EUROPEAN PARLIAMENT

2004 *2009*

Committee on Civil Liberties, Justice and Home Affairs

18.5.2006 PE 372.149v02-00

AMENDMENTS 122-208

Draft report **(PE 365.024v02-00)**
Carlos Coelho
Proposal for a regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen information system (SIS II)

Proposal for a regulation (COM(2005)0236 – C6-0174/2005 – 2005/0106(COD))

Draft legislative resolution

Amendment by Sylvia-Yvonne Kaufmann

Amendment 122
Citation 2 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.

Proposal for a regulation

Text proposed by the Commission	Amendments by Parliament

Amendment by Sylvia-Yvonne Kaufmann

Amendment 123
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 the implementation of policies linked to the movement of persons part of the Schengen acquis***.	(5) The SIS II should***, as*** a compensatory measure***, guarantee*** a high level of security within an area without internal border controls between Member States.

Or. de

Amendment by Edith Mastenbroek

Amendment 124
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 the implementation of policies linked to the movement of persons part of the Schengen acquis.	(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 the implementation of policies linked to the movement of persons part of the Schengen acquis ***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 Edith Mastenbroek

Amendment 125
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 its 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 126
Recital 7

(7) The expenditure involved in the operation of 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 127
Recital 8

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

Amendment 128
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) 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. ***The data stored within 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 129
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) ***During a transitional period of 3 years after the entry into force of this Regulation*** the Commission should be responsible for the operational management of the SIS II in

system and the start of its operations.	particular in order to ensure a smooth transition between the development of the system and the start of its operations.

Or. en

Amendment by Henrik Lax

Amendment 130
Recital 9 a (new)

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

Or. en

Amendment by Sylvia-Yvonne Kaufmann

Amendment 131
Recital 12

(12) 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.	(12) 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 16(1)(d) and (e).

Amendment by Edith Mastenbroek

Amendment 132
Recital 12

(12) 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.	(12) 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 133
Recital 13

(13) 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.	(13) 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 Carlos Coelho

Amendment 134
Recital 14

(14) Directive 1995/46/EC of the European Parliament and the Council of 24 October	(14) Directive 1995/46/EC of the European Parliament and 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 applies to the processing of personal data carried out in application of this Regulation. This includes the designation of the controller in accordance with Article 2 (d) of that Directive and the possibility for Member States to provide for exemptions and restrictions to some of the provided rights and obligations in accordance with Article 13 (1) of that Directive including as regards the rights of access and information of the individual concerned. The principles set out in Directive 1995/46/EC should be supplemented or clarified in this Regulation, where necessary.	1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data applies to the processing of personal data carried out in application of this Regulation. This includes the designation of the controller in accordance with Article 2 (d) of that Directive and the possibility for Member States to provide for exemptions and restrictions to some of the provided rights and obligations in accordance with Article 13 (1) of that Directive including as regards the rights of access and information of the individual concerned. The principles set out in Directive 1995/46/EC should be supplemented or clarified in this Regulation, where necessary. ***It is appropriate to comprehensively regulate certain data protection issues in this Regulation in order to ensure that they are applied in a uniform manner by the Member States. The provisions of Directive 95/46/EC apply in full whenever an issue is not regulated in full in this Regulation.***

Or. en

Justification

The raison d'être of this Regulation is to provide for the rules which will govern the use of the SIS II. These rules should be as comprehensive as possible to increase the clarity of the legal text and to ensure good implementation.

Amendment by Edith Mastenbroek

Amendment 135
Recital 21

(21) 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 Regulation become applicable. Some provisions of the Schengen acquis should continue to apply for a limited period of time	(21) 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

until the Member States have examined the compatibility of those alerts with the new legal framework.	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 136
Recital 21 a (new)

(21a) 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 137
Recital 21 b (new)

(21b) An overall security plan should be developed for the SIS II before the system is brought into operation. Such a 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 138
Recital 22 a (new)

	(22a) 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 139
Article 1, paragraph 1

1. A computerised information system called the second generation of the 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 to in this Regulation.***

Or. en

Amendment by Edith Mastenbroek

Amendment 140
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 shall 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 Sylvia-Yvonne Kaufmann

Amendment 141
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 142
Article 2, paragraph 2

2. This Regulation 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.	2. This Regulation also lays down provisions 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 143
Article 4, paragraph 1, point (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 144
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 145
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 on the location of

its back-up system.

