU) 45/2001] should apply to the processing of personal data by the Union institutions and bodies when carrying out their responsibilities under this Regulation.

(28c) Regulation (EU) 2016/794 of the European Parliament and of the Council[14] should apply to the processing of personal data by Europol under this Regulation.

(28d) When using the SIS, the competent authorities should ensure that the human dignity and integrity of the person whose data are processed are respected. Processing of personal data for the purposes of this Regulation is not to result in discrimination against persons on any grounds such as sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation.

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

---

[14] 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).

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

(31) The national independent supervisory authorities established in accordance with Regulation (EU) 2016/679 and Directive (EU) 2016/680 (supervisory authorities) should monitor the lawfulness of the processing of personal data by the Member States in relation to this Regulation including the exchange of supplementary information, and should be granted sufficient resources to carry out this task. The rights of data subjects for access, rectification and erasure of their personal data stored in SIS, and subsequent remedies before national courts as well as the mutual recognition of judgments should be set out. Therefore, it is appropriate to require annual statistics from Member States.

(32) The supervisory authorities should ensure that an audit of the data processing operations in their Member States' 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.

(32a) The European Data Protection Supervisor should monitor the activities of the Union institutions and bodies in relation to the processing of personal data under this Regulation. The European Data Protection Supervisor and the national supervisory authorities should cooperate with each other in the monitoring of SIS.

(32b) The European Data Protection Supervisor should be granted sufficient resources to fulfil the tasks entrusted to it under this Regulation, including assistance from persons with expertise on biometric data.

(33) Regulation (EU) 2016/794 (Europol Regulation) provides that Europol supports and strengthens actions carried out by the competent authorities of Member States and their cooperation in combating terrorism and serious crime and provides analysis and threat assessments. In order to facilitate Europol in carrying out its tasks, in particular within the European Migrant Smuggling Centre, it is appropriate to allow Europol access to the alert categories defined in this Regulation.

(34) In order to bridge the gap in information sharing on terrorism, in particular on foreign terrorist fighters – where monitoring of their movement is crucial – Member States are encouraged to share information on terrorism-related activity with Europol. 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.

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

(36) Regulation (EU) 2016/1624 of the European Parliament and of the Council[15] provides for the purpose of this Regulation, that the host Member State is to authorise the members of the teams as defined in Article 2(8) of Regulation (EU) 2016/1624, 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 teams as defined in Article 2(8) and (9) of Regulation (EU) 2016/1624 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 teams as defined in Article 2(8) and (9) of Regulation (EU) 2016/1624, 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 State 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.

(37) (deleted)

[15] 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).

(38) Owing to their technical nature, level of detail and need for regular updating, certain aspects of SIS cannot be covered exhaustively by the provisions of this Regulation. These include, for example, technical rules on entering data, updating, deleting and searching data, data quality and rules related to biometric data, rules on compatibility and priority of alerts, links between alerts, 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.

(39) In order to ensure uniform conditions for the implementation of this Regulation implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011[16]. The procedure for adopting implementing measures under this Regulation and Regulation (EU) 2018/xxx (police and judicial cooperation) should be the same.

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

[16] 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).

(40a) In order to ensure the smooth functioning of SIS, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission in respect of the determination of the circumstances in which photographs and facial images may be used for the identification of third-country nationals other than in the context of regular border crossing points. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[17]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council should receive all documents at the same time as Member States' experts, and their experts should systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

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

(42) This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. In particular, this Regulation should fully respect the protection of personal data in accordance with Article 8 of the Charter of Fundamental Rights of the European Union while seeking to ensure a safe environment for all persons residing on the territory of the European Union and protection of irregular migrants from exploitation and trafficking. In cases concerning children, the best interests of the child should be a primary consideration.

---

17 OJ L 123, 12.5.2016, p. 1.

(42a) 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[38]. Therefore, funding 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 should be allocated to the Member States and the Agency. The financial costs of upgrading the SIS as well as the implementation of the Regulation should be monitored. In case of higher estimated costs EU funding should be made available to support Member States in conformity with the Multiannual Financial Framework.

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

(44) This Regulation constitutes a development of provisions of the Schengen *acquis* in which the United Kingdom does not take part, in accordance with Council Decision 2000/365/EC[18]; the United Kingdom is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(45) This Regulation constitutes a development of the provisions of the Schengen *acquis* in which Ireland does not take part, in accordance with Council Decision 2002/192/EC[19]; Ireland is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

---

18 OJ L 131, 1.6.2000, p. 43.
19 OJ L 64, 7.3.2002, p.20.

(46) As regards Iceland and Norway, this Regulation constitutes a development of provisions of the Schengen acquis within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis[20], which fall within the area referred to in Article 1, point G of Council Decision 1999/437/EC[21] on certain arrangements for the application of that Agreement.

(47) As regards Switzerland, this Regulation constitutes a development of provisions of the Schengen acquis within the meaning of the Agreement signed between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis, which fall within the area referred to in Article 1, point G, of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/146/EC[22].

(48) As regards Liechtenstein, this Decision constitutes a development of the provisions of the Schengen acquis within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis[23], 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 2011/350/EU[24].

---

20 OJ L 176, 10.7.1999, p.36.

21 OJ L 176, 10.7.1999, p.31.

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

23 OJ L 160, 18.6.2011, p. 21.

24 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).

(49) As regards Bulgaria, Romania and Croatia, this Regulation constitutes an act building upon, or otherwise relating to, the Schengen acquis within, respectively, the meaning of 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[37] 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.[25]

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

(51) (deleted)

(52) This Regulations introduces a series of improvements to SIS which will increase its effectiveness, strengthen data protection and extend access rights. Certain of these improvements do not require complex technical developments, while others do require technical changes of varying magnitude. In order to enable improvements to the system to become available to end-users as fast as possible, this Regulation introduces amendments to Regulation (EC) No 1987/2006 in several phases. A number of improvements to the system should apply immediately upon entry into force of this Regulation, whereas others should apply either one or two years after its entry into force. This Regulation should apply in its entirety within three years after its entry into force. In order to avoid delays in its application the phased implementation of this Regulation should be closely monitored. Regulation (EC) No 1987/2006 should be repealed upon the date of application of this Regulation.

(53) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 3 May 2017,

HAVE ADOPTED THIS REGULATION:

[25] OJ L 108, 26.4.20017, 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 ensure the application of the provisions of Chapter 2 of Title V of Part Three of the Treaty on the Functioning of the European Union relating to the movement of persons on their territories, using information communicated via this system.

Article 2

Subject matter

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

2. This Regulation also lays down provisions on the technical architecture of SIS, the responsibilities of the Member States and of the European Agency 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 entered in SIS allowing the competent authorities to identify a person with a view to taking specific action;

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

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

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

(3) when the required action cannot be taken;

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

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

(6) when dealing with rights of access;

(c) 'additional data' means the data stored in SIS and connected with SIS alerts which are to be immediately available to the competent authorities where a person in respect of whom data has been entered in SIS is located as a result of searches made therein;

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

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

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

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

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

(1) a search is conducted by an 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.

(4) (deleted)

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

(a) it has been confirmed:

(i) by the end-user; or

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

and

(b) further actions are requested.

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

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

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

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

(ka) 'biometric data' means personal data resulting from specific technical processing relating to the physical or physiological characteristics of a natural person, which allow or confirm the unique identification of that natural person, i.e. photographs, facial images, dactyloscopic data;

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

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

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

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

(o) (deleted)

(p) ‘terrorist offences’ means offences under national law referred to in Articles 3 to 14 of Directive (EU) 2017/541[26], or equivalent to one of those offences for the Member States which are not bound by that Directive;

(q) ‘residence permit’ means residence permit as defined in Article 2(16) of Regulation (EU) 2016/399[27];

(r) 'long-stay visa' means long-stays visa as defined in Article 1(1) of Regulation (EU) No 265/2010[28];

(s) 'threat to public health' means threat to public health as defined by Regulation (EU) 2016/399[29].

---

26 Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ L 88, 31/03/2017, p. 6.

27 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);

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

29 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);

Article 4

Technical architecture and ways of operating SIS

1. SIS shall be composed of:

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

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

   – a uniform national interface (NI-SIS);

   (b) a national system (N.SIS) in each of the Member States, consisting of the national data systems which communicate with Central SIS. An N.SIS may contain a data file (a 'national copy'), containing a complete or partial copy of the SIS database. Two or more Member States may establish in one of their N.SIS a shared copy which may be used jointly by 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 for each N.SIS. A shared backup N.SIS may be used jointly by two or more Member States and shall be considered as the back-up N.SIS of each of the participating Member States. The N.SIS and its backup may be used simultaneously to ensure uninterrupted availability to end-users; and

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

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

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

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

3. CS-SIS shall perform technical supervision and administration functions and have a backup CS-SIS, capable of ensuring all functionalities of the principal CS-SIS in the event of failure of 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 …/2018 new eu-LISA Regulation][30] ('the Agency').

3a. The Agency shall implement technical solutions to reinforce the uninterrupted availability of SIS either through the simultaneous operation of CS-SIS and the back-up CS-SIS, provided that the backup CS-SIS remains capable of ensuring the operation of SIS in the event of failure of CS-SIS, or through duplication of the system or its components. Notwithstanding the procedural requirements laid down in Article 6a of Regulation ... [new eu-LISA Regulation] the Agency shall, no later than ... [one year after the entry into force of this Regulation, *OPOCE please insert date*], prepare a study on the options for technical solutions, containing an independent impact assessment and cost-benefit analysis.

3b. Where necessary in exceptional circumstances, the Agency may temporarily develop an additional copy of the CS-SIS database.

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

(a) provide online update of the national copies;

[30] OJ L 286, 1.11.2011, p.1.

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

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

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

2. Funding is allocated from the envelope of EUR 791 million foreseen under Article 5(5), point (b) of the ISF Borders and Visa Regulation[31] to cover the costs of implementation of this Regulation.

3. From the envelope referred to in paragraph 2, and without prejudice to further funding for this purpose from other sources of the general budget of the European Union, an amount of EUR 31.098.000 is allocated to the Agency. Such funding shall be implemented under indirect management and shall contribute to carrying out the technical developments required under this Regulation concerning Central SIS and the Communication Infrastructure, as well as the related training activities.

4. From the envelope referred to in paragraph 2, the Member States participating in the ISF Borders and Visa Fund Regulation shall receive an additional global allocation of EUR 36.810.000 to be distributed in equal shares via a lump sum to their basic allocation. Such funding shall be implemented under shared management and shall be entirely devoted to SIS national systems to ensure their quick and effective upgrading, in line with the requirements of this Regulation.

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

---

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

CHAPTER II

RESPONSIBILITIES OF THE MEMBER STATES

Article 6

National systems

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

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

Each Member State shall transmit its alerts via its N.SIS.

Article 7

N.SIS Office and SIRENE Bureau

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

   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.

   (deleted)

2. Each Member State shall designate a national authority which shall be operational 24 hours a day, 7 days a week and 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(4). The SIRENE Bureau shall serve as single contact point for Member States to exchange supplementary information regarding alerts and to facilitate the requested actions to be taken when alerts on persons have been entered in SIS and those persons are located following a hit.

The SIRENE Bureau shall, in accordance with national law, have easy direct or indirect access to all relevant national information, including national databases and all information on its own alerts, and to expert advice to be able to react to requests for supplementary information swiftly and within the deadlines provided for 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 Office and of their SIRENE Bureau. The Agency shall publish the list of them together with the list referred to in Article 36(8).

Article 8

Exchange of supplementary information

1. Supplementary information shall be exchanged in accordance with the provisions of the SIRENE Manual referred to in paragraph 4 and using the Communication Infrastructure. Member States shall provide the necessary technical and human resources to ensure the continuous availability and timely and effective exchange of supplementary information. In the event that the Communication Infrastructure is unavailable, Member States shall use other adequately secured technical means to exchange supplementary information. A list of adequately secured technical means shall be laid down in the SIRENE Manual referred to in paragraph 4.

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

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

Requests for supplementary information with highest priority shall be marked ‘URGENT’, in the SIRENE forms, and the reason for urgency shall be specified.

4. The Commission shall adopt implementing acts to lay down detailed rules for the tasks of the SIRENE Bureaux pursuant to this Regulation and the exchange of supplementary information in the form of a manual entitled the 'SIRENE Manual'. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 55(2).

Article 9

Technical and functional compliance

1. When setting up its N.SIS, each Member State shall comply with common standards, protocols and technical procedures established to ensure the compatibility of its N.SIS with CS-SIS for the prompt and effective transmission of data.

2. If a Member State uses a national copy, it shall ensure, by means of the services provided by CS-SIS and by means of automatic updates referred to in Article 4(4) that the data stored in the national copy are identical to and consistent with the SIS database, and that a search in its national copy produces a result equivalent to that of a search in the SIS database.

2a. End-users shall receive the data required to perform their tasks, in particular and where necessary all the available data allowing for the identification of the data subject and the required action to be taken.

2b. Member States and the Agency shall undertake regular tests to verify the technical compliance of the national copies referred to in paragraph 2. The results of these tests shall be taken into consideration as part of the mechanism established by Regulation (EU) No 1053/2013.

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

Article 10

Security – Member States

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

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

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

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

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

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

(ea) prevent the unauthorised processing of data in SIS and any unauthorised modification or erasure of data processed in SIS (control of data entry);

(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 identifiers and confidential access modes only (data access control);

(g) ensure that all authorities with a right of access to SIS or to the data processing facilities create profiles describing the functions and responsibilities of persons who are authorised to access, enter, update, delete and search the data and make these profiles available to the national supervisory authorities referred to in Article 50(1) without delay upon their request (personnel profiles);

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

(i) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems, when, by whom and for what purpose the data were input (input control);

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

(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);

(ka) ensure that the installed system may, in case of interruption, be restored (recovery); and

(kb) ensure that SIS performs its functions correctly, that faults are reported (reliability) and that personal data stored in SIS cannot be corrupted by means of the system malfunctioning (integrity).

2. Member States shall take measures equivalent to those referred to in paragraph 1 as regards security in respect of the processing and exchange of supplementary information, including securing the premises of the SIRENE Bureau.

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

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

Article 11

Confidentiality – Member States

1. Each Member State shall apply its rules of professional secrecy or other equivalent duties of confidentiality to all persons and bodies required to work with SIS data and supplementary information, in accordance with its national law. That obligation shall also apply after those persons leave office or employment or after the termination of the activities of those bodies.

2. Where a Member State cooperates with external contractors in any SIS-related tasks, that Member State shall closely monitor the activities of the contractor to ensure compliance with all provisions of this Regulation, including in particular security, confidentiality and data protection.

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

Article 12

Keeping of logs at national level

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

2. The logs shall show, in particular, the history of the alert, the date and time of the data processing activity, the data used to perform a search, a reference to the data processed and the individual and unique user identifiers of both the competent authority and the person processing the data.

3. By way of derogation from paragraph 2, if the search is carried out with dactyloscopic data or facial image in accordance with Article 22 the logs shall show the type of data used to perform the search instead of the actual data.

4. The logs may be used only for the purpose referred to in paragraph 1 and shall be deleted three years after their creation. The logs which include the history of alerts shall be deleted three years after deletion of the alerts.

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

6. The competent national 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.

Article 13

Self-monitoring

Member States shall ensure that each authority entitled to access SIS data takes the measures necessary to comply with this Regulation and cooperates, where necessary, with the national supervisory authority.

Article 14

Staff training

1. Before being authorised to process data stored in SIS and periodically after access to SIS data has been granted, the staff of the authorities having a right to access SIS shall receive appropriate training about data security, fundamental rights including data protection rules and the procedures on data processing as set out in the SIRENE Manual referred to in Article 8(4). The staff shall be informed of any relevant criminal offences and penalties, including those laid down in accordance with Article 53a of this Regulation.

2. Member States shall have a national SIS training programme. This training programme shall include training for end-users as well as the staff of the SIRENE Bureaux.

   This training programme may be part of a generic training approach and programme at national level encompassing training in other relevant areas.

