COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 31.5.2005
COM(2005) 230 final

2005/0103 (CNS)

Proposal for a

COUNCIL DECISION

on the establishment, operation and use of the second generation Schengen information system (SIS II)

(presented by the Commission)

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

1.1. Grounds for and objectives of the proposal

General objective

The main objective of this Decision, together with the Regulation on the establishment, operation and use of the second generation of the Schengen Information System (hereinafter referred to as the "SIS II") based on Title IV of the Treaty establishing the European Community (hereinafter referred to as "EC Treaty") is to establish the legal framework that shall govern the SIS II. The availability of the SIS II as a compensatory measure that contributes to maintain a high level of security within an area without internal border controls is crucial so that the new Member States can fully apply the Schengen acquis and that their citizens can benefit from all the advantages of an area of free movement.

In this context, the Council laid down in December 2001 the first foundations for the SIS II by assigning its technical development to the Commission and allocating the necessary financial resources from the Budget of the European Union[1]. This Decision together with the aforementioned Regulation (hereinafter referred to as the "Regulation") represent now the second legal step, both instruments lay down common provisions on the architecture, financing, responsibilities and general data processing and data protection rules for the SIS II. Apart from these common rules, this Decision contains specific provisions regarding the processing of SIS II data for supporting police and judicial cooperation in criminal matters, while the Regulation rules on the processing of SIS II data supporting the implementation of policies linked to the movement of persons which are part of the Schengen acquis (e.g. external borders and visa).

Specific objectives

This Decision, as well as the Regulation, is largely based on the current provisions on the Schengen Information System (hereinafter referred to as the "SIS") contained in 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] (hereinafter referred to as the "Schengen Convention") taking also into account the Conclusions of the Council and the Resolutions of the European Parliament on SIS II[3]. In addition, this Decision also aims at better aligning the SIS legal framework with European Union law and enlarge the use of the SIS II, in particular, in the following areas:

---

1 Regulation EC No 2424/2001 and Decision 2001/886/JHA on the development of the second generation of the Schengen Information System.

2 Articles 92 to 119 of the Schengen Convention (OJ L 239, 22.09.2000, p.19) taking into account also the amendments to be entered in the Convention following the adoption of the Council Decision 2005/211/JAI concerning the introduction of some new functions for the SIS, including in the fight against terrorism, OJL68 15/03/05, p.44.

3 Council Conclusions on SIS II of 5-6 June 2003, 29 April and 14 June 2004 and European Parliament's Opinions and Resolutions T4-0082/1997, T5-0610/2002, T5-0611/2002, T5-0391/2003, T5-0392/2003 and T5-0509/2003.

– The European Arrest Warrant. This Decision provides for the processing (e.g. entering and sharing) of data necessary for the effective implementation of the Framework Decision on the European Arrest Warrant and surrender procedure between Member States. These data will be directly available in the SIS II improving therefore the current situation where these data are only exchanged bilaterally.

– Better data quality and improved identification performance. This Decision lays down the possibility, subject to the consent of the individual, of entering in the SIS II information on persons whose identity has been abused in order to avoid further inconveniences caused by misidentifications. This Decision also allows for the processing of biometrics that will result in more accurate identifications and improved quality of the personal data entered in the system.

– Data protection. In order to ensure consistent and homogeneous application of the data protection rules regarding the SIS II, this Decision provides for the application of Regulation (EC) 45/2001 on the protection of individuals with regard to the processing of personal data and entrusts the European Data Protection Supervisor with the monitoring of the personal data processing activities related to the SIS II carried out by the Commission in accordance with this Decision. The advantage is that the same body will be competent for all Commission's data processing activities under both the first and third pillar. This Decision provides that the Council of Europe Convention No 108 of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data must be respected by Member States when processing SIS II data in the context of this Decision.[4]

– Transfer of personal data to a third party or country. This Decision foresees the possibility of transferring SIS II personal data to third countries or international organisations subject to the appropriate legal instruments, however, this possibility remains as an exception to the general rule.

– Inter-governmental origin of the current SIS provisions. These provisions developed in an inter-governmental framework will be replaced by classic European law instruments. The advantage is that the different European Union institutions (hereinafter referred to as the "EU institutions") will be this time associated in the adoption and implementation of these new instruments and the legal value of the rules governing the SIS will be reinforced.

– Operational management of the SIS II. This Decision entrusts the Commission with the operational management of the system. The operational management of the Central Part of the current SIS is carried out by one Member State.

[4] When the Commission will have proposed the necessary instrument regarding the protection of personal data in the framework of Title VI of the Treaty on the European Union, it will be necessary to replace the reference to Convention No 108 in order to apply this new instrument to the processing of personal data carried out in application of this Decision.

1.2. General context

The SIS

The progressive establishment of an area of freedom, security and justice involves the creation of an area without internal frontiers. To this end, Article 61 of the EC Treaty requires the adoption of measures aimed at ensuring the free movement of persons, in accordance with Article 14 of the EC Treaty, in conjunction with flanking measures on external border controls, asylum and immigration, as well as measures to prevent and combat crime.

The SIS is a common information system allowing the competent authorities in the Member States to cooperate, by exchanging information for the implementation of the various policies required in order to establish an area without internal border controls. It allows these authorities, through an automatic query procedure, to obtain information related to alerts on persons and objects. The information obtained is used, in particular, for police and judicial cooperation in criminal matters as well as for controls of persons at the external borders or on national territory and for the issuance of visas and residence permits. The SIS, therefore, is an indispensable component of the Schengen area for applying the Schengen provisions on the movement of persons and in ensuring a high level of security in this area. Consistency with a wide range of policies linked to control of external borders, visa, immigration and also police and judicial cooperation in criminal matters is, therefore, essential.

Existing provisions and related proposals

Articles 92 – 119 of the Schengen Convention are the basic legal provisions governing the SIS. Adopted in an inter-governmental framework, they were incorporated in the institutional and legal framework of the European Union following the entry into force of the Treaty of Amsterdam.

This Decision is tabled together with a Regulation on the establishment, operation and use of the SIS II, based on Title IV of the EC Treaty. A third proposal based on Title V EC Treaty (Transport) regarding the specific issue of access to the SIS II by the authorities and services in the Member States responsible for issuing registration certificates for vehicles will complete these two proposals.

This Decision and the Regulation based on Title IV of the EC Treaty, will replace Articles 92-119 of the Schengen Convention and the Decisions and Declarations of the Schengen Executive Committee which are related to the SIS.

In addition, this Decision will also repeal Council Decision 2004/201/JHA of 19 February 2004 on procedures for amending the SIRENE Manual[5].

Calendar

The legal instruments regulating the SIS II should be adopted in due time for allowing the necessary preparations to this new system and, in particular, the migration from the current system to the SIS II.

[5] O J L 64, 02.03.2004, pp. 45.

2. LEGAL ASPECTS

2.1. Legal basis

The Schengen acquis, including the SIS, was integrated in the EU framework on 1 May 1999 by the Protocol annexed to the Amsterdam Treaty. The Council defined the parts of the Schengen acquis integrated in the Union framework in its Decision of 20 May 1999. These included the arrangements regarding the SIS i.e. Articles 92 to 119 of the Schengen Convention and the relevant Executive Committee decisions and declarations.

Council Decision 1999/436/EC of 20 May 1999[6] determined the legal basis in the Treaties for each of the provisions or decisions which constitute the Schengen acquis. Nevertheless, the Council did not reach a decision on the provisions regarding the SIS. Therefore, the provisions of the Schengen acquis concerning the SIS are regarded as acts based on Title VI of the Treaty on European Union (hereinafter referred to as "EU Treaty") on the basis of Article 2 (1) of the Schengen Protocol. However, under Article 5 (1) of the Protocol, any new proposal concerning the Schengen acquis must be based on the appropriate legal basis in the Treaties.

The legal bases for this Decision are Articles 30 (1) (a) and (b), Article 31 (1) (a) and (b) and Article 34 (2) (c) of the EU Treaty.

This proposal falls under Article 30 (1) (a) of the EU Treaty as it aims at improving operational cooperation between the competent authorities in relation to the prevention and detection of criminal offences and under Article 30 (1) (b) as it regulates the collection, storage, processing, and exchange of relevant information.

This proposal also aims at facilitating cooperation between judicial or equivalent authorities of the Member States in relation to criminal proceedings and the enforcement of criminal decisions, and therefore it falls as well under Article 31 (1) (a) of the EU Treaty. Article 31 (1) (b) is relevant to the extent that this proposal intends to facilitate extradition and surrender between Member States.

2.2. Subsidiarity and proportionality

In accordance with the principle of subsidiarity, the objective of the proposed action, namely the sharing of information regarding certain categories of persons and objects, through a computerised information system, cannot be sufficiently achieved by the Member States. Because of the very nature of a common information system and by reason of the scale and impact of the action, it can be better achieved at the level of the European Union. The present initiative does not go beyond what is necessary to achieve its objective.

The activities of the Commission are limited to the operational management of the SIS II comprising a central database, national access points and the communication infrastructure connecting both. Member States are competent for the national systems , for their connection to the SIS II and will enable the competent authorities to process SIS II data. The consultation of the data is restricted to competent authorities of each Member State, specified for each of the purposes as defined in this Decision and limited to the extent that the data are required for the performance of the tasks in accordance with these purposes.