Or. en

Amendment by Edith Mastenbroek

Amendment 146
Article 4 a (new)

Article 4a

The European Agency for the Operational Management of the SIS II will determine where the CS-SIS and its backup system will 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 147
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 will implement the guidelines as provided for in the overall security plan.***

Or. en

Amendment by Edith Mastenbroek

Amendment 148
Article 7, paragraph 1

1. Each Member State shall designate ***an*** office which shall ensure competent	1. Each Member State shall designate ***a SIS II national*** office***, under the clear***

authorities' access to the SIS II in accordance with this Regulation.	***responsibility of the Member State,*** which shall ***bear the central responsibility for the national system, be responsible for the smooth operation and security of the national system and*** ensure competent authorities' access to the SIS II in accordance with this Regulation.

Or. en

Amendment by Edith Mastenbroek

Amendment 149
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 150
Article 9, paragraph 3

3. ***Where relevant,*** Member States shall ensure that 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 that 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 151
Article 9, paragraph 3 a (new)

	3a. Member States shall ensure that the authorities accessing the data of the copy will only be able to see the information,

alerts and links they are entitled to see.

Or. en

Amendment by Edith Mastenbroek

Amendment 152
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.

Or. en

Amendment by Edith Mastenbroek

Amendment 153
Article 10

Security ***and confidentiality***	Security
	-1. Member States shall implement the security guidelines as adopted in the common security plan.
1. Member States ***having access to*** data processed in the SIS II ***shall take the necessary measures to***:	1. ***This common security plan shall include the measures that*** Member States***, when accessing*** data processed in the SIS II, ***need to take in order to***:
	(-aa) physically protect the infrastructure and sites of the access points (NI-SIS) and the communication infrastructure between the NI-SIS and C-SIS;
	(-ab) 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 who determines the risks, an information manager who audits the data for their integrity and a network manager who is in charge of the secure network and communications infrastructure. A Member State will be able to hold these managers accountable;

(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 ***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 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 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 only***;
	(ea) ensure that all authorities with a right of access to the SIS II develop profiles of personnel authorised to access either the premises or SIS II itself. An up-to-date list will be maintained 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 of access);	(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);	(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 ***while 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 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.	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 Sylvia-Yvonne Kaufmann

Amendment 154
Article 10, paragraph 1, point (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 155
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 Edith Mastenbroek

Amendment 156
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 23 shall keep logs of any processing of SIS II data within those copies, for the same purposes***.

Or. en

Amendment by Edith Mastenbroek

Amendment 157
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 transmitted 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 Carlos Coelho

Amendment 158
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 from the date of the erasure of the alert to which they refer. The logs that include the history of the alerts shall be erased after a period of three years from the date of the erasure of the alert to which they refer. Logs may be kept for longer*** if they are required for monitoring procedures which have already begun.

Or. en

(Modifies AM 33)

Justification

A one-year storage period for the logs is too short. A longer period would allow checking for a longer time whether data was accessed unlawfully and therefore guarantees better protection of citizens. It is therefore proposed to allow Member States to keep the logs for three years which is the maximum period currently allowed in the SIC. At the same time, it is important to state exactly when this period begins.

Amendment by Edith Mastenbroek

Amendment 159
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 year***s, if they are not required for monitoring procedures which have already begun.

Or. en

Amendment by Edith Mastenbroek

Amendment 160
Article 11 a (new)

	Article 11a
	Internal auditing
	Each authority with a right of access to the SIS II shall have an internal monitoring structure to ensure full compliance with this Regulation. Each authority shall report regularly to the national supervisory authority.

Or. en

Amendment by Edith Mastenbroek

Amendment 161
Article 12, paragraph 1

1. The Commission shall be responsible for the operational management of the SIS II.	1. The Commission shall be responsible for 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 within the current SIS can only be transferred into the new system after auditing the current system and verifying the integrity of the data.***

Or. en

Amendment by Henrik Lax

Amendment 162
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 the present Regulation*** 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 163
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 European Commission will develop a common Security Plan for the SISII system. This Security Plan will consist of obligations for both Member States as the European Commission.***
	2. The European Commission will communicate the specific security guidelines for Member States and assure that Member States apply them fully.
	3. This common security plan will include; the European Commission taking the necessary measures 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 who determines the risks, an information manager who audits the data for their integrity and a network manager who is in charge of the secure network and communications infrastructure. The Commission will be able to hold these managers accountable but will 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 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 only;

(g) develop profiles of personnel authorised to access either the premises or the C-SIS system itself. An up-to-date list will be maintained and made available to the European Data Protection Supervisor;

(h) ensure that, authorised persons have access only to C-SIS system and not 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 will include all the provisions as identified in Article 10.