3. Common training courses shall be organised at EU level at least once a year to enhance cooperation between SIRENE Bureaux.

CHAPTER III

RESPONSIBILITIES OF THE AGENCY

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 technology, subject to 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;

(d) tasks relating to implementation of the budget;

(e) acquisition and renewal;

(f) contractual matters.

3. (deleted)

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, 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.

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

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

5a. The Agency shall also perform tasks related to providing training on the technical use of SIS and on measures to improve the quality of SIS data.

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 set out in Article 9 of this Regulation.

7. The Commission shall adopt an implementing act to set out the technical requirements of the Communication Infrastructure referred to in paragraph 2. This implementing act shall be adopted in accordance with the examination procedure referred to in Article 55(2).

Article 16

Security –Agency

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

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

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

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

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

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

(ea) prevent the unauthorised processing of data in SIS and any unauthorised modification or erasure of data processed in SIS (control of data entry);

(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 identifiers and confidential access modes only (data access control);

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

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

(i) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems, when and by whom the data were input (input control);

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

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

(ka) ensure that the system installed may, in case of interruption, be restored (recovery);

(kb) ensure that SIS performs its functions correctly, that faults are reported (reliability) and that personal data stored in SIS cannot be corrupted by means of the system malfunctioning (integrity);

(kc) ensure the security of its technical sites.

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

Article 17

Confidentiality – Agency

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

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

3. Where the Agency cooperates with external contractors in any SIS-related tasks, it shall closely monitor the activities of the contractor to ensure compliance with all provisions of this Regulation, including in particular security, confidentiality and data protection.

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

Article 18

Keeping of logs at central level

1. 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 alert, the date and time of the data processing activity, the data used to perform a search, a reference to the data processed and the individual and unique user identifiers of the competent authority processing the data.

3. By way of derogation from paragraph 2, if the search is carried out with dactyloscopic data or facial image in accordance with Article 22 the logs shall show the type of data used to perform the search instead of the actual data.

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

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

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

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

CHAPTER IV

INFORMATION TO THE PUBLIC

Article 19

SIS information campaigns

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

CHAPTER V

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

Article 20

Categories of data

1. Without prejudice to Article 8(1) or the provisions of this Regulation providing for the storage of additional data, SIS shall contain only those categories of data which are supplied by each of the Member States, as required for the purposes laid down in Articles 24 and 24A.

2. Any alert in SIS which includes information on persons shall only contain the following data:

   (a) surnames;

   (b) forenames;

   (c) names at birth;

   (d) previously used names and aliases;

   (e) any specific, objective, physical characteristics not subject to change;

   (f) place of birth;

(g) date of birth;

(h) gender;

(i) nationality/nationalities;

(j) whether the person concerned:

i. is armed;

ii. is violent;

iii. has absconded or escaped;

iv. poses a risk of suicide;

v. poses a threat to public health; or

vi. is involved in an activity as referred to in Articles 3 to 14 of Directive (EU) 2017/541;

(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) links to other alerts issued in SIS pursuant to Article 43;

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

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

- a previous conviction as referred to in Article 24(2)(a);
- a serious security threat as referred to in Article 24(2)(b);
- circumvention of Union or national law on entry and stay as referred to in Article 24(2)(c);
- an entry ban as referred to in Article 24(1)(b); or
- a restrictive measure as referred to in Article 24A;

(r) type of offence;

(s) the category of the person's identification documents;

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

(u) the number(s) of the person's identification documents;

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

(w) photographs and facial images;

(x) dactyloscopic data;

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

3. 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 and the common standards referred to in paragraph 4. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 55(2).

4. These technical rules shall be similar for searches in CS-SIS, in national or shared copies and in technical copies, as referred to in Article 36(2) and they shall be based on common standards.

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 existence of an alert in SIS.

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

Article 22

(moved to Art 27A)

Article 23

Requirement for an alert to be entered

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

2. (deleted)

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

Article 23a

Compatibility of alerts

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

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

3. Where a person is already the subject of an alert in SIS, a Member State wishing to enter a new alert shall check that there is no incompatibility between the alerts. If there is no incompatibility, the Member State may enter the new alert. If the alerts are incompatible, the SIRENE Bureaux concerned shall consult each other by exchanging supplementary information in order to reach an agreement. Rules on the compatibility of alerts shall be laid down in the SIRENE Manual referred to in Article 8(4). Departures from the compatibility rules may be made after consultation between the Member States if essential national interests are at stake.

4. In case of simultaneous hits on multiple alerts on the same person the executing Member State shall observe the priority rules of alerts as laid down in the SIRENE Manual referred to in Article 8(4).

In case a person is subject to multiple alerts issued by different Member States alerts for arrest issued pursuant to Article 26 of Regulation (EU) 2018/xxx [police cooperation and judicial cooperation in criminal matters] shall be executed as a priority subject to Article 25 of that Regulation.

Article 24

Conditions for issuing alerts on refusal of entry and stay

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

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

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

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

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

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

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

3. (deleted)

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

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

Article 24A

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

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

2. The alerts shall be entered, kept up-to-date and deleted by the competent authority of the Member State which holds the Presidency of the Council of the European Union at the time of the adoption of the measure. If that Member State does not have access to SIS or alerts under Article 24 the responsibility shall be taken up by the Member State which holds the subsequent Presidency and has access to SIS, including access to the alerts under Article 24.

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

Article 25

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

1. An alert concerning a third-country national who is a beneficiary of the right of free movement within the Union, within the meaning of Directive 2004/38/EC of the European Parliament and of the Council[32] or within the meaning of an agreement between the Union or the Union and its Members States on the one hand, and a third country on the other hand, shall be in conformity with the rules adopted in implementation of that Directive or that agreement.

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

Article 26A

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

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

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

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

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

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

---

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

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

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

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

Article 26B

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

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

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

(b) the exchange of information referred to in point (a) shall contain sufficient information about the reasons for the decision referred to in Article 24;

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

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

(e) within fourteen calendar days after the receipt of the consultation request the granting Member State shall notify the Member State that has taken the decision referred to in Article 24 about its decision or where it was impossible to take a decision within that period shall make a reasoned request to prolong the time period for the response; the period may exceptionally be extended for a maximum of further twelve calendar days;

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

Article 26C

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

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

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

(b) the exchange of information referred to in point (a) shall contain sufficient information about the reasons for the refusal of entry and stay alert;

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

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

(e) within fourteen calendar days after the receipt of the consultation request the granting Member State shall notify the issuing Member State or where it was impossible to take a decision within that period shall make a reasoned request to prolong the time period for the response; the period may exceptionally be extended for a maximum of further twelve calendar days;

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

Article 26D

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

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

(a) the executing Member State shall inform the issuing Member State about the situation and the issuing Member State shall initiate the procedure laid down in Article 26C;

(b) the issuing Member State shall notify the executing Member State about the final outcome of the consultation.

The decision on the entry of the third-country national shall be taken by the executing Member State in accordance with the Schengen Borders Code.

Article 26E

Statistics

Member States shall provide on an annual basis statistics to the Agency about the exchanges of information carried out in accordance with Article 26A to Article 26D and the instances in which the deadlines were not met.

Article 27

(moved to Article 24A)

CHAPTER VI

SEARCH WITH BIOMETRIC DATA

Article 27A

Specific rules for entering photographs, facial images and dactyloscopic data

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

1a. Dactyloscopic data entered in SIS may consist of one to ten flat fingerprints and one to ten rolled fingerprints. It may also include up to two palm prints.

2. Quality standards and technical specifications shall be established for the storage of the biometric data referred to in paragraph 1. These quality standards and technical specifications shall set the level of quality required for using the data to verify the identity of the person in accordance with Article 28(1) and for using the data to identify the person in accordance with Article 28(2)-(4).

2a. The Commission shall adopt implementing acts to lay down the quality standards and technical specifications referred to in paragraphs 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 55(2).

Article 28

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

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

2. If the identity of the person cannot be ascertained by other means, dactyloscopic data shall be searched for identification purposes. Dactyloscopic data may be searched in all cases to identify a person. For this purpose the Central SIS shall contain an Automated Fingerprint Identification System (AFIS).

3. Dactyloscopic data stored in SIS in relation to alerts issued under Articles 24 and 24A may also be searched with complete or incomplete sets of fingerprints or palm prints discovered at the scenes of serious crimes or terrorist offences under investigation and where it can be established to a high degree of probability that they belong to a perpetrator of the offence provided that the search is carried out simultaneously in their relevant national fingerprints databases.

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 in the context of regular border crossing points.

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

After the start of the use of the functionality at regular border crossing points, the Commission is empowered to adopt delegated acts in accordance with Article 54a to supplement this Regulation concerning the determination of other circumstances in which photographs and facial images may be used for the identification of persons.

CHAPTER VII

RIGHT TO ACCESS AND REVIEW OF ALERTS

Article 29

Authorities having a right to access alerts

1. National competent authorities responsible for the identification of third-country nationals shall have access to data entered in SIS and the right to search such data directly or in a copy of SIS data 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) the prevention, detection, investigation or prosecution of terrorist offences or other serious criminal offences or the execution of criminal penalties, within the Member State concerned, provided that Directive (EU) 2016/680 applies;

   (d) examining the conditions and taking decisions related to the entry and stay of third-country nationals on the territory of the Member States, including on residence permits and long-stay visas, and to the return of third-country nationals, as well as checks on third-country nationals who are illegally entering or staying on the territory of the Member States.

(da) security checks on third-country nationals who apply for international protection, insofar as those authorities do not constitute "determining authorities" as defined in Article 2(f) of Directive 2013/32/EU of the European Parliament and of the Council[33], and, where relevant, providing advice in accordance with Council Regulation (EU) 377/2004[34];

(e) examining visa applications and taking decisions related to those applications including on whether to annul, revoke or extend visas, in accordance with Regulation (EU) No 810/2009 of the European Parliament and of the Council.[35]

1a. The right to access data entered in SIS and the right to search such data directly may be exercised by national competent authorities responsible for naturalisation, as provided for in national law, for the purposes of examining an application for naturalisation.

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

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

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

---

33 Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection (OJ L 180, 29.6.2013, p. 60).

34 Council Regulation (EC) No 377/2004 of 19 February 2004 on the creation of an immigration liaison officers network (OJ L 64, 2.3.2004, p. 1).

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

Article 30

Access to SIS data by Europol

1. The European Union Agency for Law Enforcement Cooperation (Europol) shall, where necessary to fulfil its mandate, have the right to access and search data entered into SIS and may exchange and further request supplementary information in accordance with the provisions of the SIRENE Manual laid down in Article 8.

2. Where a search by Europol reveals the existence of an alert in SIS, Europol shall inform the issuing Member State through the exchange of supplementary information by means of the Communication Infrastructure and in accordance with the provisions set out in the SIRENE Manual. Until Europol is able to use the functionalities intended for the exchange of supplementary information, it shall inform issuing Member States 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 comparing with its databases and operational analysis projects, aimed at identifying connections or other relevant links and for strategic, thematic or operational analyses as defined in points (a), (b) and (c) of Article 18(2) of Regulation (EU) 2016/794. Any processing by Europol of supplementary information for the purpose of this Article shall be carried out in accordance with Regulation (EU) 2016/794.

3. The use of information obtained from a search in SIS or from the processing of supplementary information is subject to the consent of the issuing Member State. If the Member State allows the use of such information, the handling thereof by Europol shall be governed by Regulation (EU) 2016/794. Europol may only communicate such information to third countries and third bodies with the consent of the issuing Member State and in full respect of Union law on data protection.

4. (deleted)

5. Europol shall:

   (a) without prejudice to paragraphs 3 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. By way of derogation, where Europol has information in its databases or operational analysis projects on a case to which the supplementary information is related, in order for Europol to perform its tasks, Europol may exceptionally continue to store the supplementary information when necessary. Europol shall inform the issuing and the executing Member State of the continued storage of such supplementary information and present a justification of such continued storage.

(b) limit access to data entered in SIS, including supplementary information, to specifically authorised staff of Europol requiring access for the performance of their tasks;

(c) adopt and apply measures to ensure security, confidentiality and self-monitoring in accordance with Articles 10, 11 and 13;

(ca) ensure that its staff authorized to process SIS data receives appropriate training and information in accordance with Article 14(1); and

(d) without prejudice to Regulation (EU) 2016/794, allow the European Data Protection Supervisor to monitor and review the activities of Europol in the exercise of its right to access and search data 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. (deleted)

8. (deleted)

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

9a. Member States shall inform Europol through the exchange of supplementary information of any hit on alerts related to terrorist offences. Member States may exceptionally refrain from informing Europol if doing so would jeopardise current investigations, the safety of an individual or be contrary to essential interests of the security of the issuing Member State.

9b. Paragraph (9a) shall apply from the date when Europol is able to receive supplementary information in accordance with paragraph 1.

Article 31

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

1. In accordance with Article 40(8) of Regulation (EU) 2016/1624, the members of the teams as defined in Article 2(8) and (9) of Regulation (EU) 2016/1624 shall, within their mandate and provided that they are authorised to carry out checks in accordance with Article 29(1) and have received the required training in accordance with Article 14(1), have the right to access and search data entered in SIS in so far it is necessary for the performance of their task and as required by the operational plan for a specific operation. Access to data entered in SIS shall not be extended to any other team members.

2. Members of the teams referred to in paragraph 1 shall exercise the right to access and search data entered in SIS in accordance with paragraph 1 via a technical interface which is set up and maintained by the European Border and Coast Guard Agency and which allows a direct connection to Central SIS.

3. Where a search by a member of the teams referred to in paragraph 1 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. For the purpose of verifying the lawfulness of data processing, self-monitoring and ensuring proper data security and integrity the European Border and Coast Guard Agency shall keep logs of every access to and search in SIS in accordance with the provisions of Article 12.

5. (deleted)

6. The European Border and Coast Guard Agency shall adopt and apply measures to ensure security, confidentiality and self-monitoring in accordance with Articles 10, 11 and 13 and shall ensure that the teams referred to in paragraph 1 apply those measures.

7. 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.

8. Without prejudice to paragraph 2 no parts of SIS shall be connected to any computer system for data collection and processing operated by the teams referred to in paragraph 1 of this Article or by the European Border and Coast Guard Agency, nor shall the data contained in SIS to which those teams have access be transferred to such a system. No part of SIS shall be downloaded. The logging of access and searches shall not be construed to be the downloading or copying of SIS data.

9. Without prejudice to the further provisions of [new Regulation 45/2001], the European Border and Coast Guard Agency shall allow the European Data Protection Supervisor to monitor and review the activities of the teams as referred to in this Article in the exercise of their right to access and search data entered in SIS.

Article 32

(deleted)

Article 32A

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

1. The Commission shall carry out an evaluation of the operation and the use of SIS in accordance with this Regulation by Europol and the teams referred to in Article 31(1) at least every five years.

2. Europol and the EBCG Agency shall ensure adequate follow-up to the findings and recommendations stemming from this evaluation.

3. A report on the results and follow-up of the evaluation shall be sent to the European Parliament and to the Council.

Article 33

Scope of access

End-users, including Europol and the members of the teams as defined in Article 2(8) and (9) of Regulation (EU) 2016/1624, may only access data which they require for the performance of their tasks.

Article 34

Review period of alerts

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

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

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

4. 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 and proportionate 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.

5. Alerts shall automatically be deleted after the review period referred to in paragraph 2 except where the issuing Member State has informed CS-SIS about the extension of the alert 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.

6. Member States shall keep statistics about the number of alerts which have been extended in accordance with paragraph 5 and transmit them, upon request, to the supervisory authorities referred to in Article 50.

7. As soon as 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 immediately notify the authority which created the alert. The authority shall have fifteen calendar days from the receipt of that notification to indicate that the alert has been or shall be deleted or shall state reasons for the retention of the alert. If the fifteen-day period expires without such a reply, the SIRENE Bureau shall ensure that the alert is deleted. Where permissible under national law 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.

Article 35

Deletion of alerts

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

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

3. Alerts issued in respect of a person who has acquired citizenship of any State whose nationals are beneficiaries of the right of free movement under the Union Law shall be deleted as soon as the issuing Member State becomes aware, or is informed pursuant to Article 39 that the person in question has acquired such citizenship.