---

[6] OJ L 176, 10.7.1999, p. 17.

2.3. Choice of instruments

The use of a Decision as the act is warranted in view of the need to apply common rules, in particular in relation to the processing of data in the system. A framework decision is not the appropriate instrument because the proposal involves no approximation of the laws of the Member States.

2.4. Participation in the SIS II

This Decision has its legal basis in Title VI of the EU Treaty and constitutes a development of the Schengen acquis. It must, therefore, be proposed and adopted in compliance with the Protocols annexed to the Amsterdam Treaty on the position of the United Kingdom, Ireland and the Protocol integrating the Schengen acquis into the framework of the European Union.

a) United Kingdom and Ireland

The proposed Decision develops the provisions of the Schengen acquis, in which the United Kingdom and Ireland participate, in accordance with 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[7], and with Council Decision 2002/192/EC of 28 February 2002, concerning Ireland's request to take part in some of the provisions of the Schengen acquis[8].

b) Norway and Iceland

In addition, in accordance with the first paragraph of Article 6 of the Protocol integrating the Schengen acquis, an Agreement was signed on 18 May 1999 between the Council, Norway and Iceland in order to associate those two countries with the implementation, application and development of the Schengen acquis.

Article 1 of the Agreement provides that Norway and Iceland are to be associated with the activities of the European Community and the European Union in the fields covered by the provisions referred to in Annexes A (provisions of the Schengen acquis) and B (provisions of European Community acts which have replaced corresponding provisions of or were adopted pursuant to the Schengen Convention) to the Agreement and further developments.

Pursuant to Article 2, the acts and measures adopted by the European Union to amend or supplement the Schengen acquis which has been integrated (Annexes A and B) are implemented and applied by Norway and Iceland. The proposal presented develops the Schengen acquis, as defined in Annex A to the Agreement.

c) New Member States

Since the initiative constitutes an act building upon the Schengen acquis or otherwise related to it within the meaning of Article 3(2) of the Act of Accession, the Decision shall only apply in a new Member State pursuant to a Council Decision in conformity with this provision.

---

7 OJ L 131, 1.6.2000, p. 43.

8 OJ L 64, 7.3.2002, p. 20.

d) Switzerland

As regards Switzerland, this Decision constitutes a development of the provisions of the Schengen acquis within the meaning of the Agreement signed by the European Union, the European Community and the Swiss Confederation on the latter's association with the implementation, application and development of the Schengen acquis[9] which falls within the area referred to in Article 1, point G of Council Decision 1999/437/EC read in conjunction with Article 4 (1) of the Council decision 2004/849/EC on the signing, on behalf of the European Union, and on the provisional application of certain provisions of this Agreement[10].

3. BUDGETARY IMPLICATIONS

Council Regulation (EC) No 2424/2001 and Council Decision 2001/886/JHA on the development of the second generation of the Schengen Information System[11] laid down that the expenditure involved in the development of the SIS II is to be charged to the budget of the European Union. The present proposal establishes that the cost incurred for the operation of the SIS II shall continue to be covered by the budget of the European Union. Although the biggest expenditure will be made during the development phase (design, construction and testing of the SIS II), the operational phase, starting in 2007, will constitute a long-term budgetary commitment that must be examined in the light of the new financial perspectives. Adequate human and financial resources will have to be allocated to the Commission, which is responsible for the operational management of the system during a first transitional or interim phase. For the mid to long-term the Commission will assess the different externalisation options, taking into account the synergy effects resulting from the operation of several other large-scale IT systems such as the VIS (Visa Information system) and EURODAC.

The Commission has prepared a common financial statement annexed to the Regulation proposed under Title IV of the EC Treaty.

---

9 Council document 13054/04.

10 OJ L 368, 15.12.2004, p.26.

11 OJ L 328 of 13.12.2001, p. 1.

2005/0103 (CNS)

Proposal for a

COUNCIL DECISION

on the establishment, operation and use of the second generation Schengen information system (SIS II)

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Article 30 (1) (a) and (b), Article 31 (1) (a) and (b) and Article 34 (2) (c) thereof,

Having regard to the proposal from the Commission[12],

Having regard to the opinion of the European Parliament[13],

Whereas:

(1) The Schengen information system (hereinafter referred to as "SIS") 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[14] (hereinafter referred to as the "Schengen Convention"), constitutes an essential tool for the application of the provisions of the Schengen acquis as integrated into the framework of the European Union.

(2) The development of the second generation of the SIS (hereinafter referred to as "SIS II") has been entrusted to the Commission pursuant to Council Regulation (EC) No 2424/2001[15] and Council Decision 2001/886/JHA[16] of 6 December 2001 on the development of the second generation Schengen Information System (SIS II). The SIS II will replace the SIS as established by the Schengen Convention.

(3) This Decision constitutes the necessary legislative basis for governing the SIS II in respect of matters falling within the scope of the Treaty on European Union (hereinafter referred to as the "EU Treaty"). Regulation (EC) No 2006/XX of the European Parliament and of the Council of the European Union on the establishment, operation and use of the SIS II[17] constitutes the necessary legislative basis for

---

12 OJ C , , p. .
13 OJ C , , p. .
14 OJ L 239, 22.9.2000, p. 19. Convention as last amended by Council Decision 2005/211/JHA.
15 OJ L 328, 13.12.2001, p. 4.
16 OJ L 328, 13.12.2001, p. 1.
17 OJ L...

governing the SIS II in respect of matters falling with the scope of the Treaty establishing the European Community (hereinafter referred to as the "EC Treaty").

(4) The fact that the legislative basis necessary for governing the SIS II consists of separate instruments does not affect the principle that the SIS II constitutes one single information system that should operate as such. Certain provisions of these instruments should therefore be identical.

(5) The SIS II should constitute a compensatory measure contributing to maintaining a high level of security within an area without internal border controls between Member States by supporting operational cooperation between police authorities and judicial authorities in criminal matters

(6) It is necessary to specify the objectives of the SIS II and to lay down rules concerning its operation, use and responsibilities, including technical architecture and financing, categories of data to be entered into the system, the purposes for which they are to be entered, the criteria for their entry, the authorities authorised to access it, the interlinking of alerts and further rules on data processing and the protection of personal data.

(7) The expenditure involved in the operation of the SIS II should be charged to the budget of the European Union.

(8) It is appropriate to establish a manual setting out detailed rules for the exchange of supplementary information in relation with the action required by the alert. National authorities in each Member States should ensure the exchange of this information.

(9) The Commission should be responsible for the operational management of the SIS II in particular in order to ensure a smooth transition between the development of the system and the start of its operations.

(10) The SIS II should contain alerts on persons wanted for arrest and surrender or extradition. In addition to alerts, it is appropriate to include in the SIS II additional data 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[18] should be processed in the SIS II.

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

(12) The SIS II should contain alerts on missing persons to ensure their protection or prevent threats, alerts on persons wanted for judicial procedure, alerts on persons and objects for discreet surveillance or specific checks and alerts on objects for seizure or use as evidence in criminal proceedings.

(13) It is appropriate to lay down maximum conservation periods for each category of alerts that can only be exceeded if necessary and proportionate for fulfilling the purpose of

[18] OJ L 190, 18.07.2002, p. 1.

the alert. As a general rule, alerts should be erased from the SIS II as soon as the action requested by the alert is taken.

(14) It should be possible to keep in SIS II alerts on persons wanted for arrest and surrender or extradition as well as persons wanted in order to ensure protection or prevent threats and persons wanted for judicial procedure for a maximum of 10 years, given the importance of these alerts for maintaining public security in the Schengen area.

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

(16) 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 the purpose of arrest and surrender, the use of the flag should be brought into line with Framework Decision 2002/584/JHA. The decision to add a flag to an alert should only be taken by the competent judicial authority and should only be based on the grounds for refusal contained in that Framework Decision.

(17) The SIS II should offer Member States the possibility to establish links between alerts. The establishment of links by a Member State between two or more alerts should have no impact on the action to be taken, the conservation period or the access rights to the alerts.

(18) It is appropriate to strengthen the cooperation between the European Union and third countries or international organisations in the field of police and judicial cooperation by promoting an efficient exchange of information. Where personal data is transferred from the SIS II to a third party, these personal data should be subject to an adequate level of protection by the third party, guaranteed by an agreement.

(19) All Member States have ratified the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data. Article 9 of that Convention allows exceptions and restrictions to the rights and obligations it provides, within certain limits. The personal data processed in the context of the implementation of this Decision should be protected in accordance with the principles of that Convention. The principles set out in the Convention should be supplemented or clarified in this Decision where necessary.

(20) The principles contained in Recommendation N° R (87) 15 of the Committee of Ministers of the Council of Europe of 17 September 1987 regulating the use of personal data in the police sector should be taken into account when personal data is processed by police authorities in application of this Decision.

(21) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of

personal data by the Community institutions and bodies and on the free movement of such data[19] applies to the processing of personal data by the Commission, when such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law. Part of the processing of personal data in the SIS II falls within the scope of Community law. Consistent and homogeneous application of the rules regarding the protection of individuals' fundamental rights and freedoms with regard to the processing of personal data requires clarification that, when the Commission is processing personal data in application of this Decision, Regulation (EC) No 45/2001 is applicable to it. The principles set out in that Regulation should be supplemented or clarified in this Decision where necessary.