Or. en

Amendment by Edith Mastenbroek

Amendment 164
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 Edith Mastenbroek

Amendment 165
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 Carlos Coelho

Amendment 166
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 from the date of the*** erasure of the alert to which they ***refer. The logs that include the history of the alerts shall be erased after a period of three years from the date of the erasure of the alert to which they refer. Logs may be kept for longer*** if they are required for monitoring procedures which have already begun.

Or. en

(Modifies AM 44)

Justification

See justification for amendment to Article 11(3).

Amendment by Manfred Weber

Amendment 167
Chapter IV, Title

Alerts issued in respect of third country nationals ***for the purpose of refusing entry***	Alerts issued in respect of third country nationals

Or. de

Justification

The structure of Chapter IV should be revised, as outlined here, so that it can also cover alerts issued in respect of third country nationals which deal with the legalisation of residence status.

Amendment by Manfred Weber

Amendment 168
Article 15, Title

Objectives and conditions for issuing alerts	Objectives and conditions for issuing alerts ***for the purpose of refusing entry to third country nationals***

Or. de

Justification

Makes clear that this article deals only with negative alerts.

Amendment by Tatjana Ždanoka

Amendment 169
Article 15, paragraph 1

1. Member States shall issue alerts in respect of third country nationals for the purpose of refusing entry into the territory of the Member States on the basis of a decision defining the period of refusal of entry taken by the competent ***administrative or*** judicial authorities, in the following cases:	1. Member States shall issue alerts in respect of third country nationals for the purpose of refusing entry into the territory of the Member States on the basis of a decision defining the period of refusal of entry taken by the competent judicial authorities, ***only*** in the following cases:
(a) if the presence of the third country national in the territory of a Member State represents a serious threat to public policy or	(a) if the presence of the third country national in the territory of a Member State represents a serious threat to public policy or

public security of any Member State based on an individual assessment***, in particular if***:	public security of any Member State based on an individual assessment, ***in the following cases***:
(i) the third country national has been sentenced to a penalty involving deprivation of liberty of at least one year following a conviction of offence referred to in Article 2 (2) of Council Framework Decision 2002/584/JHA on the European arrest warrant and the surrender procedures between Member States;	(i) the third country national has been sentenced ***in a EU Member State*** to a penalty involving deprivation of liberty of at least one year following a conviction of offence referred to in Article 2 (2) of Council Framework Decision 2002/584/JHA on the European arrest warrant and the surrender procedures between Member States;
(b) if the third country national is the subject of a re-entry ban in application of a return decision or removal order taken in accordance with Directive 2005/XX/EC[on Return] .	(b) if the third country national is the subject of a re-entry ban in application of a return decision or removal order taken in accordance with Directive 2005/XX/EC[on Return] ***in case of refusal of voluntary return by the third country national***.

Or. en

Amendment by Carlos Coelho

Amendment 170
Article 15, paragraph 1, introductory wording

1. ***Member States shall issue*** alerts in respect of third country nationals for the purpose of refusing entry into the territory of the Member States on the basis of a decision defining the period of refusal of entry taken by the competent administrative or judicial authorities, in the following cases:	1. Alerts in respect of third country nationals for the purpose of refusing entry into ***or stay within*** the territory of the Member States ***shall be issued*** on the basis of a ***national alert stemming from a decision taken by the Member State's*** competent administrative or judicial authorit***y in accordance with national law,*** in the following cases:

Or. en

Justification

The amendment reintroduces part of the current Article 96(1) SIC in order to ensure an equivalent level of security as today. In addition, the rapporteur wishes for harmonisation in respect of SIS II alerts, which should always be based on a national alert. Harmonising national alerts would not, however, be appropriate. The word 'stay' is also added in order to make it clear that a third-country national can also be monitored within the territory of a Member State with a view to establishing whether or not he is in a legal situation within the territory, or before a residence permit is issued.

Amendment by Henrik Lax

Amendment 171
Article 15, paragraph 1, introductory wording

1. ***Member States shall issue*** alerts in respect of third country nationals for the purpose of refusing entry into the territory of the Member States on the basis of a ***decision defining the period of refusal of entry taken by the*** competent administrative or judicial ***authorities,*** in the following cases:	1. Alerts in respect of third country nationals for the purpose of refusing entry into ***or residence within*** the territory of the Member States ***shall be issued in a harmonised manner*** on the basis of a ***national alert stemming from a decision taken by the Member State's*** competent administrative or judicial ***authority in accordance with national law,*** in the following cases:

Or. en

Amendment by Manfred Weber

Amendment 172
Article 15, paragraph 1, point (a), introductory part

(a) if the presence of the third country national in the territory of a Member State represents a ***serious*** threat to public policy or public security of any Member State based on an individual assessment, in particular if:	(a) if the presence of the third country national in the territory of a Member State represents a threat to public policy or public security of any Member State based on an individual assessment, in particular if:

Or. de

Justification

For the sake of consistency with the following amendment.

