EUROPEAN PARLIAMENT

2004 *2009*

Committee on Civil Liberties, Justice and Home Affairs

25.4.2006 PE 372.150v01-00

AMENDMENTS 175-256

Draft report **(PE 365.022v01-00)**
Carlos Coelho
Proposal for a Council decision on the establishment, operation and use of the second generation Schengen information system (SIS II)

Proposal for a decision (COM(2005)0230 – C6-0301/2005 – 2005/0103(CNS))

Draft legislative resolution

Amendment by Sylvia-Yvonne Kaufmann
Amendment 175
Citation 4 a (new)

- having regard to the opinion of the European Data Protection Supervisor of 19 October 2005 and the opinion of the Article 29 Working Party of 25 November 2005,

Or. de

Justification

The amendment emphasises the importance of data protection and highlights the opinions many passages from which provide the basis for other amendments.

Amendment by Sylvia-Yvonne Kaufmann

Amendment 176
Paragraph 4 a (new)

4a. Calls on the Council to ensure that this decision does not come into force until Council Framework Decision 2005/XX/JHA on the protection of personal data processed in the

context of police and judicial cooperation in criminal matters has entered into force;

Or. de

Justification

It is vitally important that the framework decision on data protection referred to above should enter into force before this decision in order to guarantee a high level of data protection in connection with the processing of personal data contained in the SIS II under the third pillar.

Proposal for a decision

Text proposed by the Commission	Amendments by Parliament

Amendment by Edith Mastenbroek

Amendment 177
Recital 5

(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.	(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 ***and to applying the provisions of Title IV of the EC Treaty relating to the free movement of persons.***

Or. en

Justification

Title IV of the Consolidated version of the Treaty establishing the European Community refers to visas, asylum, immigration and other policies related to free movement of persons and should therefore be included in the proposal.

Amendment by Sylvia-Yvonne Kaufmann

Amendment 178
Recital 5

(5) The SIS II should ***constitute*** a	(5) The SIS II ***should, as*** a compensatory

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***.	measure***, guarantee*** a high level of security within an area without internal border controls between Member States.

Or. de

Amendment by Edith Mastenbroek

Amendment 179
Recital 6

(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.	(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, ***a high level of security*** 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.

Or. en

Justification

Managing a database of this kind requires clear guidelines to guarantee its secure functioning. Therefore it is necessary to determine responsibilities.

Amendment by Edith Mastenbroek

Amendment 180
Recital 7

(7) The expenditure involved in the operation of the SIS II should be charged to the budget of the European Union.	(7) The expenditure involved in the operation of the SIS II should be charged to the budget of the European Union. ***However, if Member States decide to make use of the***

	possibility to create national copies, they should bear the costs related thereto.

Or. en

Amendment by Edith Mastenbroek

Amendment 181
Recital 8

(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.	(8) It is ***necessary*** 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.

Or. en

Amendment by Henrik Lax

Amendment 182
Recital 9

(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.	(9) ***During a transitional period of 3 years after the entry into force of this Decision*** 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.

Or. en

Amendment by Edith Mastenbroek

Amendment 183
Recital 9

(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	(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.	system and the start of its operations. ***The data stored in the current SIS may be transferred to the new system only after the current system has been audited and the integrity of the data held therein checked.***

Or. en

Justification

The old data should be checked and audited before transferring it into the new database to ensure that no false or untrustworthy information will be transmitted.

Amendment by Henrik Lax

Amendment 184
Recital 9 a (new)

	(9a) After the transitional period of 3 years after the entry into force of this Decision, the operational management should be the responsibility of a European Agency for the Operational Management of large-scale IT-systems.

Or. en

Amendment by Edith Mastenbroek

Amendment 185
Recital 13

(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 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.	(13) Maximum conservation periods for each category of alerts ***should be laid down***. As a general rule, alerts should be be erased from the SIS II as soon as the action requested by the alert is taken.

Or. en

Amendment by Edith Mastenbroek

Amendment 186
Recital 14

(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.	(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 for a maximum of 10 years, given the importance of these alerts for maintaining public security in the Schengen area.