CHAPTER VIII

GENERAL DATA PROCESSING RULES

Article 36

Processing of SIS data

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

2. Data may only be copied for technical purposes, provided that such copying is necessary in order for the authorities referred to in Article 29 to carry out a direct search. The provisions of this Regulation shall apply to such copies. A Member State shall not copy alert data or additional data entered by another Member State from its N.SIS or from the CS-SIS into other national data files.

3. Technical copies, as referred to in paragraph 2, which lead to off-line databases may be retained for a period not exceeding 48 hours.

   Notwithstanding the first subparagraph, technical copies which lead to off-line databases to be used by visa issuing authorities shall not be permitted, except for copies made to be used only in an emergency following the unavailability of the network for more than 24 hours.

   Member States shall keep an up-to-date inventory of those copies, make that inventory available to their national supervisory authority, and ensure that the provisions of this Regulation, in particular those of Article 10, are applied in respect of those copies.

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

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

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

7. Any use of data which does not comply with paragraphs 1 to 6 shall be considered as misuse under the national law of each Member State and subject to penalties in accordance with Article 53a of this Regulation.

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. The Agency shall maintain a continuously updated list on its website containing changes sent by Member States between the annual publications.

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

Article 37

SIS data and national files

1. Article 36(2) shall not prejudice the right of a Member State to keep in its national files SIS data in connection with which action has been taken on its territory. Such data shall be kept in national files for a maximum period of three years, except if specific provisions in national law provide for a longer retention period.

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

Article 38

Information in case of non-execution of alert

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

Article 39

Quality of the data processed in SIS

1. An issuing Member State shall be responsible for ensuring that the data are accurate, up-to-date and entered in SIS lawfully.

1a. Where an issuing Member State receives relevant additional or modified data as listed in Article 20(2), that Member State shall complete or modify the alert without delay.

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

2a. Where a Member State other than the issuing Member State has relevant additional or modified data as listed in Article 20(2), it shall transmit them without delay, through the exchange of supplementary information, to the issuing Member State to enable the latter to complete or modify the alert. The data shall only be transmitted if the identity of the third-country national is ascertained.

3. Where a Member State other than the issuing Member State has evidence suggesting that an item of data is factually incorrect or has been unlawfully stored, it shall, through the exchange of supplementary information, inform the issuing Member State at the earliest opportunity and not later than two working 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 national supervisory authorities concerned and to the European Data Protection Supervisor for a decision, by means of cooperation in accordance with Article 52.

5. The Member States shall exchange supplementary information where a person complains that he or she is not the person wanted by an alert. Where the outcome of the check shows that there are in fact two different persons the complainant shall be informed of the measures laid down in Article 42 and of his or her right to redress in accordance with Article 49(1).

6. (deleted)

Article 40

Security incidents

1. Any event that has or may have an impact on the security of SIS or may cause damage or loss to SIS data or to the supplementary information shall be considered to be a security incident, especially where unlawful access to data may have occurred or where the availability, integrity and confidentiality of data has or may have been compromised.

2. Security incidents shall be managed to ensure a quick, effective and proper response.

3. Without prejudice to the notification and communication of a personal data breach pursuant to Article 33 of Regulation (EU) No 2016/679 or to Article 30 of Directive (EU) No 2016/680, Member States, Europol and the European Border and Coast Guard Agency shall notify the Commission, the Agency, the national supervisory authority and the European Data Protection Supervisor without delay of security incidents The Agency shall notify the Commission and the European Data Protection Supervisor without delay of any security incident concerning the CS-SIS.

4. Information regarding a security incident that has or may have an impact on the operation of SIS in a Member State or within the Agency or on the availability, integrity and confidentiality of the data entered or sent by other Member States or on supplementary information exchanged, shall be provided to all the Member States without delay and reported in compliance with the incident management plan provided by the Agency.

4a. The Member States and the Agency shall collaborate in the event of a security incident.

4b. The Commission shall report serious incidents immediately to the European Parliament and the Council. These reports shall be classified as EU RESTRICTED/RESTREINT UE in accordance with applicable security rules.

4c. Where a security incident is caused by the misuse of data, Member States, Europol and the European Border and Coast Guard Agency shall ensure that penalties or disciplinary measures are imposed in accordance with Article 53a.

Article 41

Distinguishing between persons with similar characteristics

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

(a) the SIRENE Bureau shall contact within 12 hours the issuing Member State via the exchange of supplementary information 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 23a. Where the outcome of the check is that there are in fact two different persons, the SIRENE Bureau shall approve the request for entering the second alert by adding the necessary elements to avoid any misidentifications.

Article 42

Additional data for the purpose of dealing with misused identities

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

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, and subject to the explicit consent of the person whose identity was misused for each data category, only the following personal data of the person whose identity has been misused may be entered and further processed in SIS:

   (a) surnames;

   (b) forenames;

   (c) names at birth;

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

   (e) any specific objective and physical characteristic not subject to change;

   (f) place of birth;

   (g) date of birth;

   (h) gender;

   (i) photographs and facial images;

   (j) fingerprints, palm prints or both

   (k) nationality/nationalities;

(l) the category of the person's identification documents;

(m) the country of issue of the person's identification documents;

(n) the number(s) of the person's identification documents;

(o) the date of issue of a person's identification documents;

(p) address of the person;

(q) person's father's name;

(r) person's mother's name.

4. The Commission shall adopt implementing acts to lay down and develop technical rules necessary for entering and further processing the data referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 55(2).

5. The data referred to in paragraph 3 shall be deleted at the same time as the corresponding alert or earlier where the person so requests.

6. Only the authorities having a right of access to the corresponding alert may access the data referred to in paragraph 3. They may do so for the sole purpose of avoiding misidentification.

Article 43

Links between alerts

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

2. The creation of a link shall not affect the specific action to be taken on the basis of each linked alert or the review period of each of the linked alerts.

3. The creation of a link shall not affect the rights of access provided for in this Regulation. Authorities with no right of access to certain categories of alerts shall not be able to see the link to an alert to which they do not have access.

4. A Member State shall create a link between alerts when there is an operational need.

5. Where a Member State considers that the creation by another Member State of a link between alerts is incompatible with its national law or 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 Article 55(2).

Article 44

Purpose and retention period of supplementary information

1. Member States shall keep a reference to the decisions giving rise to an alert at the SIRENE Bureau in order to support the exchange of supplementary information.

2. Personal data held in files by the SIRENE Bureau as a result of information exchanged shall be kept only for such time as may be required to achieve the purposes for which they were supplied. They shall in any event be deleted at the latest one year after the related alert has been deleted from SIS.

3. Paragraph 2 shall not prejudice the right of a Member State to keep in national files data relating to a particular alert which that Member State has issued or to an alert in connection with which action has been taken on its territory. The period for which such data may be held in such files shall be governed by national law.

Article 45

Transfer of personal data to third parties

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

CHAPTER IX

DATA PROTECTION

Article 46

Applicable legislation

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

2. Regulation (EU) 2016/679 shall apply to the processing of personal data by the authorities referred to in Article 29 of this Regulation with the exception of processing for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security where Directive 2016/680 applies.

3. (deleted)

Article 46A

Right of information

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

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

Article 47

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

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

2. (deleted)

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

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

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

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

(c) protect public security;

(d) protect national security; or

(e) protect the rights and freedoms of others.

In such cases, the Member State shall inform the data subject in writing, without undue delay, of any refusal or restriction of access and of the reasons for the refusal or restriction. Such information may be omitted where its provision would undermine a purpose under this paragraph. The Member State shall inform the data subject of the possibility of lodging a complaint with a supervisory authority or of seeking a judicial remedy.

The Member State shall document the factual or legal reasons on which the decision is based. That information shall be made available to the supervisory authorities.

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

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

6. (deleted)

Article 48

Moved to Article 46A

Article 49

Remedies

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

2. The Member States undertake mutually to enforce final decisions handed down by the courts or authorities referred to in paragraph 1 of this Article, without prejudice to the provisions of Article 53.

3. Member States shall report annually on:

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

   (b) the number of access requests submitted to the 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) the number of court proceedings launched;

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

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

   A template for the reporting referred to in the first subparagraph shall be developed by the Commission. The reports from the Member States shall be forwarded to the European Data Protection Board established by Regulation (EU) 2016/679 and included in the joint report referred to in Article 52(4).

Article 50

Supervision of N.SIS

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

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

Article 51

Supervision of the Agency

1. The European Data Protection Supervisor shall be responsible for monitoring the personal data processing activities of the Agency and for ensuring that those activities are carried out in accordance with this Regulation. The tasks and powers referred to in Articles 58[36] and 59[37] of Regulation (EC) 2018/XXX [new data protection Regulation for Union institutions and bodies] shall apply accordingly.

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

Article 52

Cooperation between national supervisory authorities and the European Data Protection Supervisor

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

---

36 This number is not the definitive one [*LL: please remove this footnote.*]

37 This number is not the definitive one [*LL: please remove this footnote.*]

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 annually by the Board established by Regulation (EU) 2016/679 to the European Parliament, the Council, and the Commission.

CHAPTER X

LIABILITY AND PENALTIES

Article 53

Liability

1. Without prejudice to the right to compensation from, and liability under Regulation (EU) 2016/679, Directive (EU) 2016/680 and [new Regulation (EC) No 45/2001]:

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

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

   That Member State or the Agency shall be exempted from their liability, in whole or in part, if they prove that they are not responsible for the event which gave rise to the damage.

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

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

Article 53A

Penalties

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

The penalties provided shall be effective, proportionate and dissuasive.

CHAPTER XI

FINAL PROVISIONS

Article 54

Monitoring and statistics

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

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

3. The Agency shall produce, daily, monthly and annual statistics showing the number of records per category of alert, in total, and for each Member State. The Agency shall also provide annual reports on the number of hits per category of alert, how many times SIS was searched and how many times SIS was accessed for the purpose of entering, updating or deleting an alert, in total and for each Member State, including statistics about the exchanges of information in accordance with Article 26A to Article 26E. The statistics produced shall not contain any personal data. The annual statistical report shall be published.

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

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

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

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

6. For the purpose of paragraphs 3, 4 and 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 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. Upon request, the Agency shall give access to Member States, the Commission, Europol, and the European Border and Coast Guard Agency, to the extent required for the performance of their tasks, 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.

7. Two years after the start of operations of SIS pursuant to this Regulation and every two years thereafter, the Agency shall submit to the European Parliament and the Council a report on the technical functioning of Central SIS and the Communication Infrastructure, including the security thereof, the automated fingerprint identification system and the bilateral and multilateral exchange of supplementary information between Member States. This report shall also contain, once the technology is in use, an evaluation of the use of facial images to identify persons.

8. Three years after the start of operations of SIS pursuant to this Regulation and every four years thereafter, the Commission shall produce an overall evaluation of Central SIS and the bilateral and multilateral exchange of supplementary information between Member States. That overall evaluation shall include an examination of results achieved against objectives, and an assessment of the continuing validity of the underlying rationale, the application of this Regulation in respect of Central SIS, the security of Central SIS and any implications for future operations. The overall evaluation report shall also include an assessment of the automated fingerprint identification system and the SIS information campaigns organised by the Commission in accordance with Article 19.

   It shall also contain statistics on the number of alerts under Article 24 which fall respectively under paragraph 1(a) and paragraph 1(b). As regards alerts falling under paragraph 1(a) it shall detail how many alerts were issued following the situations referred to in paragraph 2(a), paragraph (2b) and paragraph 2(c). The overall evaluation report shall also contain an assessment of the application of Article 24 by Member States.

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

9. The Commission shall adopt implementing acts to lay down detailed rules on the operation of the central repository referred to in paragraph 6 and the data protection and security rules applicable to that repository. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 55(2).

Article 54a

Exercise of the delegation

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

2. The power to adopt delegated acts referred to in Article 28(4) shall be conferred on the Commission for an indeterminate period of time from ... [*the date of entry into force of this Regulation*].

3. The delegation of power referred to in Article 28(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

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

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

6. A delegated act adopted pursuant to Article 28(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 55

Committee procedure

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

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

Article 56

(deleted)

Article 56a

Amendments to Regulation (EC) No 1987/2006

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

1) Article 6 is replaced by the following:

"Article 6

National Systems

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

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

2) in Article 11, the following paragraphs 2 and 3 are added:

"2. Where a Member State cooperates with external contractors in any SIS II-related tasks, that Member State shall closely monitor the activities of the contractor to ensure compliance with all provisions of this Regulation, including in particular security, confidentiality and data protection.

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

3) Article 15 is amended as follows:

(a) the following paragraph 3a is inserted:

"3a. The Management Authority shall develop and maintain a mechanism and procedures for carrying out quality checks on the data in CS-SIS and shall provide regular reports to the Member States. The Management Authority shall provide a regular report to the Commission covering the issues encountered and the Member States concerned. The Commission shall provide the European Parliament and the Council with a regular report on data quality issues encountered."

(b) paragraph 8 is replaced by the following:

"8. Operational management of Central SIS II shall consist of all the tasks necessary to keep Central SIS II 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 II and the national systems, ensuring that Central SIS II and the national systems operate in accordance with the technical requirements set out in Article 9 of this Regulation."

4) In Article 17, the following paragraphs 3 and 4 are added:

"3. Where the Management Authority cooperates with external contractors in any SIS II-related tasks, it shall closely monitor the activities of the contractor to ensure compliance with all provisions of this Regulation, including in particular security, confidentiality and data protection.

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

5) In Article 20, paragraph 2, the following point (ka) is added:

"(ka) the type of offence"

6) In Article 21, the following second subparagraph is added:

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

7) Article 22 is replaced by the following:

"Article 22

Specific rules for verification or search with photographs and fingerprints

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

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

3. If the identity of the person cannot be ascertained by other means, fingerprint data shall be searched for identification purposes. Fingerprint data may be searched in all cases to identify a person. For this purpose the Central SIS II shall contain an Automated Fingerprint Identification System (AFIS).

4. Fingerprint data stored in SIS II in relation to alerts issued under Articles 24 and 26 may also be searched with complete or incomplete sets of fingerprints discovered at the scenes of serious crimes or terrorist offences under investigation and where it can be established to a high degree of probability that they belong to a perpetrator of the offence provided that the search is carried out simultaneously in their relevant national fingerprints databases."

8) Article 26 is replaced by the following:

"Article 26

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

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

2. The alerts shall be entered, kept up-to-date and deleted by the competent authority of the Member State which holds the Presidency of the Council of the European Union at the time of the adoption of the measure. If that Member State does not have access to SIS II or alerts under Article 24, the responsibility shall be taken up by the Member State which holds the subsequent Presidency and has access to SIS II, including access to the alerts under Article 24. Member States shall put in place the necessary procedures for entering, updating and deleting such alerts."

9) the following Articles 27a and 27b are inserted:

"*Article 27a*

Access to SIS II data by Europol

1. The European Union Agency for Law Enforcement Cooperation (Europol) shall, where necessary to fulfil its mandate, have the right to access and search data entered into SIS II and may exchange and further request supplementary information in accordance with the provisions of the SIRENE Manual laid down in Article 8.

2. Where a search by Europol reveals the existence of an alert in SIS II, Europol shall inform the issuing Member State through the exchange of supplementary information by means of the communication infrastructure and in accordance with the provisions set out in the SIRENE Manual. Until Europol is able to use the functionalities intended for the exchange of supplementary information, it shall inform issuing Member States via the channels defined by Regulation (EU) 2016/794.

3. Europol may process the supplementary information that has been provided to it by Member States for the purposes of comparing with its databases and operational analysis projects, aimed at identifying connections or other relevant links and for strategic, thematic or operational analyses as defined in points (a), (b) and (c) of Article 18(2) of Regulation (EU) 2016/794. Any processing by Europol of supplementary information for the purpose of this Article shall be carried out in accordance with Regulation (EU) 2016/794.