Amendment by Manfred Weber

Amendment 173
Article 15, paragraph 1, point (a), point (i)

(i) the third country national has been ***sentenced to a penalty involving deprivation of liberty of at least one year following a conviction of offence referred***	(i) the third country national has been ***convicted of an offence which carries a penalty involving imprisonment or deprivation of liberty of a maximum of at***

to in Article 2(2) of Council Framework Decision 2002/584/JHA on the European arrest warrant and the surrender procedures between Member States;	***least one year***;

Or. de

Justification

The purpose of the amendment is to expand the provision to cover offences punishable by a suspended term of imprisonment of at least one year and to clarify the issue of minimum or maximum penalties.

Amendment by Manfred Weber

Amendment 174
Article 15, paragraph 1, point (a), point (ii) a (new)

(iia) there are justified grounds for suspecting that the third country national has committee serious offences, including those covered by Article 71 of the Schengen Convention, or there is firm evidence to suggest that he or she is planning such offences in the territory of a Member State;

Or. de

Justification

For the sake of consistency with Article 96(2)(b) of the Schengen Convention.

Amendment by Henrik Lax

Amendment 175
Article 15, paragraph 1 a (new)

1a. Such decisions may be taken only on the basis of an individual assessment, which shall be documented and founded on points of fact and law.

Or. en

Amendment by Tatjana Ždanoka

Amendment 176
Article 15, paragraph 2 a (new)

2a. While applying such provisions, Member States shall ensure full respect of non-refoulement principle.

Or. en

Amendment by Edith Mastenbroek

Amendment 177
Article 15, paragraph 3 a (new)

3a. Where the decision to issue an alert is taken, the information to the third country national will be provided immediately after the measure resulting in entry of the alert in the SIS II is adopted.

Or. en

Amendment by Sylvia-Yvonne Kaufmann

Amendment 178
Article 16, paragraph 1, points (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 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 Edith Mastenbroek

Amendment 179
Article 16, paragraph 1, point (i), indent 2

- a return decision and/or removal order accompanied by a re-entry ban;	***deleted***

Or. en

Amendment by Edith Mastenbroek

Amendment 180
Article 16, paragraph 1, point (j)

(j) link(s) to other alerts processed in the SIS II.	(j) link(s) to other alerts processed in the SIS II ***pursuant to article 26***.

Or. en

Amendment by Manfred Weber

Amendment 181
Article 16, paragraph 3 a (new)

	3a. Member States may at any time issue the third country national illegally present in their territory with a residence permit. Irrespective of whether his/her name already appears in SIS II, this item of information shall then be entered as an alert.

Or. de

Justification

In keeping with the return directive, information concerning the legalisation of the status of illegally resident third country nationals should be entered in SIS II. This is necessary both to protect such persons when controls are carried out and to ensure that information is exchanged among the Member States. For that reason, the new Article 16a deals with alerts relating to legalisation of status.

Amendment by Sylvia-Yvonne Kaufmann

Amendment 182
Article 16 a (new)

Article 16a

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

Or. de

Justification

See the justification for the amendment to Article 16(1)(d) and (e). This amendment is intended as an adjunct to the rapporteur's amendment introducing a new Article 16a.

Amendment by Manfred Weber

Amendment 183
Article 16 a (new)

Article 16a

From a date to be set in accordance with Article 39, fingerprints and photographs may also be used to search and identify whether an individual is subject to an alert in the SIS II.

Or. en

Justification

To enable biometrical search in the SIS II if the legal and technical requirements are met.

Amendment by Henrik Lax

Amendment 184
Article 16 a (new)

Article 16a

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 185
Article 17, paragraph 1, points (a)

(a) authorities ***responsible for control of persons at the external borders of the Member States***;	(a) ***border protection and customs*** authorities ***and police and other law enforcement authorities taking action under Title VI of the Treaty on European Union***;

Or. de

Justification

Makes the article clearer.