Or. en

Amendment by Sylvia-Yvonne Kaufmann

Amendment 187
Recital 14

(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.	(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 ***three*** years, given the importance of these alerts for maintaining public security in the Schengen area.

Or. de

Justification

The current system lays down a maximum retention period of three years (Article 112 of the Schengen implementing agreement). The Commission provides no justification for keeping alerts in the system for a longer period, so that the current maximum period of three years should be retained.

Amendment by Sylvia-Yvonne Kaufmann

Amendment 188
Recital 15

(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.	(15) The SIS II should 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.

Or. de

Justification

See the justification for the amendment to Article 39(1)(d) and (e).

Amendment by Edith Mastenbroek

Amendment 189
Recital 15

(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.	(15) The SIS II should permit the processing of biometric data in order to assist in the reliable identification of individuals concerned. ***However, biometric data may not be used as a search tool.*** 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.

Or. en

Amendment by Edith Mastenbroek

Amendment 190
Recital 17

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

Or. en

Amendment by Edith Mastenbroek

Amendment 191
Recital 18

(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.	(18) Where personal data is transferred from the SIS II to a third party, these personal data should be subject to ***a high*** level of protection by the third party, guaranteed by an agreement.

Or. en

Amendment by Edith Mastenbroek

Amendment 192
Recital 18 a (new)

	(18a) The SIS II may be linked to other databases only after a thorough security

analysis has been conducted.

Or. en

Amendment by Sylvia-Yvonne Kaufmann

Amendment 193
Recital 19

(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.***	(19) ***The processing of personal data under this decision is assessed on the basis of Council Framework Decision 2005/XX/JHA on the protection of personal data processed in the context of police and judicial cooperation in criminal matters. The framework decision must therefore be in force before this Decision enters into force.***

Or. de

Justification

See the justification for the amendment incorporating a new paragraph 4a into the draft legislative resolution.

Amendment by Edith Mastenbroek

Amendment 194
Recital 22

(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	(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) should monitor the activities of the Commission in relation to the processing of personal data.	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) should monitor the activities of the Commission in relation to the processing of personal data. ***The national supervisory authorities and the European Data Protection Supervisor should cooperate closely.***

Or. en

Justification

As there will be issues with repercussions on both levels, it is appropriate that the two competent authorities work together.

Amendment by Edith Mastenbroek

Amendment 195
Recital 29

(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.	(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. ***Those alerts may be entered into the SIS II only if their integrity can be assured.*** 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. ***Alerts that are found to be incompatible therewith should be erased.***

Or. en

Amendment by Edith Mastenbroek

Amendment 196
Recital 29 a (new)

(29a) To ensure the proper functioning of the SIS II, an audit should be carried out of the current SIS, taking into account both the security and integrity of the information and alerts held in the system, the technical system as such, the communication infrastructure with the national access points and so forth. The results of that audit should be taken into account before the SIS II is brought into operation.

Or. en

Amendment by Edith Mastenbroek

Amendment 197
Recital 29 b (new)

(29b) An overall security plan should be developed for the SIS II before the system is brought into operation. Such plan should take into account both the physical and behavioural aspects of security of the system at national and European level. The plan should give a clear overview of the responsibilities of each person concerned at each level.

Or. en

Justification

Making a broad analysis of security is more than technically securing the system but also entails the behaviour of the people operating the system.

Amendment by Edith Mastenbroek

Amendment 198
Article 1, paragraph 1

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***.	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 ***referred in this Decision***.

Or. en

Amendment by Sylvia-Yvonne Kaufmann

Amendment 199
Article 1, paragraph 2

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

Or. de

Amendment by Edith Mastenbroek

Amendment 200
Article 1, paragraph 2

2. The SIS II shall contribute to maintaining a high level of security within an area without internal border controls between Member States.	2. The SIS II contribute to maintaining a high level of security within an area without internal border controls between Member States ***and applying the provisions of Title IV of the EC Treaty relating to the free movement of persons.***

Or. en

Amendment by Edith Mastenbroek

Amendment 201
Article 2, paragraph 2

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

Or. en

Amendment by Sylvia-Yvonne Kaufmann

Amendment 202
Article 4, paragraph 1, letter (b)

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

Or. de

Justification

Until such time as a convincing justification has been provided that two access points are needed, with a view to reducing the risk of misuse provision should be made for only one access point (opinion of the European Data Protection Supervisor, p. 21).