4. The use of information obtained from a search in SIS II or from the processing of supplementary information is subject to the consent of the issuing Member State. If the Member State allows the use of such information, the handling thereof by Europol shall be governed by Regulation (EU) 2016/794. Europol may only communicate such information to third countries and third bodies with the consent of the issuing Member State and in full respect of Union law on data protection.

5. Europol shall:

   a) without prejudice to paragraphs 3 and 6, not connect parts of SIS II 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 II;

   b) notwithstanding Article 31(1) of Regulation (EU) 2016/794, delete supplementary information containing personal data at the latest one year after the related alert has been deleted from SIS II. By way of derogation, where Europol has information in its databases or operational analysis projects on a case to which the supplementary information is related, in order for Europol to perform its tasks, Europol may exceptionally continue to store the supplementary information when necessary. Europol shall inform the issuing and the executing Member State of the continued storage of such supplementary information and present a justification of such continued storage;

   c) limit access to data entered in SIS II, including supplementary information to specifically authorised staff of Europol requiring access for the performance of their tasks;

   d) adopt and apply measures to ensure security, confidentiality and self-monitoring in accordance with Articles 10, 11 and 13;

e) ensure that its staff authorized to process SIS II data receives appropriate training and information in accordance with Article 14;

f) without prejudice to Regulation (EU) 2016/794, allow the European Data Protection Supervisor to monitor and review the activities of Europol in the exercise of its right to access and search data entered in SIS II 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 II 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 II data. Europol shall not copy alert data or additional data issued by Member States or from CS-SIS II into other Europol systems.

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

8. Member States shall inform Europol through the exchange of supplementary information of any hit on alerts related to terrorist offences. Member States may exceptionally refrain from informing Europol if doing so would jeopardise current investigations, the safety of an individual or be contrary to essential interests of the security of the issuing Member State.

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

Article 27b

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

1. In accordance with Article 40(8) of Regulation (EU) 2016/1624, the members of the teams as defined in Article 2(8) and (9) of Regulation (EU) 2016/1624 shall, within their mandate and provided that they are authorised to carry out checks in accordance with Article 27(1) and have received the required training in accordance with Article 14(1), have the right to access and search data entered in SIS II in so far it is necessary for the performance of their task and as required by the operational plan for a specific operation. Access to data entered in SIS II shall not be extended to any other team members.

2. Members of the teams referred to in paragraph 1 shall exercise the right to access and search data entered in SIS II in accordance with paragraph 1 via a technical interface which is set up and maintained by the European Border and Coast Guard Agency and which allows a direct connection to Central SIS II.

3. Where a search by a member of the teams as referred to in paragraph 1 reveals the existence of an alert in SIS II, the issuing Member State shall be informed thereof. In accordance with Article 40 of Regulation (EU) 2016/1624, members of the teams may only act in response to an alert in SIS II under instructions from and, as a general rule, in the presence of border guards or staff involved in return-related tasks of the host Member State in which they are operating. The host Member State may authorise members of the teams to act on its behalf.

4. For the purpose of verifying the lawfulness of data processing, self-monitoring and ensuring proper data security and integrity the European Border and Coast Guard Agency shall keep logs of every access to and search in SIS II in accordance with the provisions of Article 12.

5. The European Border and Coast Guard Agency shall adopt and apply measures to ensure security, confidentiality and self-monitoring in accordance with Articles 10, 11 and. 13 and shall ensure that the teams referred to in paragraph 1, apply those measures.

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

7. Without prejudice to paragraph 2, no parts of SIS II shall be connected to any computer system for data collection and processing operated by the teams referred to in paragraph 1 of this Article or by the European Border and Coast Guard Agency, nor shall the data contained in SIS II to which those teams have access be transferred to such a system. No part of SIS II shall be downloaded. The logging of access and searches shall not be construed to be the downloading or copying of SIS II data.

8. Without prejudice to the further provisions of [new Regulation 45/2001], the European Border and Coast Guard Agency shall allow the European Data Protection Supervisor to monitor and review the activities of the teams as referred to in this Article in the exercise of their right to access and search data entered in SIS II."

Article 56b

Amendment to the Convention implementing the Schengen Agreement.[38]

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

Article 57

Repeal

Regulation (EC) No 1987/2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) is repealed from the date of application of this Regulation set out in the first subparagraph of Article 58(4).

Article 58

Entry into force, start of operation and application

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

2. No later than 3 years after the entry into force of this Regulation the Commission shall adopt a decision setting the date on which SIS starts operations pursuant to this Regulation, after the verification that the following conditions are met:

   (a) the implementing acts necessary for the application of this Regulation have been adopted;

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

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

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

3. The Commission shall closely monitor the process of gradual fulfilment of the conditions set out in paragraph 2 and shall inform the European Parliament and the Council about the outcome of the verification.

3a. By [one year after the entry into force of this Regulation] *[OPOCE, please replace with the actual date]* and every year thereafter until the decision of the Commission referred to in paragraph 2 has been taken, the Commission shall submit a report to the European Parliament and the Council on the state of play of the preparation of the full implementation of this Regulation. That report shall contain also detailed information about the costs incurred and information as to any risks which may impact the overall costs.

4. This Regulation shall apply from the date determined in accordance with paragraph 2.

By way of derogation from the first subparagraph:

(a) Article 4(3a), Article 5(2) to (4), Article 8(4), Article 9(1) and (3), Article 15(7), Article 19, Article 20(3) and (4), Article 27A(2), Article 28(4), Article 42(4), Article 43(4), Article 54(6) and (9), Article 54a, Article 55, Article 56a (1) to (6) and (8), Article 58(3)-(3a) shall apply from the date of entry into force of this Regulation;

(b) Article 56a(9) shall apply from [one year after the entry into force of this Regulation];

(c) Article 56a(7) shall apply from [two years after the entry into force of this Regulation].

5. The Commission decision referred to in paragraph 2 shall be published in *the Official Journal of the European Union*.

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

Done at Brussels,

For the European Parliament
The President

For the Council
The President

ANNEX III

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 and repealing Council Decision 2007/533/JHA and repealing Regulation (EC) No 1986/2006 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) 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 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 competent national authorities, in particular border guards, police, customs, authorities responsible for the prevention, the detection, investigation or prosecution of criminal offences or the execution of criminal penalties and immigration authorities.

(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[2] (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[3] and Council Decision 2001/886/JHA (SIS)[4] and it was established by Regulation (EC) No 1987/2006[5] as well as by Council Decision 2007/533/JHA[6]. 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[1]. The recommendations set out in those documents should be reflected, as appropriate, in this Regulation.

(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[8] 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.

---

1 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.

(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, rules on the deletion of alerts, the authorities authorised to access the data, the use of biometric data and further rules on data protection and data processing.

(6a) SIS alerts contain only the information necessary for the identification of a person or an object and the action to be taken. Therefore, Member States should exchange supplementary information related to alerts where required.

(7) SIS includes a central system (Central SIS) and national systems that may contain 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 border 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.Each Member State should set up a 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 and the Communication Infrastructure should be operated to ensure its functioning 24 hours a day, 7 days a week. For this reason the Agency should implement technical solutions to reinforce the uninterrupted availability of SIS, subject to an independent impact assessment and cost-benefit analysis.

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

(9) In order to ensure the efficient exchange of supplementary information, including on 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.

(9a) Member States should ensure that the staff of the SIRENE Bureau have the necessary linguistic skills and knowledge in relevant legislation and rules of procedure to perform their tasks.

(9b) In order to be able to fully exploit the functionalities of SIS, Member States should ensure that end-users and the staff of the SIRENE Bureaux regularly receive training, including on data security and protection, as well as on data quality. SIRENE Bureax should be involved in the development of training programs. To the extent possible, SIRENE Bureaux should also provide for staff exchanges with other SIRENE Bureaux at least once a year. Member States are encouraged to take appropriate measures to avoid the loss of skills and experience through staff turnover.

(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[9] (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 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. The Commission should report to the European Parliament and the Council on data quality issues encountered. To further increase the quality of data in SIS, the Agency should also offer training on the use of SIS to national training bodies and, insofar as possible, to SIRENE Bureaux and to end-users.

(12) In order to allow better monitoring of the use of SIS to analyse trends concerning criminal offences and border management, the Agency should be able to develop a state-of-the-art capability for statistical reporting to the Member States, the European Parliament, the Council, the Commission, Europol, Eurojust and the European Border and Cost Guard Agency without jeopardising data integrity. Therefore, a central statistical repository should be established. Any statistic retained in the repository or produced by the repository should not contain personal data as defined in [new Regulation (EC) No 45/2001] of the European Parliament and of the Council. Member States should communicate statistics concerning the right of access, rectification of inaccurate data and erasure of unlawfully stored data to the cooperation mechanism.

(13) New data categories should be introduced in the SIS to allow end-users to take informed decisions based upon an alert without losing time. Therefore, in order to facilitate identification and detect multiple identities, the alert should include a reference to the personal identification document or number and a copy, whenever possible in colour, of such document, where available.

(13aa) Competent authorities should be able, where strictly necessary, to enter into SIS specific information relating to any specific, objective, physical characteristics of a person not subject to change, such as tattoos, marks or scars.

(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. Any entry and use of photographs, facial images or dactyloscopic data should not exceed what is necessary for the objectives pursued, should be authorised by Union law, respect fundamental rights, including the best interests of the child, and be in accordance with relevant provisions on data protection laid down in this Regulation and Union data protection legislation. 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, with the consent for each data category, and in particular palm prints, of the individual concerned and a strict limitation of the purposes for which such personal 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 subject to the principles set out in Article 4 of Directive (EU) 2016/680 of the European Parliament and of the Council and Article 5 of Regulation (EU) 2016/679. 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 dactyloscopic data, photographs and facial images for identification and verification purposes. Facial images and photographs for identification purposes should initially only be used in the context of regular border crossing points subject to a report by the Commission confirming the availability, readiness and reliability of the technology.

(18) 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[2]. The SIS dactyloscopic data search allows an active search of the perpetrator. Therefore, it should be possible to upload the dactyloscopic data of an unknown perpetrator into SIS, provided that the owner of the dactyloscopic data can be identified to a very high degree of probability as the perpetrator of a serious crime or act of terrorism. This is in particular the case if dactyloscopic data are found on the weapon or on any object used for the offence. The mere presence of the dactyloscopic data at the crime scene should not be considered as indicating a very high degree of probability that the dactyloscopic data are those of the perpetrator. A further precondition for the creation of such alert should be that the identity of the suspect cannot be established on the basis of data from any other relevant national, Union or international database. Should a dactyloscopic data search lead to a potential match the Member State should carry out further checks, together with the involvement of 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 to national law. Such identification could substantially contribute to the investigation and could lead to an arrest provided that all conditions for an arrest are met.

(19) Complete or incomplete sets of fingerprints or palm prints found at a crime scene should be allowed to be checked against the dactyloscopic data stored in SIS if it can be established to a high degree of probability that they belong to the perpetrator of the serious crime or terrorist offence provided that the search is carried out simultaneously in the relevant national fingerprints databases. Particular attention should be given to the establishement of quality standards applicable to the storage of biometric data, including latent dactyloscopic data.

---

[2] 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).

(20) It should be possible to add a DNA profile to an alert in clearly defined cases where dactyloscopic data are not available. This DNA profile 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 direct ascendants, descendants or siblings to enable identification. DNA data should contain only the minimum information necessary for the identification of the missing person.

(20a) Wherever the identity of the person cannot be ascertained by any other means, dactyloscopic data should be used to attempt to ascertain the identity. It should be allowed in all cases to identify a person by using dactyloscopic data.

(20b) DNA profiles should only be retrieved from SIS in case that an identification is necessary and proportionate for the purposes laid down in this Regulation. DNA profiles should not be retrieved and processed for any other purpose than those for which they were entered. The data protection and security rules laid down in this Regulation should apply. 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.

(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[3] should be processed in SIS. Due to operational reasons, it is appropriate for the issuing Member State to make an existing alert for arrest temporarily 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.

---

[3] 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).

(23) SIS should contain alerts on missing persons or on vulnerable persons who need to be prevented from travelling to ensure their protection or to prevent threats to public security or public order. In cases of children, these alerts and the corresponding procedures should serve the best interests of the child in accordance with Article 24 of the Charter of Fundamental Rights of the European Union and Article 3 of the United Nations Convention on the Rights of the Child of 20 November 1989. Actions and decisions by the competent authorities, including judicial authorities, following an alert on a child should be taken in cooperation with child protection authorities. The national hotline for missing children should be informed, where appropriate.

(23a) Alerts on missing persons who need to be placed under protection should be entered at the request of the competent authority. All children who have gone missing from Member States' reception facilities should be entered in SIS as missing persons.

(23b) Alerts on children at risk of parental child abduction should be entered in SIS at the request of competent authorities, including judicial authorities having jurisdiction in matters of parental responsibility in accordance with national law. Issuing an alert in SIS for children at risk of parental child abduction, where this risk is concrete and apparent, should be limited, therefore it is appropriate to provide for strict and appropriate safeguards. In assessing whether a concrete and apparent risk exists that a child may be unlawfully and imminently removed from a Member State, the competent authority should take into account the child's personal circumstances and the environment to which the child is exposed.

(23c) This Regulation should establish a new category of alerts for certain categories of vulnerable persons who need to be prevented from travelling. Persons who, due to their age, disabilities, or their family circumstances require protection should be considered vulnerable.

(23d) Alerts on children who need to be prevented from travelling for their own protection should be entered in SIS if there is a concrete and apparent risk of them being removed from or leaving the territory of a Member State. Such alerts should be entered if the travel would put them at risk of becoming victims of trafficking of human beings or of forced marriage, female genital mutilation or other forms of gender-based violence, or at risk of becoming victims or being involved in terrorist offences, or, at risk of being conscripted or enlisted into armed groups or of being made to participate actively in hostilities.

(23e) Alerts on vulnerable adults who need to be prevented from travelling for their own protection should be entered if travel would put them at risk of becoming victims of trafficking of human beings or gender-based violence.

(23f) In order to guarantee strict and appropriate safeguards the alerts on children or other vulnerable persons who need to be prevented from travelling should, where required under national law, be entered into SIS following a decision by a judicial authority or a decision by a competent authority confirmed by a judicial authority.

(24) A new action should be introduced for cases where, based on a clear indication, a person is suspected of intending to commit or of committing any of the offences referred to in Article 2(1) and (2) of Framework Decision 2002/584/JHA. A new action should also be included where the relevant information is necessary for the execution of a custodial sentence or detention order against a person convicted of any of the offences referred to in Article 2(1) and (2) of Framework Decision 2002/584/JHA, or where there is a reason to believe that he or she will commit any of those offences, to allow that person to be stopped and interviewed in order to supply the most detailed information to the issuing Member State. This action should be also without prejudice to existing mutual legal assistance mechanisms. It should supply sufficient information to decide about further actions. This new action to be carried out during a police or border check should not amount to searching the person nor to his or her arrest and the procedural rights of suspects and accused persons under Union and national law should be preserved, including their right to have access to a lawyer in accordance with Directive 2013/48/EU of the European Parliament and of the Council.

(24a) In case of alerts on objects for seizure or use as evidence in criminal proceedings, the objects should be seized in accordance with national law that determines if and in accordance with which conditions an object is seized, particularly 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 which can be identified and searched with a unique number.

(25a) As regards documents to be entered into SIS for seizure or use as evidence in criminal proceedings, the term "false" should be construed as encompassing both forged 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 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 the non execution of 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 specific purposes for which they were issued. The review periods for different alerts should be appropriate for the purpose of the corresponding alerts. Alerts on objects which are linked to an alert on a person should only be kept for as long as the alert on the person is kept. Decisions to retain alerts on persons should be based on a comprehensive individual assessment. Member States should review alerts on persons and objects within the review periods and keep statistics about the number of alerts 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. In cases of terrorist offences the case should be considered adequate, relevant and important enough to warrant the existence of an alert in SIS. For public or national security reasons Member States should be allowed exceptionally to refrain from creating an alert, when it is likely to obstruct official or legal inquiries, investigations or procedures.