(22) National independent supervisory authorities should monitor the lawfulness of the processing of personal data by the Member States, whilst the European Data Protection Supervisor appointed by Decision 2004/55/EC of the European Parliament and of the Council of 22 December 2003 appointing the independent supervisory body provided for in Article 286 of the EC Treaty (European Data Protection Supervisor)[20] should monitor the activities of the Commission in relation to the processing of personal data.

(23) Liability of the Community arising from any breach by the Commission of this Decision is governed by the second paragraph of Article 288 of the EC Treaty.

(24) The provisions of the Convention of 26 July 1995 on the establishment of a European Police Office[21] (hereinafter referred to as the "Europol Convention") concerning data protection apply to the processing of SIS II data by Europol, including the powers of the Joint Supervisory Body, set up under Article 24 of the Europol Convention, to monitor the activities of Europol and liability for any unlawful processing of personal data by Europol.

(25) The provisions of Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime [22]concerning data protection apply to the processing of SIS II data by Eurojust, including the powers of the Joint Supervisory Body, set up under Article 23 of that Decision, to monitor the activities of Eurojust and liability for any unlawful processing of personal data by Eurojust.

(26) In order to ensure transparency, a report on the activities of the SIS II and on the exchange of supplementary information should be produced every two years by the Commission. An overall evaluation should be issued by the Commission every four years.

(27) Some aspects of the SIS II such as compatibility of alerts, the adding of flags, links between alerts and exchange of supplementary information cannot be covered exhaustively by the provisions of this Decision due to their technical nature, level of detail and need for regular updates. Implementing powers in respect of those aspects should therefore be delegated to the Commission.

---

19 OJ L 8, 12.1.2001, p.1.
20 OJ L 12, 17.1.2004, p. 47.
21 OJ C 316, 27.11.1995, p. 2.
22 OJ L 63, 6.3.2002, p. 1.

(28) This Decision should define the procedure for the adoption of the measures necessary for its implementation. The procedure for adopting implementing measures under this Decision and Regulation (EC) No XX/2006 should be the same.

(29) It is appropriate to lay down transitional provisions in respect of alerts issued in the SIS in accordance with the Schengen Convention, which will be transferred to the SIS II or alerts issued in the SIS II during a transitional period before all provisions of this Decision become applicable. Some provisions of the Schengen acquis should continue to apply for a limited period of time until the Member States have examined the compatibility of those alerts with the new legal framework.

(30) It is necessary to lay down special provisions regarding the remainder of the budget affected to the operations of the SIS which is not part of the budget of the European Union.

(31) Since the objectives of the action to be taken, namely the establishment and regulation of a joint information system, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of the action, be better achieved at the level of the European Union, the Council may adopt measures in accordance with the principle of subsidiarity, as set out in Article 5 of the EC Treaty and referred to in Article 2 of the EU Treaty. In accordance with the principle of proportionality as set out in Article 5 of the EC Treaty, this Decision does not go beyond what is necessary to achieve those objectives.

(32) This Decision respects the fundamental rights and observes the principles recognised, in particular by the Charter of Fundamental Rights of the European Union.

(33) The United Kingdom is taking part in this Decision, in accordance with Article 5 of the Protocol integrating the Schengen acquis into the framework of the European Union annexed to the EU Treaty and to the EC Treaty, and Article 8 (2) of Council Decision 2000/365/EC of 29 May 2000, concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis [23].

(34) Ireland is taking part in this Decision in accordance with Article 5 of the Protocol integrating the Schengen acquis into the framework of the European Union annexed to the EU Treaty and to the EC Treaty, and Article 6 (2) of Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen acquis[24].

(35) This Decision is without prejudice to the arrangements for the United Kingdom and Ireland's partial participation in the Schengen acquis, as defined in Decision 2000/365/EC and 2002/192/EC, respectively.

(36) As regards Iceland and Norway, this Decision 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 association of those two States with the implementation,

---

[23] OJ L 131, 1.6.2000, p. 43.

[24] OJ L 64, 7.3.2002, p. 20.

application and development of the Schengen acquis which fall within the area referred to in Article 1, point G of Council Decision 1999/437/EC of 17 May 1999[25] on certain arrangements for the application of that Agreement.

(37) As regards Switzerland, this Decision constitutes a development of the 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 Council Decision 1999/437/EC read in conjunction with Article 4 (1) of the Council decision 2004/849/EC on the signing, on behalf of the European Union, and on the provisional application of certain provisions of that Agreement[26].

(38) This Decision constitutes an act building on the Schengen acquis or otherwise related to it within the meaning of Article 3 (2) of the 2003 Act of Accession,

HAS DECIDED AS FOLLOWS :

CHAPTER I

General provisions

Article 1

Establishment and general objective of the SIS II

1. A computerised information system called the second generation Schengen information system (hereinafter referred to as "SIS II") is hereby established to enable competent authorities of the Member States to cooperate by exchanging information for the purposes of controls on persons and objects.

2. The SIS II shall contribute to maintaining a high level of security within an area without internal border controls between Member States.

Article 2

Scope

1. This Decision defines the conditions and procedures for the processing of alerts and additional data related to them in the SIS II and the exchange of supplementary information for the purposes of police and judicial cooperation in criminal matters.

---

[25] OJ L 176, 10.7.1999, p. 31.
[26] OJ L 368, 15.12.2004, p. 26

2. This decision also lays down provisions on the technical architecture of the SIS II, responsibilities of the Member States and the Commission, general data processing, rights of individuals concerned and liability.

Article 3

Definitions

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

   (a) "alert" means a set of data entered in the SIS II allowing the competent authorities to identify a person or an object in view of a specific action to be taken;

   (b) "supplementary information" means the information not stored in the SIS II, but connected to SIS II alerts, which is necessary in relation to the action to be taken;

   (c) "additional data" means the data stored in the SIS II and connected to SIS II alerts which is necessary for allowing the competent authorities to take the appropriate action;

2. "Processing of personal data", "processing" and "personal data" shall be understood in accordance with Article 2 of Directive 95/46/EC of the European Parliament and of the Council[27].

Article 4

Technical architecture and ways of operating the SIS II

1. The SIS II is composed of:

   (a) a central database called "the Central Schengen Information System" (hereinafter referred to as "CS-SIS");

   (b) one to two access points defined by each Member State (hereinafter referred to as "NI-SIS");

   (c) a communication infrastructure between the CS-SIS and the NI-SIS.

2. The National Systems of the Member States (hereinafter referred to as "NS") shall be connected to the SIS II via the NI-SIS.

---

[27] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 23.11.1995 p. 31.

3. The national competent authorities referred to in Article 40 (4) shall enter data, access and perform searches in the SIS II directly or in a copy of data of the CS-SIS available in their NS.

4. The communication infrastructure between the CS-SIS and the NI-SIS shall be used by Member States for the exchange of supplementary information.

Article 5

Costs

1. The costs incurred in connection with the operation and maintenance of the SIS II comprising CS-SIS, NI-SIS and the communication infrastructure between CS-SIS and NI-SIS shall be borne by the budget of the European Union.

2. The costs of developing, adapting and operating each NS shall be borne by the Member State concerned.

3. Additional costs incurred as a result of the use of the copies referred to in Article 4 (3) shall be borne by the Member States that make use of such copies.

CHAPTER II

Responsibilities of the Member States

Article 6

National Systems

Each Member State shall be responsible for operating and maintaining its NS and connecting it to the SIS II.

Article 7

SIS II National office and SIRENE authorities

1. Each Member State shall designate an office which shall ensure competent authorities' access to the SIS II in accordance with this Decision.

2. Each Member State shall designate the authorities which shall ensure the exchange of all supplementary information, hereinafter referred to as the "SIRENE authorities". These authorities shall verify the quality of the information entered into the SIS II. For those purposes they shall have access to data processed in the SIS II.

3. The Member States shall inform each other and the Commission of the officereferred to in paragraph 1 and of the SIRENE authorities referred to in paragraph 2.

Article 8

Exchange of supplementary information

1. Member States shall exchange all supplementary information through the SIRENE authorities. Such information shall be exchanged in order to allow Member States to consult or inform each other whilst entering an alert, following a hit, when the required action cannot be taken, when dealing with the quality of SIS II data and compatibility of alerts as well as for the exercise of the right of access.

2. Detailed rules for the exchange of supplementary information shall be adopted in accordance with the procedure defined in Article 61 in the form of a manual, to be called the "SIRENE Manual".

Article 9

Technical Compliance

1. Each Member State shall ensure the compatibility of its NS with the SIS II and observe the procedures and technical standards established for that purpose in accordance with the procedure referred to in Article 60.

2. Where relevant, Member States shall ensure that the data present in the copies of the data of the CS-SIS database is at all times identical and consistent with the CS-SIS.

3. Where relevant, Member States shall ensure a search in copies of the data of the CS-SIS produces the same result as a search performed directly in the CS-SIS.