Amendment by Edith Mastenbroek

Amendment 203
Article 4, paragraph 2

2. The National Systems of the Member States (hereinafter referred to as “NS”) shall be connected to the SIS II via 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. ***The communication system must need all safety protocols as outlined in the overall SIS II security plan.***

Or. en

Amendment by Henrik Lax

Amendment 204
Article 4 a (new)

Article 4a

Location

Acting in accordance with the procedure laid down in Article 251 of the Treaty, the European Parliament and the Council shall adopt a Regulation to establish the location of the main Central Schengen Information System and the location of its back-up system.

Or. en

Amendment by Edith Mastenbroek

Amendment 205
Article 4 a (new)

Article 4a

The European Agency for the Operational Management of the SIS II shall determine where the CS-SIS and its backup system are to be located.

Or. en

Justification

As soon as the operational management has been decided upon, a location has to be chosen where the CS-SIS and its back up will be. The European Agency should have the right to decide on the best possible location.

Amendment by Edith Mastenbroek

Amendment 206
Article 6

Each Member State shall be responsible for operating and maintaining its NS and connecting it to the SIS II.	Each Member State shall ***set up and*** be responsible for operating and maintaining its NS and connecting it to the SIS II. ***Each Member State shall implement the guidelines set out in the overall security plan.***

Or. en

Amendment by Edith Mastenbroek

Amendment 207
Article 7, paragraph 1

1. Each Member State shall designate ***an*** office which shall ensure competent authorities' access to the SIS II in accordance with this Decision.	1. Each Member State shall designate ***a SIS II national*** office***, under the clear responsibility of the Member State,*** which shall ***bear the central responsibility for the national system, be responsible for the smooth operation and the security of the national system and*** ensure competent authorities' access to the SIS II in accordance with this Decision.

Or. en

Amendment by Edith Mastenbroek

Amendment 208
Article 9, paragraph 2

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.	2. 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.

Or. en

Amendment by Edith Mastenbroek

Amendment 209
Article 9, paragraph 3

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.	3. 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.

Or. en

Amendment by Edith Mastenbroek

Amendment 210
Article 9, paragraph 3 a (new)

3a. Member States shall ensure that the authorities accessing the data present in the copies are only be able to see the information, alerts and links they are entitled to see.

Or. en

Amendment by Edith Mastenbroek

Amendment 211
Article 9, paragraph 3 b (new)

3b. Member States shall keep a detailed log of who accesses the copies, how many copies exist and where the copies are held.

Or. en

Amendment by Edith Mastenbroek

Amendment 212
Article 10

Security ***and confidentiality***	Security
	-1Member States shall implement the security guidelines laid down in the security plan set out in paragraph 1.
1. Member States ***having access to*** data processed in the SIS II ***shall take the necessary measures*** to:	1***.The common security plan shall include the measures that*** Member States, ***when accessing*** data processed in the SIS II***, need to take in order*** to:
	(-a) physically protect the infrastructure and sites of the access points (NI-SIS) and the communication infrastructure between the NI-SIS and C-SIS;