(31) It is necessary to provide rules 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 the data processing should be bound by the security requirements of this Regulation, be appropriately trained, be subject to a uniform incident reporting procedure and be informed of any offences and penalties in this respect.

(32a) The European Data Protection Supervisor should be granted sufficient resources to fulfil the tasks entrusted to it under this Regulation, including assistance from persons with expertise on biometric data.

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

(34) It is appropriate to grant access to SIS to services 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. It is also appropriate to grant access to SIS to services 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.

(34a) Direct access to SIS should only be provided to competent government services. This access should be limited to alerts concerning the respective conveyances and their registration document or number plate or firearms and requesting persons. Any hit in SIS should be reported by the abovementioned government services 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) Without prejudice to more specific rules laid down in this Regulation, the national laws, regulations and administrative provisions adopted pursuant to Directive (EU) 2016/680 should apply to the processing, including collection and communication, of personal data by the competent authorities of Member States for the purposes of prevention, detection, investigation or prosecution of terrorist offences or other serious criminal offences or the execution of criminal penalties pursuant to this Regulation. Access to data entered into SIS and the right to search such data by national competent authorities which are responsible for the prevention, detection, investigation or prosecution of terrorist offences or other serious criminal offences or the execution of criminal penalties are to be subject to all the relevant provisions of this Regulation and those of Directive (EU) 2016/680 as transposed into national law, in particular the monitoring by the supervisory authorities established in accordance with Article 41(1) of Directive (EU) 2016/680.

(36) Without prejudice to more specific rules laid down in this Regulation for the processing of personal data, Regulation (EU) 2016/679 of the European Parliament and of the Council should apply to the processing of personal data by the Member States in application of this Regulation unless such processing is carried out by the competent authorities of the Member States for the purposes of the prevention, investigation, detection or prosecution of terrorist offences or of other serious criminal offences.

(36a) [Regulation (EU) No …./2018] should apply to the processing of personal data by the institutions and bodies of the Union when carrying out their responsibilities under this Regulation.

(36b) Regulation (EU) 2016/794 of the European Parliament and of the Council[4] should apply to the processing of personal data by Europol under this Regulation.

(37) deleted

[4] 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).

(38) In cases when searches carried out by national members of Eurojust and their assistants in SIS reveal the existence of an alert issued by a Member State, Eurojust should not be able to take the required action. Therefore it should inform the Member State concerned allowing it to follow up the case.

(38a) When using the SIS, the competent authorities should ensure that the human dignity and integrity of the person whose data are processed are respected. Processing of personal data for the purposes of this Regulation is not to result in discrimination against persons on any grounds such as sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation.

(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 established in accordance with Regulation (EU) 2016/679 and Directive (EU) 2016/680 (supervisory authorities) should monitor the lawfulness of the processing of personal data by the Member States in relation to this Regulation including the exchange of supplementary information, and should be granted sufficient resources to carry out this task. 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.

(42) The supervisory authorities should ensure that an audit of the data processing operations in their Member States' 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.

(42a) The European Data Protection Supervisor should monitor the activities of the Union institutions and bodies in relation to the processing of personal data under this Regulation. The European Data Protection Supervisor and the national supervisory authorities should cooperate with each other in the monitoring of SIS.

(42b) The European Data Protection Supervisor should be granted sufficient resources to fulfil the tasks entrusted to it under this Regulation, including assistance from persons with expertise on biometric data.

(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.

(44) 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 are encouraged to share information on terrorism-related activity with Europol. 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.

(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.

(46) Regulation (EU) 2016/1624 of the European Parliament and of the Council[5] provides for the purpose of this Regulation, that the host Member State is to authorise the members of the teams as defined in Article 2(8) of Regulation (EU) 2016/1624, 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.

[5] 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).

The objective of the deployment of the teams as defined in Article 2(8) and (9) of Regulation (EU) 2016/1624 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 teams as defined in Article 2(8) and (9) of Regulation (EU) 2016/1624 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 State 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.

(47) (deleted)

(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 rules related to biometric data, rules on compatibility and priority of alerts, links between alerts, setting the expiry date of alerts within the maximum time limit and the exchange of supplementary information. Implementing powers in respect of those aspects should therefore be conferred to the Commission. Technical rules on searching alerts should take into account the smooth operation of national applications.

(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 Regulation (EU) No 182/2011[6]. The procedure for adopting implementing measures under this Regulation and Regulation (EU) 2018/xxx (border checks) should be the same.

---

[6] 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 two years after the start of operations by the Agency. An overall evaluation should be issued by the Commission every four years.

(50a) In order to ensure the smooth functioning of SIS, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission in respect of:

- new sub-categories of objects to be sought under alerts on objects for seizure or use as evidence in criminal proceedings

- the determination of the circumstances in which photographs and facial images may be used for the identification of third-country nationals other than in the context of regular border crossing points.

It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(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 should fully respect the protection of personal data in accordance with Article 8 of the Charter of Fundamental Rights of the European Union while seeking 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 abduction. In cases concerning children, the best interests of the child should be a primary consideration.

(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 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.

(55) Ireland is taking part in this Regulation in accordance with Article 5 of 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.

(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[7], which fall within the area referred to in Article 1, point G of Council Decision 1999/437/EC[8]on certain arrangements for the application of that Agreement.

---

7 OJ L 176, 10.7.1999, p.36.

8 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 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 3 of Council Decision 2008/149/JHA[9].

(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[10], 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[11].

---

9 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).

10 OJ L 160, 18.6.2011, p. 21.

11 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).

(59) As regards Bulgaria, Romania and Croatia, this Regulation constitutes an act building upon, or otherwise relating to, the Schengen acquis within, respectively, the meaning of 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[12] 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.[13]

(60) Concerning Cyprus this Regulation constitutes an act building upon, or otherwise relating to, the Schengen acquis within the meaning of Article 3(2) of the 2003 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) (deleted)

(63) This Regulation introduces a series of improvements to SIS which will increase its effectiveness, strengthen data protection and extend access rights. Certain of these improvements do not require complex technical developments, while others do require technical changes of varying magnitude. In order to enable improvements to the system to become available to end-users as fast as possible, this Regulation introduces amendments to Council Decision 2007/533/JHA and Commission Decision 2010/261/EU in several phases. A number of improvements to the system should apply immediately upon entry into force of this Regulation, whereas others should apply either one or two years after its entry into force. This Regulation should apply in its entirety within three years after its entry into force. In order to avoid delays in its application the phased implementation of this Regulation should be closely monitored.

(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 3 May 2017,

---

12 OJ L 166, 1.7.2010, p. 17.
13 OJ L 108, 26.4.20017, p. 31.

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

General purpose of SIS

The purpose of SIS shall be to ensure a high level of security within the area of freedom, security and justice of the Union including the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States, and to ensure the application of the provisions of Chapter 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

Subject matter

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 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, recording, logging, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

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

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

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

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

(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

(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 and vulnerable persons and alerts for discreet, inquiry and specific checks;

(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 personal data resulting from specific technical processing relating to the physical or physiological characteristics of a natural person, which allow or confirm the unique identification of that natural person, i.e. photographs, facial images, dactyloscopic data and DNA profile;

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

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

(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);

(m) (deleted)

(n) 'terrorist offences' means offences under national law referred to in Articles 3 to 14 of Directive (EU) 2017/541[14], or equivalent to one of those offences for the Member States which are not bound by that Directive.

(o) 'threat to public health' means threat to public health as defined by Regulation (EU) 2016/399[15].

Article 4

Technical architecture and ways of operating SIS

1. SIS shall be composed of:

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

- a technical support function ('CS-SIS') containing a database, the 'SIS database',
- a uniform national interface (NI-SIS);

(b) a national system (N.SIS) in each of the Member States, consisting of the national data systems which communicate with Central SIS. An N.SIS may contain a data file (a 'national copy'), containing a complete or partial copy of the SIS database. Two or more Member States may establish in one of their N.SIS a shared copy which may be used jointly by 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 for 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

---

14 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.

15 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);

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

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

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

2. Member States shall enter, update, delete and search 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(3) (a) to (v) of this Regulation. It shall not be possible to search the data files of other Member States' N.SIS except in case of shared copies.

3. CS-SIS shall perform technical supervision and administration functions and have a backup CS-SIS, capable of ensuring all functionalities of the principal CS-SIS in the event of failure of 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 …/2018 new eu-LISA Regulation] ('the Agency').

3a. The Agency shall implement technical solutions to reinforce the uninterrupted availability of SIS either through the simultaneous operation of CS-SIS and the back-up CS-SIS, provided that the backup CS-SIS remains capable of ensuring the operation of SIS in the event of failure of CS-SIS, or through duplication of the system or its components. Notwithstanding the procedural requirements laid down in Article 6a of Regulation ... [new eu-LISA Regulation] the Agency shall no later than ... [one year after the entry into force of this Regulation, *OPOCE please insert date*], prepare a study on the options for technical solutions, containing an independent impact assessment and cost-benefit analysis.

3b. Where necessary in exceptional circumstances, the Agency may temporarily develop an additional copy of the CS-SIS database.

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

(a) provide online update of the national copies;

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

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

CS-SIS shall 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.

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

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 uninterrupted availability of SIS data to end-users.

Each Member State shall transmit its alerts via its N.SIS.

Article 7

N.SIS Office and SIRENE Bureau

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

   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.

   (deleted)

2. Each Member State shall designate a national authority which shall be operational 24 hours a day, 7 days a week and 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(4). The SIRENE Bureau shall serve as single contact point for Member States to exchange supplementary information regarding alerts and to facilitate the requested actions to be taken when alerts on persons or objects have been entered in SIS and those persons or objects are located following a hit.

   The SIRENE Bureau shall, in accordance with national law, have easy direct or indirect access to all relevant national information, including national databases and all information on its own alerts, and to expert advice to be able to react to requests for supplementary information swiftly and within the deadlines provided for 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 Office 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 referred to in paragraph 4 and using the Communication Infrastructure. Member States shall provide the necessary technical and human resources to ensure the continuous availability and timely and effective exchange of supplementary information. In the event that the Communication Infrastructure is unavailable, Member States shall use other adequately secured technical means to exchange supplementary information. A list of adequately secured technical means shall be laid down in the SIRENE Manual referred to in paragraph 4.

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 to a request for supplementary information as soon as possible but not later than 12 hours after the receipt of the request. In case of alerts for terrorist offences, of alerts for persons wanted for arrest for surrender or extradition purposes, and in cases of alerts concerning children referred to in Article 32(2)(c) the SIRENE Bureaux shall act immediately.

   Requests for supplementary Information with highest priority shall be marked 'URGENT', in the SIRENE forms, and the reason for urgency shall be specified.

4. The Commission shall adopt implementing acts to lay down detailed rules for the tasks of the SIRENE Bureaux pursuant to this Regulation and the exchange of supplementary information in the form of a manual entitled the 'SIRENE Manual'. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72(2).

Article 9

Technical and functional compliance

1. When setting up its N.SIS, each Member State shall comply with common standards, protocols and technical procedures established to ensure the compatibility of its N.-SIS with CS-SIS for the prompt and effective transmission of data.

2. If a Member State uses a national copy, it shall ensure, by means of the services provided by CS-SIS and by means of automatic updates referred to in Article 4(4) that the data stored in the national copy are identical to and consistent with the SIS database, and that a search in its national copy produces a result equivalent to that of a search in the SIS database.

2a. End-users shall receive the data required, to perform their tasks, in particular and where necessary, all the available data allowing for the identification of the data subject and the required action to be taken.

2b. Member States and the Agency shall undertake regular tests to verify the technical compliance of the national copies referred to in paragraph 2. The results of these tests shall be taken into consideration as part of the mechanism established by Regulation (EU) No 1053/2013.

3. 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, 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);

(ea) prevent the unauthorised processing of data in SIS and any unauthorised modification or erasure of data processed in SIS (control of data entry);

(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 identifiers and confidential access modes only (data access control);

(g) ensure that all authorities with a right of access to SIS or to the data processing facilities create profiles describing the functions and responsibilities of persons who are authorised to access, enter, update, delete and search the data and make these profiles available to the national supervisory authorities referred to in Article 67(1) without delay upon their request (personnel profiles);

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

(i) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems, when, by whom and for what purpose the data were input (input control);

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

(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);

(ka) ensure that the installed system may, in case of interruption, be restored (recovery); and

(kb) ensure that SIS performs its functions correctly, that faults are reported (reliability) and that personal data stored in SIS cannot be corrupted by means of the system malfunctioning (integrity).

2. Member States shall take measures equivalent to those referred to in paragraph 1 as regards security in respect of the processing and exchange of supplementary information, including 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 encompassing multiple IT-systems. However, the requirements foreseen in this Article and its applicability to the SIS shall be clearly identifiable in and ensured by that plan.

Article 11

Confidentiality – Member States

1. Each Member State shall apply its rules of professional secrecy or other equivalent duties of confidentiality to all persons and bodies required to work with SIS data and supplementary information, in accordance with its national law. That obligation shall also apply after those persons leave office or employment or after the termination of the activities of those bodies.

2. Where a Member State cooperates with external contractors in any SIS-related tasks, that Member State shall closely monitor the activities of the contractor to ensure compliance with all provisions of this Regulation, including in particular security, confidentiality and data protection.

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

Article 12

Keeping of logs at national level

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

2. The logs shall show, in particular, the history of the alert, the date and time of the data processing activity, the data used to perform a search, a reference to the data processed and the individual and unique user identifiers of both the competent authority and the person processing the data.

3. By way of derogation from paragraph 2, if the search is carried out with dactyloscopic data or facial image in accordance with Article 22 the logs shall show the type of data used to perform the search instead of the actual data.

4. The logs may be used only for the purpose referred to in paragraph 1 and shall be deleted three years after their creation. The logs which include the history of alerts shall be deleted three years after deletion of the alerts.

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

6. The competent national 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, in accordance with national law, 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. If necessary, a full search may be carried out in SIS in order to verify whether a hit has been achieved. The provisions of paragraphs 1 to 6 of this Article shall apply to any full search.

8. 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.

Article 14

Staff training

1. Before being authorised to process data stored in SIS and periodically after access to SIS data has been granted, the staff of the authorities having a right to access SIS shall receive appropriate training about data security, fundamental rights including data-protection rules and the procedures on data processing as set out in the SIRENE Manual referred to in Article 8(4). The staff shall be informed of any relevant criminal offences and penalties, including those laid down in accordance with Article 70a of this Regulation.

2. Member States shall have a national SIS training programme. This training programme shall include training for end-users as well as the staff of the SIRENE Bureaux.

   This training programme may be part of a generic training approach and programme at national level encompassing training in other relevant areas.

3. Common training courses shall be organised at EU level at least once a year to enhance cooperation between SIRENE Bureaux.

CHAPTER III

RESPONSIBILITIES OF THE AGENCY

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 technology, subject to 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;

   (ca) tasks relating to implementation of the budget;

   (cb) acquisition and renewal;

   (cc) contractual matters.

3. (deleted)

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, 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.

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

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

5a. The Agency shall also perform tasks related to providing training on the technical use of SIS and on measures to improve the quality of SIS data.

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 set out in Article 9 of this Regulation.

7. The Commission shall adopt an implementing act to set out the technical requirements of the Communication Infrastructure referred to in paragraph 2. This implementing act 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, including a security plan, a business continuity plan and a disaster recovery plan for Central SIS and the Communication Infrastructure in order to:

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

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

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

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

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

(ea) prevent the unauthorised processing of data in SIS and any unauthorised modification or erasure of data processed in SIS (control of data entry);

(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 identifiers and confidential access modes only (data access control);

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

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

(i) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems, when and by whom the data were input (input control);

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

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

(ka) ensure that the system installed may, in case of interruption, be restored (recovery);

(kb) ensure that SIS performs its functions correctly, that faults are reported (reliability) and that personal data stored in SIS cannot be corrupted by means of the system malfunctioning (integrity);

(kc) ensure the security of its technical sites.