Article 10

Security and confidentiality

1. Member States having access to data processed in the SIS II shall take the necessary measures to:

   (a) prevent any unauthorised person having access to installations in which operations relating to the NI-SIS and NS are carried out (checks at the entrance to the installation);

   (b) prevent SIS II data and data media from being accessed, read, copied, modified or erased by unauthorised persons (control of data media);

(c) prevent the unauthorised accessing, reading, copying, modification or erasure of SIS II data for the transmission between the NS and the SIS II (control of transmission);

(d) ensure the possibility of checking and establishing *a posteriori* what SIS II data has been recorded into, when and by whom (control of data recording);

(e) prevent unauthorised processing of SIS II data in the NS and any unauthorised modification or erasure of SIS II data recorded in the NS (control of data entry);

(f) ensure that, in using the NS, authorised persons have access only to SIS II data which fall within their competence (control of access);

(g) ensure that it is possible to check and establish to which authorities SIS II data recorded in NS may be transmitted by data transmission equipment (control of transmission).

(h) monitor the effectiveness of the security measures referred to in this paragraph (self-auditing).

2 Member States shall take measures equivalent to those referred to in paragraph 1 as regards security and confidentiality in respect of the exchange and further processing of supplementary information.

3. Professional secrecy or an equivalent obligation of confidentiality shall apply to all persons and to all bodies required to work with SIS II data and supplementary information.

The obligation of confidentiality shall also apply after those people leave office or employment or after the termination of the activities of those bodies.

Article 11

Keeping of logs at national level

1. Each Member State shall keep logs of all exchanges of data with the SIS II and its further processing, for the purpose of monitoring the lawfulness of data processing, ensuring the proper functioning of the NS, data integrity and security.

2. The logs shall show, in particular, the date and time of the data transmitted, the data used for interrogation, the data transmission and the name of both the competent authority and the person responsible for processing the data.

3. The logs shall be protected by appropriate measures against unauthorised access and erased after a period of one year, if they are not required for monitoring procedures which have already begun.

4. The competent authorities of the Member States, in particular those in charge of the supervision of the processing of data in the SIS II, shall have the right to access the

logs for the purposes of monitoring the lawfulness of data processing and to ensure the proper functioning of the system, including data integrity and security. Each Member State shall transmit the findings of such monitoring to the Commission without delay for the purpose of integrating them, as appropriate, into the reports provided for in Article 59 (3).

Chapter III

Responsibilities of the Commission

Article 12

Operational management

1. The Commission shall be responsible for the operational management of the SIS II.

2. The operational management shall consist of all the tasks necessary to keep the SIS II functioning on a 24 hours a day, 7 days a week basis in accordance with this Decision, in particular the maintenance work and technical developments necessary for the smooth running of the system.

Article 13

Security and confidentiality

With reference to the operation of the SIS II, the Commission shall apply Article 10 mutatis mutandis.

Article 14

Keeping of logs at central level

1. All processing operations within the SIS II shall be logged for the purposes of monitoring the lawfulness of data processing and ensuring the proper functioning of the system, data integrity and security.

2. The logs shall show, in particular, the date and time of the operation, the data processed and the identification of the competent authority.

3. The logs shall be protected by appropriate measures against unauthorised access and erased after a period of one year following erasure of the alert to which they are related, if they are not required for monitoring procedures which have already begun.

4. The competent national authorities, in particular those in charge of the supervision of processing data in the SIS II, shall have the right to access the logs only for the purposes of monitoring the lawfulness of data processing and to ensure the proper functioning of the system, including data integrity and security. .

   Such access shall be reserved to the logs relating to the processing operations carried out by the Member State concerned.

5. The Commission shall have the right to access the logs only for the purposes of ensuring the proper functioning of the system, data integrity and security.

6. The European Data Protection Supervisor shall have the right to access the logs for the sole purpose of monitoring the lawfulness of the personal data processing operations performed by the Commission including data security.

CHAPTER IV

Alerts in respect of persons wanted for arrest and surrender or extradition

Article 15

Objectives and conditions for issuing alerts

Alerts shall be issued in the SIS II at the request of the competent judicial authority in respect of persons wanted for arrest and surrender on the basis of a European Arrest Warrant or in respect of persons wanted for provisional arrest with a view to extradition.

Article 16

Additional data on persons wanted for arrest and surrender

1. In addition to the alert referred to in Article 15, the issuing Member State shall enter into the SIS II the data referred to in Article 8 (1) of Framework Decision 2002/584/JHA and a copy of the original of the European Arrest Warrant.

2. The issuing Member State may enter a translation of the data referred to in paragraph 1 and/or of the original of the European Arrest Warrant in one or more other official languages of the institutions of the European Union.

Article 17

Additional data on persons wanted for arrest and extradition

1. In addition to the alert referred to in Article 15, the issuing Member State shall enter into the SIS II the following data on persons wanted for arrest and extradition:

   (a) the identity and nationality of the wanted person;

   (b) the name, address, telephone and fax numbers and e-mail address of the issuing judicial authority;

   (c) evidence of an enforceable judgment or any other enforceable judicial decision having the same effect;

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

   (e) a description of the circumstances in which the offence was committed, including the time, place and degree of participation in the offence by the wanted person;

   (f) the penalty imposed, if there is a final judgment, or the prescribed scale of penalties for the offence under the law of the issuing Member State;

   (g) if possible, other consequences of the offence.

2. The issuing Member State may enter a translation of the additional data referred to in paragraph 1 in one or more other official languages of the institutions of the European Union.

Article 18

Authorities with right to access to alerts and additional data on persons wanted for arrest

1. The following authorities shall have the right to access the alerts referred to in Article 15, for the purposes specified :

   (a) police and border authorities, for the purposes of arrest;

   (b) national judicial authorities and those responsible for public prosecutions, for the purpose of criminal proceedings.

2. The European Police Office (Europol) shall have the right to access the data contained in alerts for arrest which is necessary for the performance of its tasks in accordance with the Convention of 26 July 1995 on the establishment of a European Police Office ("the Europol Convention").

3. Eurojust shall have the right to access the data contained in alerts for arrest and the data referred in Articles 16 and 17 which is necessary for the performance of its tasks in accordance with Decision 2002/187/JHA.

4. National judicial authorities and those responsible for public prosecutions shall have the right to access the data referred to in Article 16 for the purpose of executing a European Arrest Warrant and the data referred to in Article 17 for the purpose of the extradition procedure.

Article 19

Conservation period of the alerts and additional data for arrest

1. Alerts issued for arrest and the additional data referred to in Articles 16 and 17 shall be kept in the SIS II until the wanted person has been surrendered or extradited. They shall only be kept for as long as the issuing Member State considers the warrant valid according to its national law.

2. Alerts issued for arrest and the additional data referred to in Articles 16 and 17 shall automatically be erased after 10 years from the date of the decision giving rise to the alert. The Member State having entered the data in the SIS II may decide to keep it in the system, should this prove necessary for the purpose for which the data was entered.

3. Member States will be informed systematically one month before the automatic erasure of the data from the system.

Article 20

Flagging related to alerts on persons wanted for arrest

1. When a flag has been added to an alert for arrest in accordance with Article 45 and the arrest cannot be made but the location of the person is known, the Member State which added the flag shall regard the alert as being an alert for the purposes of communicating the place of residence of the person concerned.

2. The need for maintaining a flag added to an alert on a person wanted for arrest shall be reviewed at least every six months by the Member State adding the flag. Member States may provide for a shorter review period.

Article 21

Flagging related to alerts for arrest and surrender

1. A flag as provided for in Article 45 (1) prohibiting arrest may only be added to an alert for arrest and surrender where the competent judicial authority has given authorisation on the basis of a clear and obvious ground for the non-execution of a European Arrest Warrant based on Framework Decision 2002/548/JHA or where the person has been provisionally released following arrest.

The flag shall be added at the earliest opportunity and if possible not later than seven days after the alert has been issued in the SIS II.

2. The prohibition on arrest and surrender shall remain effective until the flag is erased.

A flag shall be erased as soon as the grounds for non-execution of the European Arrest Warrant have ceased to exist or the provisional release has ended.

3. Paragraphs 4 and 5 of Article 45 shall not apply to flags related to alerts for the purpose of arrest and surrender.

Article 22

Execution of action based on an alert on a person wanted for arrest and surrender

An alert entered in the SIS II for the purpose of arrest and surrender shall have the same effect as regards the action to be taken as a European Arrest Warrant issued in accordance with Article 9 (3) of Framework Decision 2002/584/JHA.

Chapter V

Alerts on persons to ensure protection or prevent threats

Article 23

Objectives and conditions for issuing alerts

1. Member States shall issue in the SIS II alerts on missing persons or persons who, for their own protection or in order to prevent threats, need to be placed under temporary police protection at the request of the competent administrative or judicial authority.

2. Alerts referred to in paragraph 1 shall be issued in particular with respect to missing minors and persons who must be interned following a decision by a competent authority.

Article 24

Authorities with right to access to alerts

1. Police and border authorities shall have the right to access the alerts referred to in Article 23 for the purpose of putting the person concerned under police protection or for the purpose of tracing the whereabouts of a missing person.

2. National judicial authorities, *inter alia* those responsible for the initiation of public prosecutions in criminal proceedings and judicial inquiries prior to indictment, may have access to the alerts referred to in Article 23, in the performance of their tasks.

Article 25

Conservation period of the alerts

1. Alerts issued for the purpose of ensuring protection or preventing threats shall be erased as soon as the person is placed under police protection.