	(-aa) ensure a permanent level of security by monitoring and having a clear overview of who is responsible for the security by appointing a security manager to determine the risks, an information manager to audit the data for their integrity and a network manager to be in charge of the secure network and communications infrastructure. Those managers shall be accountable to the Member States.
(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);	(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 ***and within*** 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);	(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);	(c) prevent the unauthorised accessing, reading, copying, modification or erasure of SIS II data ***during the transmission of data and*** 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);	(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);	(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) ***by granting access only to duly authorised personnel holding individual and unique user identities and confidential passwords;***
	(ea) ensure that every authority with a right of access to the SIS II develops profiles of personnel authorised to access either the premises or the SIS II itself; an up-to-date list of such personnel shall be kept and made available to the national supervisory authorities;
(f) ensure that, in using the NS, authorised persons have access only to SIS II data which fall within their competence (control	(f ensure that, in using the NS, authorised persons have access only to SIS II data which fall within their competence (control

of access);	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);	(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 ***using encryption techniques*** (control of transmission);
(h) monitor the effectiveness of the security measures ***referred to in this paragraph*** (self-auditing).	(h) monitor the effectiveness of the security measures (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.	

Or. en

Amendment by Edith Mastenbroek

Amendment 213
Article 10 a (new)

	Article 10a
	Confidentiality
	1. 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.
	2. The obligation of confidentiality shall also apply after those people leave office or employment or after the termination of the activities of those bodies.

Or. en

Amendment by Sylvia-Yvonne Kaufmann

Amendment 214
Article 10, paragraph 1, letter (h a) (new)

(ha) in the event of system crashes, guarantee the immediate recovery of the data and the integrity of data which has already been stored.

Or. de

Justification

Arrangements must also be made for dealing with technical emergencies. Since system crashes cannot be ruled out, those arrangements must cover such cases (see opinion of the Article 29 Working Party of 23 June 2005 on the VIS, p. 22).

Amendment by Edith Mastenbroek

Amendment 215
Article 11, paragraph 1

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.	1. Each Member State shall keep logs of all ***accessing of data stored in, and*** exchanges of data with, the SIS II for the purpose of monitoring the lawfulness of data processing, ***internal auditing and*** ensuring the proper functioning of the NS, data integrity and security. ***Member States using copies as referred to in Article 4(3) or copies as referred to in Article 42 shall keep logs of any processing of SIS II data within those copies, for the same purposes.***

Or. en

Amendment by Edith Mastenbroek

Amendment 216
Article 11, paragraph 2

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.	2. The logs shall show, in particular, ***the history of the alerts,*** the date and time of the data transmitted, the data used for interrogation, ***the reference to*** the data transmitted and the name of both the competent authority and the person processing the data.

Or. en

Amendment by Edith Mastenbroek

Amendment 217
Article 11, paragraph 3

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

Or. en

Amendment by Sylvia-Yvonne Kaufmann

Amendment 218
Article 11, paragraph 3

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.	3. The logs shall be protected by appropriate measures against unauthorised access and erased after a period of ***three years following erasure of the alert to which they are related. Logs may be kept for a longer period*** if they are required for monitoring procedures which have already begun.

Or. de

Justification

With reference to the rapporteur's amendment to Article 11(3), a binding provision should be laid down stipulating that logs must be kept for a period of three years. This is appropriate given the importance of such logs in connection with the monitoring of lawful access to data and, hence, the legal protection of the individuals concerned.

Amendment by Edith Mastenbroek

Amendment 219
Article 11, paragraph 4 a (new)

	4a. Each authority with a right of access to the SIS II shall have an internal monitoring structure to ensure full compliance with this Decision. Those authorities shall report regularly to the national supervisory authority.

Or. en

Amendment by Henrik Lax

Amendment 220
Article 12, paragraph 1

1. The Commission shall be responsible for the operational management of the SIS II.	1. ***During a transitional period of 3 years after the entry into force of this Decision*** the Commission shall be responsible for the operational management of the SIS II ***until the entry into force of Regulation (EC) No. XX/XXXX establishing a European Agency for the Operational Management of large-scale IT-systems***.