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

Article 17

Confidentiality – Agency

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

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

2a. Where the Agency cooperates with external contractors in any SIS-related tasks, it shall closely monitor the activities of the contractor to ensure compliance with all provisions of this Regulation, including in particular security, confidentiality and data protection.

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

Article 18

Keeping of logs at central level

1. 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 alert, the date and time of the data processing activity, the data used to perform a search, a reference to the data processed and the individual and unique user identifiers of the competent authority processing the data.

3. By way of derogation from paragraph 2, if the search is carried out with dactyloscopic data or facial image in accordance with Article 22 the logs shall show the type of data used to perform the search instead of the actual data.

4. The logs may only be used for the purposes mentioned in paragraph 1 and shall be deleted three years after their creation. The logs which include the history of alerts shall be deleted three years after deletion of the alerts.

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

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

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

CHAPTER IV

INFORMATION TO THE PUBLIC

Article 19

SIS information campaigns

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

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, 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 26, 32, 34, 36 and 38.

3. Any alert in SIS which includes information on persons shall only contain the following data:

   (a) surnames;

   (b) forenames;

   (c) names at birth;

   (d) previously used names and aliases;

   (e) any specific, objective, physical characteristics not subject to change;

   (f) place of birth;

   (g) date of birth;

   (h) gender;

   (i) nationality / nationalities;

   (j) whether the person concerned:

      i. is armed;

      ii. is violent;

      iii. has absconded or escaped;

      iv. poses a risk of suicide;

      v. poses a threat to public health; or

vi. is involved in an activity as referred to in Articles 3 to 14 of Directive (EU) 2017/541;

(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 60;

(p) the type of offence;

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

(r) for alerts referred to in Article 32(2), a categorisation of the type of case;

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

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

(u) the number(s) of the person's identification documents;

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

(w) photographs and facial images;

(x) in accordance with Article 41A (1b), relevant DNA profiles;

(y) dactyloscopic data;

(z) copy of the identification documents, whenever possible in colour.

4. 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 paragraphs 2 and 3 and the common standards referred to in paragraph 5. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72(2).

5. 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 on common standards.

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 existence of an alert in SIS.

2. Where a person or an object is sought under an alert related to a terrorist offence, the case shall be considered adequate, relevant and important enough to warrant the existence of an alert in SIS. For public or national security reasons Member States may exceptionally refrain from creating an alert, when it is likely to obstruct official or legal inquiries, investigations or procedures.

Article 22

(moved to Article 41A)

Article 23

Requirement for an alert to be entered

1. The minimum set of data necessary in order to enter an alert in SIS shall be the data referred to in 20(3) (a), (g), (k) and (n) except for in the situations referred to in Article 40. The other data listed in that paragraph shall also be entered in SIS, if available.

2. (deleted)

2a. The data referred to in Article 20(3) shall only be entered when this is strictly necessary for the identification of the person concerned. When such data are inserted, Member States shall ensure the respect of the provisions of Article 10 of Directive (EU) 2016/680.

Article 23a

Compatibility of alerts

1. Before issuing an alert, the Member State shall check whether the person or the object is already the subject of an alert in SIS. To check whether the person is already subject of an alert, a check with dactyloscopic data shall also be carried out if such data are available.

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

3. Where a person or an object is already the subject of an alert in SIS, a Member State wishing to enter a new alert shall check that there is no incompatibility between the alerts. If there is no incompatibility, the Member State may enter the new alert. If the alerts are incompatible, the SIRENE Bureaux concerned shall consult each other by exchanging supplementary information in order to reach an agreement. Rules on the compatibility of alerts shall be laid down in the SIRENE Manual referred to in Article 8(4). Departures from the compatibility rules may be made after consultation between the Member States if essential national interests are at stake.

4. In case of simultaneous hits on multiple alerts on the same person or object the executing Member State shall observe the priority rules of alerts as laid down in the SIRENE Manual referred to in Article 8(4).

   In case a person is subject to multiple alerts issued by different Member States alerts for arrest issued pursuant to Article 26 shall be executed as a priority subject to Article 25.

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 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 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 or Article 216 of the Treaty on the Functioning of 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 of the Treaty on the European Union or Article 216 of the Treaty on the Functioning of 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. In the case of an ongoing operation, the issuing Member State may temporarily make an existing alert for arrest issued under this Article unavailable for searching by the end-users in the Member States involved in the operation. In that case the alert shall only be accessible to the SIRENE Bureaux. Member States shall only do so if :

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

   (b) a prior authorisation has 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.

   The functionality provided for in the first subparagraph shall only be used for a period not exceeding 48 hours. However, if operationally necessary, 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 objects referred to in Article 38(2)(a), (b), (c), (e), (g), (h), (i) and (j) are connected with a person who is the subject of an alert pursuant to paragraph 1 and 2 of this Article, 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.

6. The Commission shall adopt implementing acts to lay down and develop rules necessary for entering, updating, deleting and searching the data referred to in paragraph 5. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72(2).

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.

   A Member State shall be able to enter the copy of one or more European Arrest Warrant to an alert for arrest.

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 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 PERSONS OR VULNERABLE PERSONS WHO NEED TO BE PREVENTED FROM TRAVELLING

Article 32

Objectives and conditions for issuing alerts

1. (deleted)

2. Alerts on the following categories of persons shall be entered in SIS at the request of the 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 a threat to public order or public security;

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

   (c) children at risk of abduction by a parent, a family member or a guardian, in accordance with paragraph 4, who need to be prevented from travelling;

   (ca) children who need to be prevented from travelling in respect of whom there is a concrete and apparent risk of them being removed from or leaving the territory of a Member State and

      (i) becoming victims of trafficking in human beings or victims of forced marriage and or female genital mutilation or other forms of gender-based violence, or

      (ii) becoming victims of or involved in terrorist offences, or

      (iii) becoming conscripted or enlisted into armed groups or being made to participate actively in hostilities;

   (cb) vulnerable persons who are of age who need to be prevented from travelling for their own protection in respect of whom there is a concrete and apparent risk of them being removed from or leaving the territory of a Member State and becoming victims of trafficking in human beings or gender-based violence.

3. Point (a) of paragraph 2 shall apply in particular to children and to persons who have to be institutionalised following a decision by a competent authority.

4. An alert on a child referred to in paragraph 2(c) shall be entered following a decision by the competent authorities, including judicial authorities of the Member States having jurisdiction in matters of parental responsibility, where a concrete and apparent risk exists that the child may be unlawfully and imminently removed from the Member State where the competent authorities are situated.

4a. An alert on persons referred to in paragraph 2(ca) and (cb) shall be entered following a decision by the competent authorities, including judicial authorities.

4b. The issuing Member State shall regularly review the need to maintain the alerts referred to in paragraph 2(c), (ca) and (cb) in accordance with Article 51(3).

5. Member States shall ensure that the data entered in SIS indicate which of the categories referred to in paragraph 2 the person falls into. Member States shall also ensure that the data entered in SIS indicate which type of case is involved, wherever the type of case is known, and that, in relation to alerts issued pursuant to points (c), (ca) and (cb) of paragraph 2, all relevant information is made available at the SIRENE Bureau of the issuing Member State at the time of the alert's creation.

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, 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 the objects referred to in Article 38(2)(a), (b), (c), (e), (g), (h), and (j) are connected with a person who is the subject of an alert pursuant to paragraph 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.

8. 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. The types of cases of missing persons who are children shall include, but not be limited to, runaways, unaccompanied children in the context of migration and children at risk of parental abduction.

The Commission shall also adopt implementing acts to lay down and develop 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).

Article 33

Execution of action based on an alert

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

1a. In the case of persons who need to be placed under protection as referred to in Article 32(2)(a), (c), (ca) and (cb), the executing Member State shall immediately consult its own competent authorities and those of the issuing Member State through the exchange of supplementary information in order to agree without delay on the measures to be taken. The competent authorities in the executing Member State may, in accordance with national law, move such persons to a safe place in order to prevent them from continuing their journey.

1b. In the case of children any decision on the measures to be taken or any decision to move the child to a safe place as referred to in paragraph 1a shall be made in accordance with the best interests of the child. Such decisions shall be made immediately and not later than 12 hours of when the child is located in consultation with relevant child protection authorities, as appropriate.

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.

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 the objects referred to in Article 38(2)(a), (b), (c), (e), (g), (h), and (j) are connected with a person subject of an alert pursuant to paragraph 1, alerts on those objects 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.

3. 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

Objectives and conditions for issuing alerts

1. Data on persons, on the objects referred to in Article 38(2)(a), (b), (c), (e), (g), (h), (i), (j), (k) and on 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)(a) to (h), the issuing Member State shall add to the alert all information being sought. If that information relates to special categories of personal data referred to in Article 10 of Directive (EU) 2016/680, it may only be sought if it is strictly necessary for the specific purpose of the alert, and for the criminal offence for which the alert has been issued.

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 any of the offences referred to in Article 2(1) and (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 custodial sentence or detention order regarding a person convicted of any of the offences referred to in Article 2(1) and (2) of the Framework Decision 2002/584/JHA; 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 in the future the offences referred to in Article 2(1) and 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), (i), (j), (k) or non-cash means of payment are connected with the serious crimes referred to in paragraph 2 or the serious threats referred to in paragraph 3, alerts on those objects may be issued and linked to the alerts entered pursuant to paragraphs 2 and 3.

5. (deleted)

6. The Commission shall adopt implementing acts to lay down and develop the technical rules necessary for entering, updating, deleting and searching the data referred to in paragraph 4 as well as the additional information referred to in paragraph 1a. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72(2).

Article 37

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 issuing Member State:

   (a) the fact that the person who is the subject of an alert has been located, or that objects referred to in Article 38(2)(a), (b), (c), (e), (g), (h), (i), (j), (k) or non-cash means of payment which are the subject of an alert have been located;

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

   (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) the objects referred to in Article 38(2)(a), (b), (c), (e), (g), (h), (i), (j), (k) or non-cash means of payment used;

(g) objects carried, including travel documents;

(h) the circumstances under which the person or the objects referred to in Article 38(2)(a), (b), (c), (e), (g), (h), (i), (j), (k) or non-cash means of payment was located;

(i) any other information being sought by the issuing Member State in accordance with Article 36(1a).

If the information referred to in point (i) of the first subparagraph of this paragraph relates to special categories of personal data referred to in Article 10 of Directive (EU) 2016/680, it shall be processed in accordance with the conditions set out in that Article and only if it supplements other personal data processed for the same purpose.

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

3. 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 of the existence of the alert.

4. An inquiry check shall comprise the interviewing of the person, 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[16].

5. During specific checks, persons, vehicles, boats, aircraft, containers and objects carried, may be searched for the purposes referred to in Article 36. Searches shall be carried out in accordance with national law.

---

16 Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty (OJ L 294, 6.11.2013, p. 1).

6. Where specific checks are not authorised by national law, they shall be replaced by inquiry checks in that Member State. Where inquiry checks are not authorised by national law, they shall be replaced by discreet checks in that Member State. Where Directive 2013/48 applies , Member States shall ensure that the right of suspects and accused persons to have access to a lawyer is respected under the conditions set out in that Directive.

7. Paragraph 6 is without prejudice to the obligation of Member States to make available to the end-users the information sought under Article 36(1a).

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 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 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, lost or purport to be such a document but are false;

(k) issued identity documents - such as passports, identity cards, residence permits, travel documents and driving licences which have been stolen, misappropriated, lost or, invalidated or purport to be such a document but are false;

(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 false;

(m) banknotes (registered notes) and false banknotes;

(n) information technology items;

(o) identifiable component parts of motor vehicles;

(p) identifiable component parts of industrial equipment;

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

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

3. The Commission shall be empowered to adopt a delegated act in accordance with Article 71a to amend this Regulation by defining new sub-categories of objects under paragraph 2(n), (o), (p) and (q).

4. 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).

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.

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.

CHAPTER XI

ALERTS ON UNKNOWN WANTED PERSONS FOR IDENTIFICATION UNDER NATIONAL LAW

Article 40

Alerts on unknown wanted person for identification under national law

Dactyloscopic data which is unrelated to persons who are the subject of alerts may be entered into SIS. These dactyloscopic data shall be either complete or incomplete sets of fingerprints or palm prints discovered at the scenes of terrorist offences or other serious crimes under investigation. They shall only be entered into SIS where it can be established to a very high degree of probability that they belong to a perpetrator of the offence.

If the competent authority of the issuing Member State cannot establish the identity of the suspect on the basis of data from any other relevant national, Union or international database, the dactyloscopic data referred to in the first subparagraph may only be stored in this category of alerts as "unknown wanted person" for the purpose of identifying such a person.

Article 41

Execution of the action based on an alert

In the event of a hit 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 dactyloscopic data stored in SIS belong to the person. Member States shall communicate information about the identity and the whereabouts of the person through the exchange of supplementary information in order to facilitate timely investigation of the case.

CHAPTER XIa

SPECIFIC RULES FOR BIOMETRIC DATA

Article 41A (ex-Article 22)

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

1. Only photographs, facial images, dactyloscopic data referred to in Article 20(3)(w) and (y) which fulfil minimum data quality standards and technical specifications shall be entered into SIS. Before such data are entered, a quality check shall be performed in order to ascertain whether the minimum data quality standards and technical specifications have been met.

1a. Dactyloscopic data entered in SIS may consist of one to ten flat fingerprints and one to ten rolled fingerprints. It may also include up to two palm prints.

1b. A DNA profile may only be added to alerts in the situations provided for in Article 32(2)(a) only following a quality check to ascertain whether the minimum data quality standards and technical specifications have been met and only where photographs, facial images or dactyloscopic data are not available or not suitable for identification. 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 explicit consent. Where a DNA profile is added to an alert, that profile shall contain the minimum information strictly necessary for the identification of the missing person.

2. Quality standards and technical specifications shall be established for the storage of the biometric data referred to in paragraphs 1 and 1(b). These quality standards and technical specifications shall set the level of quality required for using the data to verify the identity of the person in accordance with Article 42 (1) and for using the data to identify the person in accordance with Article 42(2)-(4).

2a. The Commission shall adopt implementing acts to lay down the quality standards and technical specifications referred to in paragraphs 1, 1b and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72(2).

Article 42

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

1. Where photographs, facial images, dactyloscopic data and DNA profiles are available in an alert in SIS, such data shall be used to confirm the identity of a person who has been located as a result of an alphanumeric search made in SIS.

2. If the identity of the person cannot be ascertained by other means, dactyloscopic data shall be searched for identification purposes. Dactyloscopic data may be searched in all cases to identify a person. For this purpose the Central SIS shall contain an Automated Fingerprint Identification System (AFIS).

3. Dactyloscopic data stored in SIS in relation to alerts issued under Articles 26, 32, 36 and 40 may also be searched with complete or incomplete sets of fingerprints or palm prints discovered at the scenes of serious crimes or terrorist offences under investigation, and where it can be established to a high degree of probability that they belong to a perpetrator of the offence provided that the search is carried out simultaneously in their relevant national fingerprints databases.

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 in the context of regular border crossing points.

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

   After the start of the use of the functionality at regular border crossing points, the Commission is empowered to adopt delegated acts in accordance with Article 71a to supplement this Regulation concerning the determination of other circumstances in which photographs and facial images may be used for the identification of persons.

CHAPTER XII

RIGHT TO ACCESS AND REVIEW OF ALERTS

Article 43

Authorities having a right to access alerts

1. National competent authorities shall have access to data entered in SIS and the right to search such data directly or in a copy of SIS data 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) the prevention, detection, investigation or prosecution of terrorist offences or other serious criminal offences or the execution of criminal penalties, within the Member State concerned, provided that Directive (EU) 2016/680 applies;

   (d) examining the conditions and taking decisions related to the entry and stay of third-country nationals on the territory of the Member States, including on residence permits**,** and long-stay visas, and to the return of third-country nationals, as well as checks on third country nationals who are illegally entering or staying in the territory of the Member States;

   (da) security checks on third-country nationals who apply for international protection, insofar as those authorities do not constitute "determining authorities" as defined in Article 2(f) of Directive 2013/32/EU[17] of the European Parliament and of the Council, and where relevant providing advice in accordance with Council Regulation(EU) 377/2004[18].