2. The alerts referred to in paragraph 1 shall automatically be erased after 10 years from the date of the decision giving rise to the alert. The Member State having entered the alert in the SIS II may decide to keep the alert in the system, should this prove necessary for the purpose for which the alert was entered.

3. Member States will be informed systematically one month before the automatic erasure of the alerts from the system.

Article 26

Execution of action based on an alert

1. The competent authorities of the Member State where a person referred to in Article 23 is found shall communicate the whereabouts of the person to the Member State issuing the alert by the exchange of supplementary information.

   The detailed rules for this exchange shall be adopted in accordance with Article 61 and inserted in the SIRENE Manual.

2. The communication of the whereabouts of a missing person who is of age shall be subject to that person's consent.

3. The competent authorities of the Member State where a person referred to in Article 23 is found may move the person to a safe place in order to prevent that person from continuing his journey, if so authorised by national law.

Chapter VI

Alerts on persons wanted for judicial procedure

Article 27

Objectives and conditions for issuing alerts

Member States shall issue in the SIS II alerts on witnesses, persons summoned to appear before the national judicial authorities in connection with criminal proceedings in order to account for acts for which they are being prosecuted, or persons who are to be served with a criminal judgment or a summons to report in order to serve a penalty involving deprivation of liberty at the request of the competent judicial authority for the purpose of ascertaining their place of residence or domicile.

Article 28

Authorities with right to access to alerts

1. Police and border authorities shall have the right to access the alerts referred to in Article 27 for the purpose of ascertaining the place of residence or domicile of the persons concerned.

2. National judicial authorities, *inter alia* those responsible for the initiation of public prosecutions in criminal proceedings and judicial inquiries prior to indictment, may have access to the alerts referred to in Article 27 which are necessary for the performance of their tasks.

3. Eurojust shall have the right to access the data contained in alerts referred to in Article 27 which are necessary for the performance of its tasks in accordance with Decision 2002/187/JHA.

Article 29

Conservation period of alerts

1. Alerts referred to in Article 27 shall be erased as soon as the place of residence or domicile of the person concerned has been ascertained.

2. Alerts referred to in Article 27 shall automatically be erased after 10 years from the date of the decision giving rise to the alert. The Member State having entered the alert in the SIS II may decide to keep the alert in the system, should this prove necessary for the purpose for which the alert was entered.

3. Member States will be informed systematically one month before the automatic erasure of the alerts from the system.

Article 30

Execution of the action based on an alert

1. The competent authorities of the Member State where a person referred to in Article 27 is found shall communicate the place of residence or domicile of the person to the Member State issuing the alert by the exchange of supplementary information.

2. The detailed rules for this exchange shall be adopted in accordance with the procedure defined in Article 61 and inserted in the SIRENE Manual.

Chapter VII

Alerts on persons and objects for discreet surveillance or specific checks

Article 31

Objectives and conditions for issuing alerts

1. At the request of the competent judicial or administrative authority, Member States shall, for the purposes of prosecuting criminal offences and for the prevention of threats to public security, issue in the SIS II alerts on persons or vehicles, boats, aircrafts and containers for the purpose of discreet surveillance or of specific checks in the following circumstances:

   (a) where there is clear evidence that the person concerned intends to commit or is committing numerous and extremely serious criminal offences or

   (b) where an overall assessment of the person concerned, in particular on the basis of past criminal offences, gives reason to suppose that that person will also commit extremely serious criminal offences in the future.

2. Member States may issue alerts in the SIS II, at the request of the authorities responsible for national security, where there is clear evidence that the information referred to in Article 32 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 shall inform the other Member States thereof by the exchange of supplementary information. The detailed rules for this exchange shall be adopted in accordance with the procedure defined in Article 61 and inserted in the SIRENE Manual.

Article 32

Collection and exchange of supplementary information for alerts

1. In cases of alerts for discreet surveillance, the competent authorities of the Member States which carry out border checks or other police and customs checks within the country may collect and communicate to the authority issuing the alert all or some of the following information:

   (a) the fact that the person for whom, or the vehicle for which an alert has been issued has been found;

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

   (c) the route and destination of the journey;

   (d) the persons accompanying the persons concerned or the occupants of the vehicle;

   (e) the vehicle used;

   (f) objects carried;

   (g) the circumstances under which the person or the vehicle was found.

2. The information referred to in paragraph 1 shall be communicated by the exchange of supplementary information. The detailed rules for this exchange shall be adopted in accordance with the procedure defined in Article 61 and inserted in the SIRENE Manual.

3. For the collection of the information referred to in paragraph 1, Member States shall take the necessary steps not to jeopardise the discreet nature of the surveillance.

4. During the specific checks referred to in Article 31, persons, vehicles, boats, aircraft, containers and objects carried may be searched in accordance with national law for the purposes referred to in that Article. If specific checks are not authorised under the law of a Member State, they shall automatically be replaced, in that Member State, by discreet surveillance.

Article 33

Authorities with right to access to alerts

1. Police, border and customs authorities shall have the right to access to the alerts referred to in Article 31 for the purpose of performing discreet surveillance or specific checks.

2. National judicial authorities, inter alia those responsible for the initiation of public prosecutions in criminal proceedings and judicial inquiries prior to indictment, may have access to the alerts referred to in Article 31 in the performance of their tasks.

3. Europol shall have the right to access to the data of the alerts referred to in Article 31 which are necessary to perform its tasks in accordance with the Europol Convention.

Article 34

Conservation period of alerts

1. Alerts on persons issued pursuant to Article 31 shall automatically be erased after 3 years from the date of the decision giving rise to the alert.

2. Alerts on objects issued pursuant to Article 31 shall automatically be erased after 5 years from the date of the decision giving rise to the alert.

3. The Member State having entered an alert in the system may decide to keep the alert in the SIS II, should this prove necessary for the purpose for which the alert was entered.

4. Member States will be informed systematically one month before the automatic erasure of the alerts from the system.

Chapter VIII

Alerts on objects for seizure or use as evidence in criminal proceedings

Article 35

Objectives and conditions for issuing alerts

1. At the request of the competent authority, Member States shall, for the purposes of seizure or use as evidence in criminal proceedings, issue in the SIS II alerts on the following objects:

   (a) motor vehicles with a cylinder capacity exceeding 50cc, boats and aircrafts which have been stolen, misappropriated or lost;

   (b) trailers with an unladen weight exceeding 750 kg, caravans, industrial equipment, outboard engines and containers which have been stolen, misappropriated or lost;

   (c) firearms which have been stolen, misappropriated or lost;

   (d) blank official documents which have been stolen, misappropriated or lost;

(e) issued identity papers such as passports, identity cards, driving licenses, residence permits and travel documents which have been stolen, misappropriated, lost or invalidated;

(f) vehicle registration certificates and vehicle number plates which have been stolen, misappropriated, lost or invalidated;

(g) banknotes (registered notes);

(h) securities and means of payment such as cheques, credit cards, bonds, stocks and shares which have been stolen, misappropriated or lost.

2. The Commission shall establish the technical rules necessary for entering and accessing the data contained in the alerts referred to in paragraph 1 in accordance with Article 60.

Article 36

Collection and exchange of supplementary information for alerts

1. If a search brings to light an alert for an object which has been found, the authority of the Member State where the object was found shall contact the authority which issued the alert, in order to agree on the measures to be taken. For this purpose, personal data may be communicated in accordance with this Decision.

2. The contacts and communication of personal data referred to in paragraph 1 shall be done through the exchange of supplementary information. The detailed rules for this exchange shall be adopted in accordance with the procedure defined in Article 61 and inserted in the SIRENE Manual.

3. The measures to be taken by the Member State which finds the object shall be in accordance with its national law.

Article 37

Authorities with right to access to alerts

1. Police, border and custom authorities shall have the right to access the alerts referred to in Article 35 for the purpose of seizure of the object.

2. National judicial authorities, inter alia those responsible for the initiation of public prosecutions in criminal proceedings and judicial inquiries prior to indictment, may have access to the alerts referred to in Article 35, in the performance of their tasks.

3. Europol shall have the right to access the data contained in the alerts referred to in Article 35 which are necessary to perform its tasks, in accordance with the Europol Convention.

Article 38

Conservation period of alerts

1. Alerts on objects referred to in Article 35 shall be erased as soon as the objects have been seized.

2. Alerts referred to in Article 35 which contain no personal data shall automatically be erased after a period of ten years from the date of the decision giving rise to the alert.

3. Alerts referred to in Article 35 which contain personal data shall automatically be erased in the SIS II after a period of three years from the date of the decision giving rise to the alert.

4. The Member State having entered the alert in the SIS II may decide to keep the alert in the system for a period longer than the conservation periods laid down in paragraphs 2 and 3 should this prove necessary for the purpose for which the alerts were entered.

5. Member States will be informed systematically one month before the automatic erasure of the alerts from the system.

CHAPTER IX

General data processing rules

Article 39

Categories of data

1. No more than the following data shall be contained in the alerts on persons issued in the SIS II in application of this Decision:

   (a) surname(s) and forename(s), name at birth and previously used names and any aliases, possibly entered separately;

   (b) date and place of birth;

   (c) sex;

   (d) photographs;

   (e) fingerprints;

   (f) nationality;

(g) any specific objective and physical characteristics not subject to frequent change;

(h) whether the person concerned is armed, violent or has escaped;

(i) reason for the alert;

(j) authority issuing the alert;

(k) action to be taken;

(l) in cases of alerts for arrest, the type of offence;

(m) link(s) to other alerts processed in the SIS II.