Or. en

Amendment by Edith Mastenbroek

Amendment 221
Article 12, paragraph 1

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

the operational management of the SIS II.	***and in particular for ensuring a smooth transition from the current system to the new system. The data stored in the current SIS may be transferred to the new system only after the current system has been audited and the integrity of the data checked.***

Or. en

Amendment by Edith Mastenbroek

Amendment 222
Article 13

Security ***and confidentiality***	Security
With reference to the operation of the SIS II, the Commission shall apply Article 10 mutatis mutandis.	***1.The Commission shall develop a common security plan for the SIS II system. That security plan shall include obligations on the Member States and the Commission.*** ***2. The Commission shall communicate the specific security guidelines to Member States and ensure that Member States apply them in full.*** ***3.This common security plan shall include the measures needing to be taken by the Commission to:*** ***(a) physically protect the infrastructure and site of the C-SIS and the communication infrastructure between the NI-SIS and C-SIS.*** ***(b) ensure a permanent level of security by monitoring and having a clear overview of who is responsible for the security by appointing a security manager to determine the risks, an information manager to audit the data for their integrity and a network manager to be in charge of the secure network and communications infrastructure; those managers shall be accountable to the Commission, which shall bear the final responsibility.*** ***(c) prevent any unauthorised person having access to installations in which operations***

relating to the C-SIS are carried out (checks at the entrance to and within the installation);

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

(e) prevent the unauthorised accessing, reading, copying, modification or erasure of C-SIS data during the transmission of data and for the transmission between the N-SIS and the C-SIS (control of transmission);

(f) granting access to the C-SIS only to duly authorised personnel holding individual and unique user identities and confidential passwords;

(g) develop profiles of personnel authorised to access either the premises or the C-SIS system itself; an up-to-date list of such personnel shall be kept and made available to the European Data Protection Supervisor;

(h) ensure that authorised persons have access only to C-SIS system and not to the data itself (control of access);

(j) ensure that data flows on the network are encrypted;

(k) monitor the effectiveness of the security (self-auditing).

4. The common security plan shall include all the measures referred to in Article 10.

Or. en

Amendment by Edith Mastenbroek

Amendment 223
Article 13 a (new)

Article 13a

Confidentiality

	1. 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.
	2. The obligation of confidentiality shall also apply after those people leave office or employment or after the termination of the activities of those bodies.

Or. en

Amendment by Sylvia-Yvonne Kaufmann

Amendment 224
Article 14, paragraph 3

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.	3. The logs shall be protected by appropriate measures against unauthorised access and erased after a period of ***three years*** following erasure of the alert to which they are related***. Logs may be kept for a longer period*** if they are required for monitoring procedures which have already begun

Or. de

Justification

See the justification for the amendment to Article 11(3).

Amendment by Edith Mastenbroek

Amendment 225
Article 14, paragraph 3

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

Or. en

Amendment by Sylvia-Yvonne Kaufmann

Amendment 226
Article 18, paragraph 2

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").	2. The European Police Office (Europol) shall have the right to access the data contained in alerts for ***the purpose of making arrests, provided such access*** 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").

Or. de

Justification

Principle of relevance: steps must be taken to ensure that Europol has access only to data contained in alerts which it needs in order to perform its tasks in accordance with the 'Europol Convention'. The purpose of this amendment is to make that clearer.

Amendment by Sylvia-Yvonne Kaufmann

Amendment 227
Article 18, paragraph 3

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

Or. de

Justification

Principle of relevance: steps must be taken to ensure that Eurojust has access only to the data continued in alerts which it needs in order to perform its tasks in accordance with Decision 2002/187/JHA. The purpose of this amendment is to make that clearer.

Amendment by Sylvia-Yvonne Kaufmann

Amendment 228
Article 19, paragraph 2

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 data of the decision giving rise to the alert. ***The Member State having entered the data into the SIS II may decide to keep it in the system, should this prove necessary for the purpose for which the data was entered.***	2. Alerts issued for arrest and the additional data referred to in Articles 16 and 17 shall automatically be erased after ***three*** years from the data of the decision giving rise to the alert. ***If after expiry of the three-year period the conditions laid down in Article 15 are still met, the Member State which originally issued the alert shall issue a fresh alert.***

Or. de

Justification

The Commission gives no justification for extending the period during which alerts may be kept in the system. The three-year period laid down in Article 112 of the Schengen implementing agreement should therefore be retained. Moreover, it is preferable to stipulate that a fresh alert must be issued if the relevant conditions are still met.