---

[17] Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection (OJ L 180, 29.6.2013, p. 60).

[18] Council Regulation (EC) No 377/2004 of 19 February 2004 on the creation of an immigration liaison officers network (OJ L 64, 2.3.2004, p. 1.)

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, as provided for in national law, for the purposes of examining an application for naturalisation.

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 authorities referred to in this Article shall be included in the list referred to in Article 53(8).

Article 44

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[19], shall have access to data entered into SIS in accordance with Article 38(2)(a), (b), (c), (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.

(a) (deleted)

(b) (deleted)

(c) (deleted)

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.

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

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 obtained by access to SIS 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, including aircraft engines 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;

   (d) data on aircraft engines.

   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 (d) 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 obtained by access to SIS e shall be governed by national law.

Article 45A

Registration authorities for firearms

1. The services in the Member States responsible for issuing registration certificates for firearms shall have access to alerts on persons entered into SIS in accordance with Article 26 and 36 of this Regulation and to alerts on firearms entered into SIS in accordance with Article 38(2) of this Regulation. This access shall be exercised for the purpose of checking whether the person requesting registration is wanted for arrest for surrender or extradition purposes or for the purposes of discreet, inquiry or specific checks or whether firearms presented 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. 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 government services shall 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 only have access to data entered in SIS through the intermediary of an authority referred to in Article 43 of this Regulation. That 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 to 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 obtained by access to SIS shall be governed by national law.

Article 46

Access to SIS data by Europol

1. The European Union Agency for Law Enforcement Cooperation (Europol) shall, where necessary to fulfil its mandate, have the right to access and search data entered into SIS and may exchange and further request supplementary information in accordance with the provisions of the SIRENE Manual laid down in Article 8.

2. Where a search by Europol reveals the existence of an alert in SIS, Europol shall inform the issuing Member State through the exchange of supplementary information by means of the communication infrastructure and in accordance with the provisions set out in the SIRENE Manual. Until Europol is able to use the functionalities intended for the exchange of supplementary information, it shall inform issuing Member States 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 comparing with its databases and operational analysis projects, aimed at identifying connections or other relevant links and for strategic, thematic or operational analyses as defined in points (a), (b) and (c) of Article 18(2) of Regulation (EU) 2016/794. Any processing by Europol of supplementary information for the purpose of this article shall be carried out in accordance with Regulation (EU) 2016/794.

3. The use of information obtained from a search in ~~the~~ SIS or from the processing of supplementary information is subject to the consent of the issuing Member State. If the Member State allows the use of such information, the handling thereof by Europol shall be governed by Regulation (EU) 2016/794. Europol may only communicate such information to third countries and third bodies with the consent of the issuing Member State and in full respect of Union law on data protection.

4. (deleted)

5. Europol shall:

(a) without prejudice to paragraphs 3 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. By way of derogation, where Europol has information in its databases or operational analysis projects on a case to which the supplementary information is related, in order for Europol to perform its tasks, Europol may exceptionally continue to store the supplementary information when necessary. Europol shall inform the issuing and the executing Member State of the continued storage of such supplementary information and present a justification of such continued storage;

(b) limit access to data entered in SIS, including supplementary information to specifically authorised staff of Europol requiring access for the performance of their tasks;

(c) adopt and apply measures to ensure security, confidentiality and self-monitoring in accordance with Articles 10, 11 and 13;

(ca) ensure that its staff authorized to process SIS data receives appropriate training and information in accordance with Article 14(1); and

(d) without prejudice to Regulation (EU) 2016/794, allow the European Data Protection Supervisor to monitor and review the activities of Europol in the exercise of its right to access and search data 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. (deleted)

8. (deleted)

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

9a. Member States shall inform Europol through the exchange of supplementary information of any hit on alerts related to terrorist offences. Member States may exceptionally refrain from informing Europol if doing so would jeopardise current investigations, the safety of an individual or be contrary to essential interests of the security of the issuing Member State.

9b. Paragraph (9a) shall apply from the date when Europol is able to receive supplementary information in accordance with paragraph 1.

Article 47

Access to SIS data by Eurojust

1. Only the national members of Eurojust and their assistants shall, where necessary to fulfil 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. This Article is without prejudice to the provisions of Regulation (EU) 2018/XXX [new Eurojust Regulation] and Regulation (EU) 2018/XXX [new data protection Regulation for Union institutions and bodies] concerning data protection and the liability for any unauthorised or incorrect processing of such data by national members of Eurojust or their assistants, and to the powers of the European Data Protection Supervisor pursuant to those Regulations.

4. For the purpose of verifying the lawfulness of data processing, self-monitoring and ensuring proper data security and integrity, Eurojust shall keep logs of every access to and search in SIS made by a national member of Eurojust or an assistant in accordance with the provisions of Article 12.

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. (deleted)

7. Eurojust shall adopt and apply measures to ensure security and confidentiality in accordance with Articles 10 and 11 shall be adopted and applied.

Article 48

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

1. In accordance with Article 40(8) of Regulation (EU) 2016/1624, the members of the teams as defined in Article 2(8) and (9) of Regulation (EU) 2016/1624 shall, within their mandate and provided that they are authorised to carry out checks in accordance with Article 43(1) and have received the required training in accordance with Article 14(1), have the right to access and search data entered in SIS in so far it is necessary for the performance of their task and as required by the operational plan for a specific operation. Access to data entered in SIS shall not be extended to any other team members.

2. Members of the teams referred to in paragraph 1 shall exercise the right to access and search data entered in SIS in accordance with paragraph 1 via a technical interface which is set up and maintained by the European Border and Coast Guard Agency and which allows a direct connection to Central SIS.

3. Where a search by a member of the teams referred to in paragraph 1 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. For the purpose of verifying the lawfulness of data processing, self-monitoring and ensuring proper data security and integrity the European Border and Coast Guard Agency shall keep logs of every access to and search in SIS in accordance with the provisions of Article 12.

5. (deleted)

6. The European Border and Coast Guard Agency shall adopt and apply measures to ensure security, confidentiality and self-monitoring in accordance with Articles 10, 11 and. 13 and shall ensure that the teams referred to in paragraph 1, apply those measures.

7. 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.

8. Without prejudice to paragraph 2 no parts of SIS shall be connected to any computer system for data collection and processing operated by the teams referred to in paragraph 1 of this Article or by the European Border and Coast Guard Agency, nor shall the data contained in SIS to which those teams have access be transferred to such a system. No part of SIS shall be downloaded. The logging of access and searches shall not be construed to be the downloading or copying of SIS data.

9. Without prejudice to the further provisions of [new Regulation 45/2001], the European Border and Coast Guard Agency shall allow the European Data Protection Supervisor to monitor and review the activities of the teams as referred to in this Article in the exercise of their right to access and search data entered in SIS.

Article 49A

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, the national members of Eurojust and their assistants and the teams referred to in Article 48(1) at least every five years.

2. Europol, Eurojust and the EBCG Agency shall ensure adequate follow-up to the findings and recommendations stemming from this evaluation.

3. A report on the results and follow-up of the evaluation shall be sent to the European Parliament and to the Council.

Article 50

Scope of access

End-users, including Europol, the national members of Eurojust and their assistants and the members of the teams as defined in Article 2(8) and (9) of Regulation (EU) 2016/1624, may only access data which they require for the performance of their tasks.

Article 51

Review period for alerts on persons

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. A Member State may issue an alert on a person for the purposes of Article 26 and Article 32 (2)(a) and (b) of this Regulation for a period of five years. The issuing Member State shall, within those five years review the need to maintain the alert.

2a. A Member State may issue an alert on a person for the purposes of Articles 34 and 40 for a period of three years. The issuing Member State shall, within those three years, review the need to maintain the alert.

3. (deleted)

3a. A Member State may issue an alert on a person for the purposes of Article 32 (2)(c), (ca) and (cb) and Article 36 for a period of one year. The issuing Member State shall, within one year, review the need to maintain the alert.

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

5. Within the review period referred to in paragraphs 2, 2a and 3, the issuing Member State may, following a comprehensive individual assessment, which shall be recorded, decide to keep the alert on a person longer, where this proves necessary and proportionate for the purposes for which the alert was issued. In such a case paragraph 2, paragraph 2a or paragraph 3a shall apply, also to the extension. Any such decision to retain an alert shall be communicated to CS-SIS.

6. Alerts on persons shall automatically be deleted after the review period referred to in paragraphs 2, 2a and 3a, except where the issuing Member has informed CS-SIS about the decision to retain the alerts pursuant to paragraph 5. CS-SIS shall automatically inform the Member States of the scheduled deletion of data from the system four months in advance.

7. Member States shall keep statistics about the number of alerts on persons which have been extended in accordance with paragraph 5 after the expiry of the initial review period and transmit them, upon request, to the supervisory authorities referred to in Article 67.

8. As soon as 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 immediately notify the authority which created the alert. The authority shall have fifteen calendar days from the receipt of that notification to indicate that the alert has been or shall be deleted or shall state reasons for the retention of the alert. If the fifteen-day period expires without such a reply, the SIRENE Bureau shall ensure that the alert is deleted. Where permissible under national law 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.

Article 51A

Review period for alerts on 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. A Member State may issue an alert on objects for the purposes of Articles 36 and 38 for a period of ten years. The issuing Member State shall, within those ten years, review the need to maintain the alert.

2a. Alerts on objects issued in accordance with Articles 26, 32, 34, and 36, where such an alert is linked to an alert on a person, shall be reviewed pursuant to Article 51 and shall only be kept for as long as the alert on the person is kept.

2b. Within the period referred to in paragraph 2 and 2a, the issuing Member State may decide to retain the alert on an object longer, where this proves necessary for the purposes for which the alert was issued. In such a case paragraph 2 or 2a shall apply, as appropriate.

2c. Shorter review periods for certain categories of alerts on objects 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 which were retained in accordance with paragraph 2b after the expiry of the initial review period.

CHAPTER XIII

DELETION OF ALERTS

Article 52

Deletion of alerts

1. Alerts for arrest for surrender or extradition purposes pursuant to Article 26 shall be deleted when the person has been surrendered or extradited to the competent authorities of the issuing Member State. They shall also be deleted when 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 or vulnerable persons who need to be prevented from travelling pursuant to Article 32 shall be deleted in accordance with the following rules:

(a) Concerning missing children and children at risk of abduction, an alert shall be deleted upon:

– the resolution of the case, such as when the child has been located or 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; or

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

– (deleted)

(b) Concerning missing adults, 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 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 are of age who need to be prevented from travelling for their own protection and children who need to be prevented from travelling an alert shall be deleted upon:

– the carrying out of the action to be taken such as the person's placement under protection;

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

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

Without prejudice to the national law, where a person has been institutionalised following a decision by a competent authority an alert may be maintained until that person has been repatriated.

3. (deleted)

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 the executing Member State reveals the same address details, the hit shall be 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 carry out a comprehensive individual assessment of the need to maintain the alert.

4. (deleted)

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; or

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

5. (deleted)

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 upon:

(a) the identification of the person; or

(b) the expiry of the alert;

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

7. Alerts for objects issued in accordance with Articles 26, 32, 34, and 36 where such an alert is linked to an alert on a person, shall be deleted when the alert on the person is deleted in accordance with paragraph 1, 2 and 3 of this Article.

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.

Member States shall keep an up-to-date inventory of those copies, make that inventory available to their national supervisory authority, and ensure that the provisions of this Regulation, in particular those of Article 10, are applied in respect of those copies.

4. (deleted)

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. 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 issuing Member State 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 and subject to penalties in accordance with Article 70a of this Regulation.

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. The Agency shall maintain a continuously updated list on its website containing changes sent by Member States between the annual publications.

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.

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 via the exchange of supplementary information.

Article 56

Quality of the data processed in SIS

1. An issuing Member State shall be responsible for ensuring that the data are accurate, up-to-date and entered in SIS lawfully.

1a. Where an issuing Member State receives relevant additional or modified data as listed in Article 20(3), that Member State shall complete or modify the alert without delay.

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

2a. Where a Member State other than the issuing Member State has relevant additional or modified data as listed in Article 20(3), it shall transmit them without delay, through the exchange of supplementary information, to the issuing Member State to enable the latter to complete or modify the alert. If the additional or modified data relate to persons they shall only be transmitted if the identity of the person is ascertained.

3. Where a Member State other than the issuing Member State has evidence suggesting that an item of data is factually incorrect or has been unlawfully stored, it shall, through the exchange of supplementary information, inform the issuing Member State at the earliest opportunity and not later than two working 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 national supervisory authorities concerned and to the European Data Protection Supervisor for a decision by means of cooperation in accordance with Article 69.

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 and of his or her right to redress in accordance with Article 66(1).

6. (deleted)

Article 57

Security incidents

1. Any event that has or may have an impact on the security of SIS or may cause damage or loss to SIS data or to the supplementary information shall be considered to be a security incident, especially where unlawful access to data may have occurred or where the availability, integrity and confidentiality of data has or may have been compromised.

2. Security incidents shall be managed to ensure a quick, effective and proper response.

3. Without prejudice to the notification and communication of a personal data breach pursuant to Article 33 of Regulation (EU) No 2016/679 or to Article 30 of Directive (EU) No 2016/680, Member States, Europol, Eurojust and the European Border and Coast Guard Agency shall notify the Commission, the Agency, the national supervisory authority and the European Data Protection Supervisor without delay of security incidents. The Agency shall notify the Commission and the European Data Protection Supervisor without delay of any security incidents concerning the CS-SIS.

4. Information regarding a security incident that has or may have an impact on the operation of SIS in a Member State or within the Agency or on the availability, integrity and confidentiality of the data entered or sent by other Member States or on supplementary information exchanged, shall be provided to all the Member States without delay and reported in compliance with the incident management plan provided by the Agency.

4a. The Member States and the Agency shall collaborate in the event of a security incident.

4b. The Commission shall report serious incidents immediately to the European Parliament and the Council. These reports shall be classified as EU RESTRICTED/RESTREINT UE in accordance with applicable security rules.

4c. Where a security incident is caused by the misuse of data, Member States, Europol, Eurojust and the European Border and Coast Guard Agency shall ensure that penalties or disciplinary measures are imposed in accordance with Article 70a.

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, within 12 hours, the issuing Member State via the exchange of supplementary information 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 23a. 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. Any person whose identity has been misused has the right to withdraw his or her consent to the information being processed.

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, and subject to the explicit consent of the person whose identity was misused for each data category, only the following personal data of the person whose identity has been misused may be entered and further processed in SIS:

(a) surnames;

(b) forenames;

(c) names at birth;

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

(e) any specific objective and physical characteristic not subject to change;

(f) place of birth;

(g) date of birth;

(h) gender;

(i) photographs and facial images;

(j) fingerprints, palm prints or both

(k) nationality/nationalities;

(l) the category of the person's identification documents;

(m) the country of issue of the person's identification documents;

(n) the number(s) of the person's identification documents;

(o) the date of issue of a person's identification documents;

(p) address of the person;

(q) person's father's name;

(r) person's mother's name.

4. The Commission shall adopt implementing acts to lay down and develop technical rules necessary for entering and further processing the data referred to in paragraph 3. Those implementing acts shall be adopted 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 review period of each of the linked alerts.

3. The creation of a link shall not affect the rights of access provided for in this Regulation. Authorities with no right of access to certain categories of alerts shall not be able to see the link to an alert to which they do not have access.

4. A Member State shall create a link between alerts when there is an operational need.

5. Where a Member State considers that the creation by another Member State of a link between alerts is incompatible with its national law or 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 exchanged 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

(deleted)

CHAPTER XV

DATA PROTECTION

Article 64

Applicable legislation

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

2. Directive (EU) 2016/680 shall apply to the processing of personal data by competent national authorities referred to in Article 43 for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

3. Regulation (EU) 2016/679 shall apply to the processing of personal data by the competent authorities referred to in Article 43 of this Regulation with the exception of processing for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Article 65

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

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

2. (deleted)

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

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

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

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

   (c) protect public security;

   (d) protect national security; or

   (e) protect the rights and freedoms of others.