2. The data referred to in paragraph 1 shall only be used for the purpose of identifying a person in view of a specific action to be taken in accordance with this Decision.

3. The Commission shall establish the technical rules necessary for entering and accessing the data referred to in paragraph 1 in accordance with Article 61.

Article 40

Processing of SIS II data

1. Data entered in the SIS II pursuant to this Decision shall only be processed for the purposes and by the competent national authorities defined by the Member States in accordance with this Decision.

2. A Member State may change the category of an alert to another only if this is necessary to prevent an imminent serious threat to public policy, public security, on serious grounds of national security or for the purposes of preventing a serious criminal offence. The alert whose category is changed shall be considered as a new alert issued by the Member State requesting the change of category. For this purpose a prior authorisation of the Member State that issued the first alert shall be obtained by the exchange of supplementary information. The detailed rules for this exchange of supplementary information shall be adopted in accordance with the procedure defined in Article 61 and inserted in the SIRENE Manual.

3. Access to SIS II data shall only be authorised within the limits of the competence of the national authority and to duly authorised staff.

4. Each Member State shall maintain and transmit to the Commission an up-to-date list of national authorities who are authorised to process SIS II data. That list shall specify, for each authority, which category of data it may process, for what purpose and who is to be considered as controller, and shall be communicated by the Commission to the European Data Protection Supervisor. The Commission shall ensure the annual publication of the list in the *Official Journal of the European Union*.

Article 41

Entering a reference number

A Member State accessing the SIS II without making use of a copy of data of the CS-SIS referred to in Article 4 (3) may add a reference number to the alerts it issues for the sole purpose of tracing national information linked to the issued alert.

Access to the reference number shall be restricted to the Member State that issued the alert.

Article 42

Copy of SIS II data

1. Except for the copy of data of the CS-SIS referred to in Article 4 (3), the data processed in the SIS II may only be copied for technical purposes and provided that such copying is necessary for the competent national authorities to access the data in accordance with this Decision.

2. Data entered into the SIS II by another Member State shall not be copied into Member State's own national data files.

3. Paragraph 2 shall not prejudice the right of a Member State to keep in its national file SIS II 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.

4. This article shall not prejudice the right of a Member State to keep in its national files data contained in a particular alert, which that Member State has issued in the SIS II.

Article 43

Quality of the data processed in the SIS II and compatibility between alerts

1. The Member State entering the data in the SIS II shall be responsible for ensuring that that data is processed lawfully and, in particular, that it is accurate and up-to-date.

2. Only the Member State which entered data in the SIS II shall modify, add to, correct or erase it.

3. If a Member State, which did not enter the data, has evidence suggesting that data is incorrect or has been unlawfully processed in the SIS II, it shall inform the Member States which entered the data by exchanging supplementary information at the earliest opportunity and if possible not later then 10 days after the evidence comes to its attention. The Member State which entered the data shall check it and, if necessary, modify, add to, correct or erase it. The detailed rules for this exchange of

supplementary information shall be adopted in accordance with the procedure defined in Article 61 and inserted in the SIRENE Manual.

4. If Member States are unable to reach agreement within two months about the correction of the data, any of them may submit the case to the European Data Protection Supervisor who shall act as mediator.

5. The Member States shall exchange supplementary information in order to distinguish accurately between alerts in the SIS II related to persons with similar characteristics. The detailed rules for this exchange of supplementary information shall be adopted in accordance with the procedure defined in Article 61 and inserted in the SIRENE Manual.

6. When a person is already the subject of an alert in the SIS II, the Member State issuing a new alert in respect of the same person shall reach agreement on the entry of this new alert with the Member State which issued the first alert. The agreement shall be reached on the basis of the exchange of supplementary information. The detailed rules for this exchange of supplementary information shall be adopted in accordance with the procedure defined in Article 61 and inserted in the SIRENE Manual.

Different alerts on the same person may be entered in the SIS II if they are compatible.

The rules governing the compatibility of and priority of categories of alerts shall be determined in accordance with the procedure set out in Article 61.

7. Data kept in the SIS II shall be reviewed at least annually by the issuing Member State. Member States may provide for a shorter review period.

Article 44

Additional data for the purpose of dealing with misidentifications of persons

1. Where confusion may arise between the person actually intended by an alert and a person whose identity has been misused, Member States shall add data related to the latter to the alert in order to avoid the negative consequences of misidentifications.

2. The data related to an individual whose identity has been misused shall only be added with that individual's explicit consent and shall only be used for the following purposes:

(a) to allow the competent authority to differentiate the individual whose identity has been misused from the person actually intended by the alert;

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

3. No more than the following personal data may be entered and further processed in SIS II for the purpose of this article:

(a) surname(s) and forename(s), any aliases possibly entered separately;

(b) date and place of birth;

(c) sex;

(d) photographs;

(e) fingerprints;

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

(g) nationality;

(h) number(s) of identity paper(s) and date of issuing.

4. The data referred to in paragraph 3 shall be erased at the same time as the corresponding alert or earlier if the person so requests.

5. Only the authorities having the right to access the corresponding alert may access the data referred to in paragraph 3 and for the sole purpose of avoiding misidentification.

6. The technical rules referred to in Article 39 (3) shall apply to the data referred to in paragraph 3 of this article.

Article 45

Flagging

1. A Member State may add a flag to the alerts issued in accordance with Articles 15, 23 and 31 to the effect that the action to be taken on the basis of the alert will not be taken on its territory.

A flag may be added to an alert where a Member State considers that an alert issued in the SIS II is incompatible with its national law, its international obligations or essential national interests.

2. In order to enable Member States to determine whether to add a flag, all Member States shall be notified automatically via the SIS II about any new alert issued in accordance with Article 15 and about the additional data referred to in Articles 16 and 17.

A Member State issuing an alert in accordance with Articles 23 and 31 shall inform the other Member States thereof by the exchange of supplementary information. The detailed rules for that exchange shall be adopted in accordance with the procedure defined in Article 61 and inserted in the SIRENE Manual.

3. A Member State wishing to add a flag to an alert shall consult the Member State issuing the alert by the exchange of supplementary information. The detailed rules for that exchange shall be defined in accordance with the procedure defined in

Article 61 and inserted in the SIRENE Manual. If the Member State issuing the alert does not withdraw the alert, it shall continue to apply in full to Member States which do not add a flag.

4. The flag shall be erased at the latest one month after it has been added, unless the Member State refuses to take the action on legal grounds or for special reasons of expediency.

5. If in particularly urgent and serious cases, an issuing Member State requests the execution of the action, the executing Member State shall examine whether it is able to withdraw its flag. 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.

6. The procedure and technical rules for adding flags and updating them shall be adopted in accordance with Article 60.

Article 46

Links between alerts

1. A Member State may create a link between alerts it issues in the SIS II in accordance with its national legislation. 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 conservation period of each of the linked alerts.

3. The creation of links shall not affect the rights to access provided for in this Decision. Authorities with no right to access certain categories of alerts shall not have access to the links to those categories.

4. When a Member State considers that the creation 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.

5. The technical rules for linking alerts shall be adopted in accordance with Article 60.

Article 47

Purpose and conservation period of supplementary information

1. The supplementary information transmitted by another Member State shall be used only for the purpose for which it was transmitted. It shall only be kept in national files as long as the alert to which it relates is kept in the SIS II. Member States may keep this information for a longer period if necessary to achieve the purpose for which it was transmitted. In any event, the supplementary information shall be erased at the latest one year after the related alert has been erased from the SIS II.

2. Paragraph 1 shall not prejudice the right of a Member State to keep in national files data relating to a particular alert in connection with which action has been taken on its territory. Such data may be held in national files for a maximum period of three years, except if specific provisions of national law authorise retention of the data for a longer period.

Article 48

Transfer of personal data to third parties

1. Except if explicitly provided for in EU law, the personal data processed in the SIS II in application of this Decision shall not be transferred or made available to a third country or to an international organisation.

2. By way of derogation from paragraph 1, personal data may be transferred to third countries or international organisations in the framework of a European Union agreement in the field of police or judicial cooperation guaranteeing an adequate level of protection of the transferred personal data and with the consent of the Member State that entered the data in the SIS II.

CHAPTER X

Data protection

Article 49

Application of the Council of Europe data protection Convention

Personal data processed in application of this Decision shall be protected in accordance with the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data and subsequent amendments thereto.

Article 50

Right of information

1. On request, an individual whose data is to be processed in the SIS II in application of this Decision shall be informed about:

(a) the identity of the controller and his representative, if any;

(b) the purposes for which the data will be processed within the SIS II;

(c) the potential recipients of the data;

(d) the reason for issuing the alert in the SIS II;

(e) the existence of the right of access and the right to rectify his personal data.

2. Communication of the information referred to in paragraph 1 to the individual concerned shall be refused if this is indispensable for the performance of a lawful task in connection with the data entered in the SIS II or for protecting the rights and freedoms of the individual concerned or of third parties. In any event, it shall be refused during the period of validity of an alert for the purpose of discreet surveillance.