Amendment by Edith Mastenbroek

Amendment 229
Article 23, paragraph 1

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***.	1. Member States shall***, at the request of the competent administrative or judicial authority, 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 police protection***.***

Or. en

Amendment by Sylvia-Yvonne Kaufmann

Amendment 230
Article 25, paragraph 2

2. The alerts referred to in paragraph 1 shall automatically be erased after ***10*** years form	2. The alerts referred to in paragraph 1 shall automatically be erased after ***three*** years

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.***	from the date of the decision giving rise to the alert. ***If after expiry of the three-year period the conditions laid down in Article 23 are still met, the Member State which originally issued the alert shall issue a fresh alert.***

Or. de

Justification

See the justification for the amendment to Article 19(2).

Amendment by Sylvia-Yvonne Kaufmann

Amendment 231
Article 28, paragraph 3

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.	3. Eurojust shall have the right to access the data contained in alerts referred to in Article 27 ***for the purposes stated in the alerts and provided that such access is*** necessary for the performance of its tasks in accordance with Decision 2002/187/JHA.

Or. de

Justification

Data should be used only for the purposes stated in the alerts. See also the justification for the amendment to Article 18(3).

Amendment by Sylvia-Yvonne Kaufmann

Amendment 232
Article 29, paragraph 2

2. Alerts referred to Article 27 shall automatically be erased after ***10*** years from the date of the decision giving rise to the alert. ***The Member State having eneterd 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***	2. Alerts referred to Article 27 shall automatically be erased after ***three*** years from the date of the decision giving rise to the alert. ***If after expiry of the three-year period the conditions laid down in Article 27 are still met, the Member State which issued the original alert shall issue a fresh***

alert was entered.	***alert.***

Or. de

Justification

See justification for the amendment to Article 19(2).

Amendment by Edith Mastenbroek

Amendment 233
Article 31, paragraph 1

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:	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 checks ***or searches*** 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	(a) where there is clear evidence that the person concerned intends to commit or is committing numerous and extremely serious criminal offences ***as referred to in Article 2 of the Europol Convention and the Annex thereto*** 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.	(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 ***as referred to in Article 2 of the Europol Convention and the Annex thereto*** in the future.

Or. en

Amendment by Sylvia-Yvonne Kaufmann

Amendment 234
Article 33, paragraph 3

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.	3. Europol shall have the right to access to the data of the alerts referred to in Article 31 ***for the purposes stated in the alerts and provided that such access is*** necessary to perform its tasks in accordance with the Europol Convention.

Or. de

Justification

Data should be used only for the purposes stated in the alerts. See also the justification for the amendment to Article 18(2).

Amendment by Sylvia-Yvonne Kaufmann

Amendment 235
Article 37, paragraph 3

3. Europol shall have the right to access the data contained in the alerts referred to in Articles 35 ***which are*** necessary to perform its tasks in accordance with the Europol Convention.	3. Europol shall have the right to access the data contained in the alerts referred to in Articles 35 ***for the purposes stated in the alerts and provided that such access is*** necessary to perform its tasks in accordance with the Europol Convention.

Or. de

Justification

Data should be used only for the purposes stated in the alerts. See also the justification for the amendment to Article 18(2).

Amendment by Sylvia-Yvonne Kaufmann

Amendment 236
Article 39, paragraph 1, letters (d) and (e)

(d) photographs;	***Deleted***

(e) fingerprints;

Or. de

Justification

The technologies for exploiting biometric data have not yet been properly developed. However, the incorrect functioning of SIS II may have far-reaching implications for the individuals concerned, in particular where the use of such data in such a large database is concerned. As things stand, and given the expected substantial volume of data to be processed in the SIS II, security of operation cannot be guaranteed. In addition, no impact assessment has been carried out concerning the use of biometric data.