   In such cases, the Member State shall inform the data subject in writing, without undue delay, of any refusal or restriction of access and of the reasons for the refusal or restriction. Such information may be omitted where its provision would undermine a purpose under this paragraph. The Member State shall inform the data subject of the possibility of lodging a complaint with a supervisory authority or of seeking a judicial remedy.

   The Member State shall document the factual or legal reasons on which the decision is based. That information shall be made available to the supervisory authorities.

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

5. (deleted)

6. Following an application for access, rectification or erasure, the data subject shall be informed as soon as possible and in any event within the deadlines referred to in Article 12(3) of Regulation (EU) 2016/679 as to the follow-up given to the exercise of these rights.

Article 66

Remedies

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

2. The Member States undertake mutually to enforce final decisions handed down by the courts or authorities referred to in paragraph 1 of this Article, without prejudice to the provisions of Article 70.

3. Member States shall report annually on:

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

   (b) the number of access requests submitted to the 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) the number of court proceedings launched;

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

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

A template for the reporting referred to in the first subparagraph shall be developed by the Commission. The reports from the Member States shall be forwarded to the European Data Protection Board established by Regulation (EU) 2016/679 and included in the joint report referred to in Article 69(4).

Article 67

Supervision of N.SIS

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

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

Article 68

Supervision of the Agency

1. The European Data Protection Supervisor shall be responsible for monitoring the personal data processing activities of the Agency and for ensuring that those activities are carried out in accordance with this Regulation. The tasks and powers referred to in Articles 58[20] and 59[21] of Regulation (EC) 2018/XXX [new data protection Regulation for Union institutions and bodies] shall apply accordingly.

---

[20] This number is not the definitive one [*LL: please remove this footnote.*]

[21] This number is not the definitive one [*LL: please remove this footnote.*]

2. The European Data Protection Supervisor shall carry out an audit of the Agency's personal data processing activities 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 annually by the Board established by Regulation (EU) 2016/679 to the European Parliament, the Council, and the Commission.

CHAPTER XVI

LIABILITY AND PENALTIES

Article 70

Liability

1. Without prejudice to the right to compensation from, and liability under Regulation (EU) 2016/679, Directive (EU) 2016/680 and [new Regulation (EC) No 45/2001]:

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

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

   That Member State or the Agency shall be exempted from their liability, in whole or in part, if they prove that they are not responsible for the event which gave rise to the damage.

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

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

Article 70A

Penalties

Member States shall ensure that any misuse or processing of data stored in SIS or any exchange of supplementary information contrary to this Regulation is punishable in accordance with national law. The penalties provided shall be effective, proportionate and dissuasive.

CHAPTER XVII

FINAL PROVISIONS

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 annual reports on the number of hits per category of alert, how many times SIS was searched and how many times SIS was accessed for the purpose of entering, updating or deleting an alert, in total and for each Member State. The statistics produced shall not contain any personal data. The annual statistical report shall be published.

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.

4a. This information shall include separate statistics on the number of searches carried out by, or on behalf of, 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; and aircraft, including aircraft engines; and firearms. The statistics shall also show the number of hits per category of alert.

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

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

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

6. For the purpose of paragraphs 3, 4 and 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 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. Upon request, the Agency shall give access to Member States and the Commission, as well as, Europol, Eurojust and the European Border and Coast Guard Agency, to the extent required for the performance of their tasks, 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.

7. Two years after the start of operations of SIS pursuant to this Regulation and every two years thereafter, the Agency shall submit to the European Parliament and the Council a report on the technical functioning of Central SIS and the Communication Infrastructure, including the security thereof, on the automated fingerprint identification system and the bilateral and multilateral exchange of supplementary information between Member States. This report shall also contain, once the technology is in use, an evaluation of the use of facial images to identify persons.

8. Three years after the start of operations of SIS pursuant to this Regulation and every four years thereafter, the Commission shall produce an overall evaluation of Central SIS and the bilateral and multilateral exchange of supplementary information between Member States. That overall evaluation shall include an examination of results achieved against objectives, and an assessment of the continuing validity of the underlying rationale, the application of this Regulation in respect of Central SIS, the security of Central SIS and any implications for future operations. The overall evaluation report shall also include an assessment of the automated fingerprint identification system and SIS information campaigns organised by the Commission in accordance with Article 19. The Commission shall transmit the evaluation to the European Parliament and the Council.

9. The Commission shall adopt implementing acts to lay down detailed rules on the operation of the central repository referred to in paragraph 6 and the data protection and security rules applicable to that repository. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72(2).

Article 71a

Exercise of the delegation

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

2. The power to adopt delegated acts referred to in Article 38(3) and Article 42(4) shall be conferred on the Commission for an indeterminate period of time from ... [the date of entry into force of this Regulation].

3. The delegation of power referred to in Article 38(3) and Article 42(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

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

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

6. A delegated act adopted pursuant to Article 38(3) and Article 42(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 72

Committee procedure

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

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

Article 72a

Amendments to Council Decision 2007/533/JHA

Council Decision 2007/533/JHA is amended as follows:

1) Article 6 is replaced by the following:

"Article 6

National Systems

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

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

2) in Article 11, the following paragraphs 2 and 3 are added:

“2. Where a Member State cooperates with external contractors in any SIS II-related tasks, that Member State shall closely monitor the activities of the contractor to ensure compliance with all provisions of this Decision, including in particular security, confidentiality and data protection.

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

3) Article 15 is amended as follows:

(a) the following paragraph 3a is inserted:

"3a. The Management Authority shall develop and maintain a mechanism and procedures for carrying out quality checks on the data in CS-SIS and shall provide regular reports to the Member States. The Management Authority shall provide a regular report to the Commission covering the issues encountered and the Member States concerned. The Commission shall provide the European Parliament and the Council with a regular report on data quality issues encountered."

(b) paragraph 8 is replaced by the following:

“8. Operational management of Central SIS II shall consist of all the tasks necessary to keep Central SIS II functioning 24 hours a day, seven days a week in accordance with this Decision, 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 II and the national systems, ensuring that Central SIS II and the national systems operate in accordance with the technical requirements set out in Article 9 of this Decision.”

4) In Article 17, the following paragraphs 3 and 4 are added:

“3. Where the Management Authority cooperates with external contractors in any SIS II-related tasks, it shall closely monitor the activities of the contractor to ensure compliance with all provisions of this Decision, including in particular security, confidentiality and data protection.

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

5) In Article 21, the following second subparagraph is added:

"Where a person or an object is sought under an alert related to a terrorist offence, the case shall be considered adequate, relevant and important enough to warrant existence of an alert in SIS II. For public or national security reasons Member States may exceptionally refrain from creating an alert, when it is likely to obstruct official or legal inquiries, investigations or procedures."

6) Article 22 is replaced by the following:

"Article 22

Specific rules for verification or search with photographs and fingerprints

1. Photographs and fingerprints shall only be entered following a special quality check to ascertain the fulfilment of a minimum data quality standard. The specification of the special quality check shall be established in accordance with the procedure referred to in Article 67.

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

3. If the identity of the person cannot be ascertained by other means, fingerprint data shall be searched for identification purposes. Fingerprint data may be searched in all cases to identify a person. For this purpose the Central SIS II shall contain an Automated Fingerprint Identification System (AFIS).

4. Fingerprint data stored in SIS II in relation to alerts issued under Articles 26, 32 and 36 may also be searched with complete or incomplete sets of fingerprints discovered at the scenes of serious crimes or terrorist offences under investigation and where it can be established to a high degree of probability that they belong to a perpetrator of the offence provided that the search is carried out simultaneously in their relevant national fingerprints databases."

7) Article 41 is replaced by the following:

"*Article 41*

Access to SIS II data by Europol

1. The European Union Agency for Law Enforcement Cooperation (Europol) shall, where necessary to fulfil its mandate, have the right to access and search data entered into SIS II and may exchange and further request supplementary information in accordance with the provisions of the SIRENE Manual laid down in Article 8.

2. Where a search by Europol reveals the existence of an alert in SIS II, Europol shall inform the issuing Member State through the exchange of supplementary information by means of the communication infrastructure and in accordance with the provisions set out in the SIRENE Manual. Until Europol is able to use the functionalities intended for the exchange of supplementary information, it shall inform issuing Member States via the channels defined by Regulation (EU) 2016/794.

3. Europol may process the supplementary information that has been provided to it by Member States for the purposes of comparing with its databases and operational analysis projects, aimed at identifying connections or other relevant links and for strategic, thematic or operational analyses as defined in points (a), (b) and (c) of Article 18(2) of Regulation (EU) 2016/794. Any processing by Europol of supplementary information for the purpose of this Article shall be carried out in accordance with Regulation (EU) 2016/794.

4. The use of information obtained from a search in SIS II or from the processing of supplementary information is subject to the consent of the issuing Member State. If the Member State allows the use of such information, the handling thereof by Europol shall be governed by Regulation (EU) 2016/794. Europol may only communicate such information to third countries and third bodies with the consent of the issuing Member State and in full respect of Union law on data protection.

5. Europol shall:

a) without prejudice to paragraphs 3 and 6, not connect parts of SIS II 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 II;

b) notwithstanding Article 31(1) of Regulation (EU) 2016/794, delete supplementary information containing personal data at the latest one year after the related alert has been deleted from SIS II. By way of derogation, where Europol has information in its databases or operational analysis projects on a case to which the supplementary information is related, in order for Europol to perform its tasks, Europol may exceptionally continue to store the supplementary information when necessary. Europol shall inform the issuing and the executing Member State of the continued storage of such supplementary information and present a justification of such continued storage;

c) limit access to data entered in SIS II, including supplementary information to specifically authorised staff of Europol requiring access for the performance of their tasks;

d) adopt and apply measures to ensure security, confidentiality and self-monitoring in accordance with Articles 10, 11 and 13;

e) ensure that its staff authorized to process SIS II data receives appropriate training and information in accordance with Article 14;

f) without prejudice to Regulation (EU) 2016/794, allow the European Data Protection Supervisor to monitor and review the activities of Europol in the exercise of its right to access and search data entered in SIS II 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 Decision shall apply to such copies. The technical copy shall be used for the purpose of storing SIS II data whilst those data are searched. Once the data have been searched they shall be deleted. Such uses shall not be construed to be an unlawful downloading or copying of SIS II data. Europol shall not copy alert data or additional data issued by Member States or from CS-SIS II into other Europol systems.

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

8. Member States shall inform Europol through the exchange of supplementary information of any hit on alerts related to terrorist offences. Member States may exceptionally refrain from informing Europol if doing so would jeopardise current investigations, the safety of an individual or be contrary to essential interests of the security of the issuing Member State.

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

8) The following Article 41a is inserted:

"Article 41a

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

1. In accordance with Article 40(8) of Regulation (EU) 2016/1624, the members of the teams as defined in Article 2(8) and (9) of Regulation (EU) 2016/1624 shall, within their mandate and provided that they are authorised to carry out checks in accordance with Article 40(1) and have received the required training in accordance with Article 14, have the right to access and search data entered in SIS II in so far it is necessary for the performance of their task and as required by the operational plan for a specific operation. Access to data entered in SIS II shall not be extended to any other team members.

2. Members of the teams referred to in paragraph 1 shall exercise the right to access and search data entered in SIS II in accordance with paragraph 1 via a technical interface which is set up and maintained by the European Border and Coast Guard Agency and which allows a direct connection to Central SIS II.

3. Where a search by a member of the teams as referred to in paragraph 1 reveals the existence of an alert in SIS II, the issuing Member State shall be informed thereof. In accordance with Article 40 of Regulation (EU) 2016/1624, members of the teams may only act in response to an alert in SIS II under instructions from and, as a general rule, in the presence of border guards or staff involved in return-related tasks of the host Member State in which they are operating. The host Member State may authorise members of the teams to act on its behalf.

4. For the purpose of verifying the lawfulness of data processing, self-monitoring and ensuring proper data security and integrity the European Border and Coast Guard Agency shall keep logs of every access to and search in SIS II in accordance with the provisions of Article 12.

5. The European Border and Coast Guard Agency shall adopt and apply measures to ensure security, confidentiality and self-monitoring in accordance with Articles 10, 11 and. 13 and shall ensure that the teams referred to in paragraph 1, apply those measures.

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

7. Without prejudice to paragraph 2, no parts of SIS II shall be connected to any computer system for data collection and processing operated by the teams referred to in paragraph 1 of this Article or by the European Border and Coast Guard Agency, nor shall the data contained in SIS II to which those teams have access be transferred to such a system. No part of SIS II shall be downloaded. The logging of access and searches shall not be construed to be the downloading or copying of SIS II data.

8. Without prejudice to the further provisions of Regulation 45/2001, the European Border and Coast Guard Agency shall allow the European Data Protection Supervisor to monitor and review the activities of the teams as referred to in this Article in the exercise of their right to access and search data entered in SIS II."

Article 73

Amendments to Regulation (EU) 515/2014

(deleted)

Article 74

Repeal

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; 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) and Commission Decision 2010/261/EU of 4 May 2010 on the Security Plan for Central SIS II and the Communication Infrastructure[22] are repealed from the date of application of this Regulation set out in the first subparagraph of Article 75(4).

Article 75

Entry into force, start of operation and application

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

2. No later than 3 years after the entry into force of this Regulation the Commission shall adopt a decision setting the date on which SIS starts operations pursuant to this Regulation, after the verification that the following conditions are met:

   (a) the implementing acts necessary for the application of this Regulation have been adopted;

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

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

3. The Commission shall closely monitor the process of gradual fulfilment of the conditions set out in paragraph 2 and shall inform the European Parliament and the Council about the outcome of the verification.

---

[22] 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).

3a. By [one year after the entry into force of this Regulation] *[OPOCE, please replace with the actual date]* and every year thereafter until the decision of the Commission referred to in paragraph 2 has been taken, the Commission shall submit a report to the European Parliament and the Council on the state of play of the preparation of the full implementation of this Regulation. That report shall contain also detailed information about the costs incurred and information as to any risks which may impact the overall costs.

4. This Regulation shall apply from the date determined in accordance with paragraph 2.

By way of derogation from the first subparagraph:

(a) Article 4(3a), Article 8(4), Article 9(1) and (3), Article 12(8), Article 15(7), Article 19, Article 20(4) and (5), Article 26(6), Article 32(8), Article 34(3), Article 36(6), Article 38(4), Article 41A(2a), Article 42(4), Article 51A(2c), Article 59(4), Article 60(6), Article 71(6) and (9) Article 71a, Article 72, Article 72a (1) to (5) and Article 58(3)-(3a) shall apply from the date of entry into force of this Regulation;

(b) Article 72a(7) and (8) shall apply from [one year after the entry into force of this Regulation];

(c) Article 72a(6) shall apply from [two years after the entry into force of this Regulation].

5. The Commission decision referred to in paragraph 2 shall be published in *the Official Journal of the European Union*.

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

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

ANNEX IV

Statement by the European Parliament and the Council (on Ireland/Return)

The European Parliament and the Council invite the Commission, without prejudice to its right of initiative, once Ireland participates in Directive 2008/115/EC to assess the legal situation in accordance with the Treaties and the relevant Protocols and, as required, to present a legislative proposal to enable that cooperation on return between Ireland and the other Member States may be carried out through the SIS.

ANNEX V

Statement by the Council (on synergies between SIS and other information systems)

The Council considers that making the best use of data already available in relevant information systems at European level for the purposes of the Schengen Information System could facilitate the work of the Member States' competent authorities and reduce administrative burden.

Synergies between the Schengen Information System and the future Entry/Exit System, for instance, would facilitate and speed up the exchange of information in the event of hits, in particular, but not limited to, return alerts in SIS concerning third-country nationals crossing the external borders of a Member State: automated hit reporting mechanism between these systems could have significant benefits.

The Council therefore invites the European Commission to explore as soon as possible synergies between the Schengen Information System and other relevant EU information systems in the area of justice and home affairs, in particular Eurodac and the future Entry/Exit System, further to the synergies currently discussed in the context of interoperability.