Article 51

Right of access, rectification and erasure

1. The right of individuals to have access to, and to obtain the rectification or erasure of their personal data processed in the SIS II shall be exercised in accordance with the law of the Member State before which that right is invoked.

2. If the Member State before which the right of access is invoked did not enter the data, it shall communicate the data to the individual concerned after having given the Member State which entered the data an opportunity to state its position. This shall be done through an exchange of supplementary information. The detailed rules for this exchange of supplementary information shall be adopted in accordance with the procedure defined in Article 61 and inserted in the SIRENE Manual.

3. The personal data shall be communicated to the individual concerned as soon as possible and in any event not later than 60 days from the date on which he applies for access.

4. Communication of the information to the individual concerned shall be refused if this is indispensable for the performance of a lawful task in connection with the data entered in the SIS II or for protecting the rights and freedoms of the concerned individual or of third parties. In any event, it shall be refused during the period of validity of an alert for the purpose of discreet surveillance.

5. The individual shall be informed about the follow-up given to the exercise of his rights of rectification and erasure as soon as possible and in any event not later than 6 months from the date on which he applies for rectification or erasure.

Article 52

Remedies

Any person in the territory of any Member State shall have the right to bring an action or a complaint before the courts of that Member State if he is refused the right of access to or the

right to rectify or erase data relating to him or the right to obtain information or reparation in connection with the processing of his personal data contrary to this Decision.

Article 53

Data protection authorities

1. Each Member State shall ensure that an independent authority monitors the lawfulness of the processing of SIS II personal data on its territory including the exchange and further processing of supplementary information. Any individual shall have the right to ask the supervisory authority to check the lawfulness of data processing performed in the SIS II concerning him. That right shall be governed by the national law of the Member State to which the request is made. If the data was entered in the SIS II by another Member State, the control shall be carried out in close coordination with that Member State's supervisory authority.

2. The supervisory authorities referred to in Article 24 of the Europol Convention and 23 of Decision 2002/187/JHA shall ensure the lawfulness of the access to, and as the case may be, the further processing of SIS II personal data by Europol and Eurojust.

3. The European Data Protection Supervisor shall monitor that the personal data processing activities of the Commission are carried out in accordance with this Decision.

4. The authorities referred to in this Article shall cooperate with each other. The European Data Protection Supervisor shall convene a meeting for that purpose at least once a year.

CHAPTER XI

Liability and sanctions

Article 54

Liability

1. Each Member State shall be liable for any damage caused to an individual arising from unauthorised or incorrect processing of data, communicated via the SIS II or SIRENE authorities, carried out by that Member State.

2. If the Member State against which an action is brought pursuant to paragraph 1 is not the Member State which entered the data in the SIS II, the latter shall reimburse, on request, the sums paid out as compensation unless the data was used by the requested Member State in breach of this Decision.

3. If failure of a Member State to comply with its obligations under this Decision causes damage to the SIS II, that Member State shall be held liable for such damage, unless and insofar as the Commission or other Member State(s) participating in the SIS II failed to take reasonable steps to prevent the damage from occurring or to minimise its impact.

Article 55

Sanctions

Member States shall ensure that processing of SIS II data or supplementary information contrary to this Decision is subject to effective, proportionate and dissuasive sanctions in accordance with national law.

CHAPTER XII

Access to SIS II by Europol and Eurojust

Article 56

Access by Europol and Eurojust

Both Europol and Eurojust shall each define one to two access point(s) to access the SIS II.

Article 57

Access to SIS II data by Europol

1. Where access to the SIS II by Europol reveals the existence of an alert in the SIS II which is of interest for Europol, Europol shall inform the Member State which issued the alert, via the Europol national unit of this Member State.

2. Use of information obtained by Europol from access to the SIS II, including communication of the information to third countries and bodies, shall be subject to the consent of the issuing Member State. Such consent shall be obtained via the Europol national unit of that Member State.

3. If the issuing Member State allows the use of the information, the processing thereof shall be governed by the Europol Convention.

4. Europol shall adopt and apply mutatis mutandis security and confidentiality provisions in accordance with the provisions laid down in Article 10.

5. Europol shall record its access to the SIS II and further processing of SIS II data, in accordance with the prescriptions laid down in Article 11.

6. Without prejudice to paragraph 1, Europol shall not connect parts of the SIS II nor transfer the data contained therein to which it has access to any computer system for data processing in operation by or at Europol nor download or otherwise copy any part of the SIS II.

7. Europol may request supplementary information or the additional data referred to in Articles 16 and 17 from the Member State which issued the alert via the Europol national unit of the Member State concerned.

Article 58

Access to SIS II data by Eurojust

1. Where access to the SIS II by Eurojust reveals the existence of an alert in the SIS II which is of interest for Eurojust, Eurojust shall inform the Member State which issued the alert, via the concerned national members of Eurojust.

2. Use of information obtained by Eurojust from such access to the SIS II, including communication of the information to third countries and bodies, shall be subject to the consent of the issuing Member State. Such consent shall also be obtained via the national member of Eurojust of that Member State.

3. If the issuing Member State allows the use of the information, the processing thereof shall be governed by Decision 2002/187/JHA.

4. Eurojust shall adopt and apply mutatis mutandis security and confidentiality provisions in accordance with the prescriptions laid down in Article 10.

5. Eurojust shall record its access to the SIS II and further processing of SIS II data in accordance with the prescriptions laid down in Article 11.

6. Without prejudice to paragraph 1, Eurojust shall not connect parts of the SIS II, nor transfer the data contained therein to which it has access to any computer system for data processing in operation by or at Eurojust, nor download or otherwise copy any parts of the SIS II.

7. Eurojust may request supplementary information from the Member State concerned in accordance with the provisions set out in Decision 2002/187/JHA.

8. The access to data entered in the SIS II shall be limited to the national members and their assistants and not be extended to Eurojust staff.

CHAPTER XIII

Final provisions

Article 59

Monitoring, evaluation and statistics

1. The Commission shall ensure that systems are in place to monitor the functioning of the SIS II against objectives, in terms of output, cost-effectiveness and quality of service.

2. For the purposes of technical maintenance, reporting and statistics, the Commission shall have access to the necessary information related to the processing operations performed in the SIS II.

3. Two years after the SIS II starts operations and every two years thereafter, the Commission shall submit to the European Parliament and the Council a report on the activities of the SIS II and on the bilateral and multilateral exchange of supplementary information between Member States.

4. Four years after the SIS II starts operations and every four years thereafter, the Commission shall produce an overall evaluation of the SIS II and the bilateral and multilateral exchange of supplementary information between Member States. This overall evaluation shall include the examination of results achieved against objectives and assess the continuing validity of the underlying rationale and any implications of future operations. The Commission shall transmit the reports on the evaluation to the European Parliament and the Council.

5. Member States shall provide the Commission with the information necessary to draft the reports referred to in paragraphs 3 and 4.

Article 60

Advisory Committee

1. Where reference is made to this Article, the Commission shall be assisted by an advisory Committee composed of the representatives of the Member States and chaired by the representative of the Commission.

2. The Committee shall adopt its rules of procedure on a proposal made by the Chair on the basis of standard rules of procedure which have been published in the Official Journal of the European Union.

3. The representative of the Commission shall submit to the Committee a draft of the measures to be taken. The Committee shall deliver its opinion on the draft, within a

time-limit which the Chair may lay down according to the urgency of the matter, if necessary by taking a vote. The Chair shall not vote.

4. The opinion shall be recorded in the minutes; in addition, each Member State shall have the right to ask to have its position recorded in the minutes.

5. The Commission shall take the utmost account of the opinion delivered by the Committee. It shall inform the Committee of the manner in which the opinion has been taken into account.

Article 61

Regulatory Committee

1. Where reference is made to this Article, the Commission shall be assisted by a regulatory Committee composed of the representatives of the Member States and chaired by the representative of the Commission. The representative of the Commission shall submit to the Committee a draft of the measures to be taken. The Committee shall deliver its opinion on the draft within a time limit which the Chair may lay down according to the urgency of the matter. The opinion shall be delivered by the majority laid down in Article 205 (2) of the EC Treaty in the case of decisions which the Council is required to adopt on a proposal from the Commission. The votes of the representatives of the Member States within the Committee shall be weighted in the manner set out in that Article. The Chair shall not vote.

2. The Committee shall adopt its rules of procedure on a proposal made by the Chair on the basis of standard rules of procedure which have been published in the Official Journal of the European Union.

3. The Commission shall adopt the measures envisaged if they are in accordance with the opinion of the Committee. If the measures envisaged are not in accordance with the opinion of the Committee, or if no opinion is delivered, the Commission shall, without delay, submit to the Council a proposal relating to the measures to be taken.

4. The Council may act by qualified majority on the proposal, within a period of two months from the date of referral to the Council. If within that period the Council has indicated by qualified majority that it opposes the proposal, the Commission shall re-examine it. It may submit an amended proposal to the Council, re-submit its proposal or present a legislative proposal. If on the expiry of that period the Council has neither adopted the proposed implementing act nor indicated its opposition to the proposal for implementing measures, the proposed implementing act shall be adopted by the Commission.

Article 62

Amendment of the Schengen Convention

1. For the purposes of matters falling within the scope of the EU Treaty, this Decision replaces Articles 92 to 119 of the Schengen Convention with the exception of Article 102 (a) thereof.