Amendment by Henrik Lax

Amendment 237
Article 39 a (new)

Article 39a

Special rules applicable to photographs and fingerprints

1. Pursuant to Article 16(1)(d) and (e), photographs and fingerprints may be used only in the following cases:

(a) photographs and fingerprints may be contained in alerts pursuant to paragraph 1 only after a special quality check has been conducted to ascertain whether they meet a minimum data quality standard, to be established pursuant to Article 35;

(b) photographs and fingerprints may be used only to confirm the identification of a third country national based on an alphanumeric search;

(c) fingerprints may be used to identify the third-country national where the person does not carry any identification or travel documents.

Or. en

Amendment by Manfred Weber

Amendment 238
Article 39 a (new)

Article 39a

As from a date to be set in accordance with Article 65, fingerprints and photographs may also be used to search and identify whether an individual is the subject of an alert in the SIS II.

Or. en

Justification

To enable biometric search if the legal and technical standards are met.

Amendment by Sylvia-Yvonne Kaufmann

Amendment 239
Article 39 a (new)

Article 39a

Searches using biometric data shall not be carried out under any circumstances.

Or. de

Justification

See the justification for the amendment to Article 39(1)(d) and (e). This amendment is intended as an adjunct to the rapporteur's amendment incorporating a new Article 3 a.

Amendment by Edith Mastenbroek

Amendment 240
Article 40, paragraph 1 a (new)

1a. All provisions under Article 10 and 13 are fully applicable to this article.

Or. en

Amendment by Sylvia-Yvonne Kaufmann

Amendment 241
Article 40, paragraph 3

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.	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. ***Such staff may only access such data as are necessary for the performance of their tasks in accordance with this Decision. National authorities shall keep an up-to-date list of persons entitled to access the SIS II. This shall also apply to Europol and Eurojust and their staff.***

Or. de

Justification

The first two sentences of the amendment take over the rapporteur's Amendment 102 to Article 40(3). Europol and Eurojust must be subject to the same arrangements as the Member States.

Amendment by Edith Mastenbroek

Amendment 242
Article 43, paragraph 7

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.	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. ***Member States shall document the reviews including the reasons for the continued conservation of data and statistics on the percentage of the alerts kept and newly entered pursuant to Articles 19(2), 25(2), 29(2), 34(3) and 28(4).***

Or. en

Amendment by Sylvia-Yvonne Kaufmann

Amendment 243
Article 46, paragraph 1

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.	1. A Member State may create a link between alerts it issues in the SIS II***, pursuant to Article 15,*** in accordance with its national legislation. The effect of such a link shall be to establish a relationship between two or more alerts. ***Links may not be created between alerts which do not serve the same objectives.***

Or. de

Justification

Links are a typical investigatory tool employed by police forces. For that reason, restrictions should be placed on the use of such a mechanism in the SIS II. Links should be consistent with the objectives of the alerts concerned; the creation of links between alerts which serve differing purposes ('Arrest and surrender on the basis of a European arrest warrant' pursuant to Article 15 of this decision, 'Alerts on objects for seizure or use as evidence in criminal proceedings' pursuant to Chapter VIII of this decision, 'Refusal of entry' pursuant to Article 15(1) of the Commission proposal for a European Parliament and Council regulation on the establishment, operation and use of the second generation Schengen information system (SIS II), COM(2005)0236) should be ruled out.

Amendment by Sylvia-Yvonne Kaufmann

Amendment 244
Article 46, paragraph 2 a (new)

	2a. Links must under no circumstances result in authorities gaining unauthorised access to data.

Or. de

Justification

Steps must be taken to ensure that links do not serve to broaden access rights (opinion of the Article 29 Working Party, p. 17).

Amendment by Edith Mastenbroek

Amendment 245
Article 46, paragraph 3

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.	3. The creation of a link shall not affect the rights to access provided for in this Regulation. Authorities with no right to access certain categories of alerts shall not have access to the links to those categories ***nor may they see the link to an alert to which they do not have access.***

Or. en

Amendment by Sylvia-Yvonne Kaufmann

Amendment 246
Article 46, paragraph 4 a (new)

	4a. Links must be erased as soon as one of the linked alerts has been erased from the system.