2. It also replaces the following provisions of the Schengen acquis implementing these articles[28]:

   (a) Decision of the Executive Committee of 14 December 1993 on the Financial Regulation on the costs of installing and operating the Schengen information system (C.SIS) (SCH/Com-ex (93) 16);

   (b) Decision of the Executive Committee of 7 October 1997 on contributions from Norway and Iceland to the costs of installing and operating of the C.SIS (SCH/Com-ex (97) 18);

   (c) Decision of the Executive Committee of 7 October 1997 on the development of the SIS (SCH/Com-ex (97) 24);

   (d) Decision of the Executive Committee of 15 December 1997 amending the Financial Regulation on C.SIS (SCH/Com-ex (97) 35);

   (e) Decision of the Executive Committee of 21 April 1998 on C.SIS with 15/18 connections (SCH/Com-ex (98) 11);

   (f) Decision of the Executive Committee of 28 April 1999 on C.SIS installation expenditure (SCH/Com-ex (99) 4);

   (g) Decision of the Executive Committee of 28 April 1999 on updating the SIRENE manual (SCH/Com-ex (99) 5);

   (h) Declaration of the Executive Committee of 18 April 1996 defining the concept of alien (SCH/Com-ex (96) decl. 5);

   (i) Declaration of the Executive Committee of 28 April 1999 on the structure of SIS (SCH/Com-ex (99) decl. 2 rev.).

3. For the purposes of matters falling within the scope of the EU Treaty, references to the replaced articles of the Schengen Convention and relevant provisions of the Schengen acquis implementing those articles shall be construed as references to this Decision and shall be read in accordance with the correlation table set out in the Annex.

---

[28] OJ L 239 22.9.2000 p. 439.

Article 63

Repeal

Decision 2004/201/JHA is repealed[29].

Article 64

Transitional period and budget

1. Articles 94, 95, 97, 98, 99 and 100 and Article 101 (1) and (2) of the Schengen Convention shall continue to apply to alerts issued in the SIS and transferred to the SIS II or to alerts issued directly in the SIS II before the date set in accordance with Article 65 (3) of this Decision until one year after that date.

   One year after the date set in accordance with Article 65(3), those alerts shall be automatically erased from the SIS II unless Member States have reissued those alerts in accordance with this Decision.

2. The remainder of the budget at the date set in accordance with Article 65 (2), which has been approved in accordance with Article 119 of the Schengen Convention, shall be paid back to the Member States. The amounts to be repaid shall be calculated on the basis of the contributions from the Member States as laid down in the Decision of the Executive Committee of 14 December 1993 on the financial regulation on the costs of installing and operating the Schengen Information System.

Article 65

Entry into force and applicability

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

   It shall apply from a date to be determined by the Commission in accordance with paragraphs 2 and 3.

2. The date from which Articles 1 to 14 and Articles 40 to 64 with the exception of Articles 41, 44, 45 and 46 are to apply shall be determined after:

   (a) the necessary implementing measures have been adopted;

   (b) the Commission has made the necessary technical arrangements for allowing the SIS II to be connected to the Member States and

[29] OJ L 64, 2/03/2004

(c) all Member States have notified the Commission that they have made the necessary technical and legal arrangements to process SIS II data and exchange supplementary information in accordance with the aforementioned articles.

The Commission shall publish the date in the *Official Journal of the European Union*.

3. The date from which Articles 15 to 39 and Articles 41, 44, 45 and 46 are to apply shall be determined after:

(a) the necessary implementing measures have been adopted and

(b) all Member States have notified the Commission that they have made the necessary technical and legal arrangements to process SIS II data and exchange supplementary information in accordance with the aforementioned articles.

The Commission shall publish the date in the *Official Journal of the European Union*.

Done at Brussels,

For the Council
The President

ANNEX

Correlation table

Schengen Convention[30] Articles	**Decision Articles**
Art. 92(1)	Art. 1(1); Art. 2(1); Art. 4(1)(2)(3)
Art. 92(2)	Art.4 (1) (2) (3); Art. 5(2)(3); Art. 6; Art.9
Art. 92(3)	Art.4 (1)(2)(3); Art.5(1); Art. 12
Art. 92(4)	Art.3 (1); Art. 7(2)(3); Art.8
Art. 93	Art.1(2)
Art. 94(1)	Art. 40(1)
Art. 94(2)	Art.15; Art.23 (1) ; Art.27 ; Art. 31(1) Art. 35(1)
Art. 94(3)	Art. 39(1); Art. 44(3)
Art. 94(4)	Art. 45
Art. 95(1)	Art. 15
Art. 95(2)	Art. 16; Art. 17; Art. 45
Art. 95(3)	Art.20; Art. 21; Art. 45
Art. 95(4)	Art. 45(5)
Art. 95(5)	Art. 20(1)
Art. 95(6)	Art. 22
Art. 96(1)	
Art. 96(2)	
Art. 96(3)	

[30] Articles and paragraphs in italics have been added or amended by Council Regulation (EC) No. 871/2004 and Council Decision 2005/211/JAI on the introduction of new functions for the Schengen Information System, including the fight against terrorism

Schengen Convention[30] Articles	**Decision Articles**
Art. 97	Art. 23; Art. 26
Art. 98(1)	Art. 27
Art. 98(2)	Art. 30
Art. 99(1)	Art. 31(1)
Art. 99(2)	Art. 31(1)
Art. 99(3)	Art. 31(2)
Art. 99(4)	Art. 32(1)(2)(3)
Art. 99(5)	Art. 32(4)
Art. 99(6)	Art. 45
Art. 100(1)	Art. 35
Art. 100(2)	Art. 36
Art. 100(3)	Art. 35
Art. 101(1)	Art. 18(1)(4); Art. 24; Art. 28(1)(2); Art.33(1)(2); Art. 37(1)(2)
Art. 101(2)	
Art. 101(3)	Art. 40(3)
Art. 101(4)	Art. 40(4)
Art. 101A(1)	Art. 18(2); Art. 33(3); Art. 37(3)
Art. 101A(2)	Art. 18(2); Art. 33(3); Art. 37(3)
Art. 101A(3)	Art. 57(1)
Art. 101A(4)	Art. 57(2)
Art. 101A(5)	Art. 57(7)
Art. 101A(6)	Art. 53(2); Art. 57(4)(5)(6)

Schengen Convention[30] Articles	**Decision Articles**
Art. 101B(1)	Art. 18(3); Art. 28(3)
Art. 101B(2)	Art. 18(3); Art. 28(3); Art. 58(8)
Art. 101B(3)	Art. 58(1)(2)
Art. 101B(4)	Art. 53(2); Art. 58(3)
Art. 101B(5)	Art. 58(5)
Art. 101B(6)	Art. 58(6)
Art. 101B(7)	Art. 58(8)
Art. 101B(8)	Art. 58(4)
Art. 102(1)	Art. 40(1)
Art. 102(2)	Art. 42(1)(2)
Art. 102(3)	Art. 40(2)
Art. 102(4)	
Art. 102(5)	Art. 54(1)
Art. 103	Art. 11
Art. 104(1)	
Art. 104(2)	
Art. 104(3)	
Art. 105	Art. 43(1)
Art. 106(1)	Art. 43(2)
Art. 106(2)	Art. 43(3)
Art. 106(3)	Art. 43(4)
Art. 107	Art. 43(6)
Art. 108(1)	Art. 7(1)
Art. 108(2)	

Schengen Convention[30] Articles	**Decision Articles**
Art. 108(3)	Art. 6; Art. 7(1); Art. 9(1)
Art. 108(4)	Art. 7(3)
Art. 109(1)	Art. 50(1); Art. 51(1)(2)(3)
Art. 109(2)	Art. 51(4)
Art. 110	Art. 51(1)(5); Art.53(1)
Art. 111(1)	Art. 52
Art. 111(2)	
Art. 112(1)	Art. 19(1)(2); Art.25(1)(2); Art. 29(1)(2); Art.34(1)(2)(3); Art. 43(7)
Art. 112(2)	Art. 43(7)
Art. 112(3)	Art. 19(3); Art. 25(3); Art. 29(3); Art. 34(4); Art. 38(5)
Art. 112(4)	Art. 19(2); Art. 25(2); Art. 29(2); Art. 34(3); Art. 38(4)
Art. 112A(1)	Art. 47(1)
Art. 112A(2)	Art. 47(2)
Art. 113(1)	Art. 38(1)(2)(3)
Art. 113(2)	Art. 14(3)(4)(5)(6)
Art. 113A(1)	Art. 47(1)
Art. 113A(2)	Art. 47(2)
Art. 114(1)	Art. 53(1)
Art. 114(2)	Art. 53

Schengen Convention[30] Articles	**Decision Articles**
Art. 115(1)	Art. 53(3)
Art. 115(2)	
Art. 115(3)	
Art. 115(4)	
Art. 116(1)	Art. 54(1)
Art. 116(2)	Art. 54(2)
Art. 117(1)	Art. 49
Art. 117(2)	
Art. 118(1)	Art. 10(1)
Art. 118(2)	Art. 10(1)
Art. 118(3)	Art. 10(3)
Art. 118(4)	Art. 13
Art. 119(1)	Art. 5(1); Art. 64(2)
Art. 119(2)	Art. 5(2)(3)