Or. de

Justification

Since links represent a separate category of data, there is a risk that an alert which as such has already been erased may continue to exist as a linked data category (Schengen Joint Supervisory Authority, p. 9). For the sake of legal security, links must be erased as soon as one of the linked alerts has been erased.

Amendment by Edith Mastenbroek

Amendment 247
Article 48

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.	1. The personal data processed in the SIS II in application of this Decision shall not be transferred or made available to ***a private party,*** a third country or to an international organisation.
2. By way of derogation from paragraph 1, personal data may be transferred to third	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***.	countries or international organisations if:
	(a) this transfer is provided for by EU law expressly requiring or authorising it;
	(b) an adequate level of data protection is ensured in the third country or by the international body to which the data concerned are to be transferred;
	(c) the transfer is necessary for the purpose for which the data concerned were collected.
	2a. The transfer shall be made in accordance with Article 15 of the Council Framework decision XX [on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters].

Or. en

Amendment by Edith Mastenbroek

Amendment 248
Article 48 a (new)

	Article 48a
	The SIS II may be linked to other databases only after a thorough security analysis has been conducted.

Or. en

Amendment by Edith Mastenbroek

Amendment 249
Article 54, paragraph 2

2. If the Member State against which an action is brought pursuant to paragraph 1 is not the Member State which entered the data	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.	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. ***Actions may be brought in one Member State only***.

Or. en

Justification

In order to avoid "shopping" it must be made impossible to claim for compensation in more as 1 member state

Amendment by Edith Mastenbroek

Amendment 250
Article 55

Sanctions	***Penalties and criminal offence***
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.	Member States shall ensure that processing of SIS II data or supplementary information contrary to this Regulation is subject to effective, proportionate and dissuasive ***penalties*** in accordance with national law. ***Serious infringements shall constitute a criminal offence. Member States shall include provisions to that end into their national law. They shall notify to the Commission all the provisions of their applicable national law by the date to be determined in accordance with Article 65(2) and they shall notify it without delay of any subsequent amendments thereto. The same shall apply for security breaches caused by neglect and or abuse.***

Or. en

Amendment by Edith Mastenbroek

Amendment 251
Article 64, paragraph 1 a (new)

	1. The data stored in the current SIS may be transferred to the new system only after the current system has been audited and the integrity of the data checked.

Or. en

Amendment by Edith Mastenbroek

Amendment 252
Article 64, paragraph 2

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.	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 ***used for auditing the current system and checking the data in the current system. Any outstanding amounts 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.

Or. en

Amendment by Tatjana Ždanoka

Amendment 253
Article 65, paragraph 1, introductory wording

1. This Decision shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.	This Decision shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union***, provided that the Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters Data Protection in the 3rd Pillar (Com(2005)475) has entered into force.***

Or. en

Amendment by Sylvia-Yvonne Kaufmann

Amendment 254
Article 65, paragraph 1, subparagraph 2

It shall apply from a date to be determined by the Commission in accordance with paragraphs 2 and 3.	It shall apply from a date to be determined by the Commission in accordance with paragraphs 2 and 3***, but not before Council Framework Decision 2005/XX/JHA on the protection of personal data processed in the context of police and judicial cooperation in criminal matters has entered into force.*** .

Or. de

Justification

See the justification for the amendment incorporating a new paragraph 4a into the draft legislative resolution.

Amendment by Edith Mastenbroek

Amendment 255
Article 65, paragraph 1 a (new)

	1a. The SIS II shall be brought into operation only after the successful completion of a comprehensive test of the system, the security of the system and its communication infrastructure at all levels, to be conducted by the Commission together with the Member States. The Commission shall inform the European Parliament of the results thereof. Should the test produce unsatisfactory results, that period shall be extended until the proper functioning of the system can be ensured.

Or. en

Amendment by Manfred Weber

Amendment 256
Article 65, paragraph 4 a (new)

3a. The date from which Article 39a is 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 search fingerprints and/or photographs.

Or. en

Justification

To be coherent with Art 16 a) and to enable the biometrical search if the standards are met.