Amendment by Carlos Coelho

Amendment 186
Article 18, paragraph 1

1. Access to the alerts issued in accordance with Article 15 (1) ***(b)*** shall be given to the authorities responsible for the ***implementation of Directive 2005/XX/EC***	1. Access to the alerts issued in accordance with Article 15 (1) shall be given to the authorities responsible for the ***identification of*** third country ***nationals*** staying illegally in

for the purpose of identifying a third country ***national*** staying illegally in the territory in order to enforce a return decision or removal order.	the territory in order to enforce a return decision or removal order***, including police and customs authorities responsible for checks carried out within the territory***.

Or. en

Justification

The situation can arise that a third-country national in respect of whom an alert is entered in the SIS II for the purpose of refusing entry nevertheless is in the territory of a Member State illegally. The police should therefore have the possibility to use the SIS II in order to identify such persons.

Amendment by Tatjana Ždanoka

Amendment 187
Article 18, paragraph 3

3. Access to the alerts issued in accordance with Article 15 (1) (a) shall be given to the authorities responsible for the implementation of Directive 2004/83/EC and Directive 2005/XX/EC [on minimum standards on procedures in Member States for granting and withdrawing refugee status] for the purpose of determining whether a third country national represents a threat to public order or internal security.	***deleted***

Or. en

Amendment by Tatjana Ždanoka

Amendment 188
Article 20 a (new)

	Article 20a
	The application of the provisions of chapter IV of this regulation shall cease three years after the entry into force of this Regulation. Acting on a proposal from the Commission, the European Parliament and the Council may extend the period of validity of the provisions of chapter IV, in accordance with the procedure referred to in Article

251 of the Treaty, and with that aim in view, shall review those provisions prior to expiry of the three-year period.

Or. en

Justification

The amendment proposes a review clause for the alerts for the purpose of refusing entry. The practical application of its provisions should be looked at and if necessary amendments introduced.

Amendment by Edith Mastenbroek

Amendment 189
Article 24, 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 and statistics about the percentage of the alerts kept and newly entered pursuant to Article 20(5).***

Or. en

Amendment by Edith Mastenbroek

Amendment 190
Article 26, paragraph 3

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.	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 will be able to see the link to an alert to which they do not have access***.

Or. en

Amendment by Edith Mastenbroek

Amendment 191
Article 27 a (new)

Article 27a

Transfer of personal data to third parties

1. The personal data processed in the SIS II in application of this Regulation shall not be transferred or made available to private parties.

2. The transfer or the availability of personal data processed in the SIS II in application of this Regulation to a third country or to an international organisation shall be in accordance with article 25 and 26 of Directive 1995/46(EC).

Or. en

Amendment by Edith Mastenbroek

Amendment 192
Article 27 b (new)

Article 27b

The interlinking of the SIS II with other databases can only occur after a thorough security analysis.

Or. en

Amendment by Edith Mastenbroek

Amendment 193
Article 29, paragraph 1

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.	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 ***and according to Directive***

95/46/EC.

Or. en

Amendment by Carlos Coelho

Amendment 194
Article 31 b (new)

Article 31b

Joint responsibilities

1. The national supervisory authorities referred to in Article 31 and the European Data Protection Supervisor shall cooperate actively in the framework of their responsibilities with each other and bear joint responsibility for the supervision of SIS II.

2. They shall exchange relevant information, conduct joint investigations, including joint audits and inspections, examine difficulties of interpretation or application of this Regulation, study problems with the exercise of independent supervision or in the exercise of the rights of the data subject, draw up harmonised proposals for joint solutions to any problems and promote awareness of data protection rights, as may be needed.

3. The European Data Protection Supervisor and the national supervisory authorities shall meet for that purpose at least twice a year. The costs of these meetings shall be borne by the European Data Protection Supervisor. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly according to need. A joint report of activities shall be sent to the European Parliament, the Council and the Commission every two years.

Or. en

Justification

Given the nature of the system supervision can only work if undertaken jointly.

This proposed description of tasks is based on Article 115 SIC which has proven its usefulness and current practice.

The amendment is based on the idea that certain basic rules must be laid down in this legal text. The remaining details must be decided upon by the EDPS and the national supervisory authorities.

Amendment by Edith Mastenbroek

Amendment 195
Article 32, 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 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 Regulation.	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 Regulation. ***One can only file a request for compensation as referred to in paragraph 1 in one Member State.***

Or. en

Justification

In order to avoid "shopping" it must be made impossible to claim for compensation in more than 1 Member State.

Amendment by Edith Mastenbroek

Amendment 196
Article 33

Sanctions	***Penalties and criminal offence***
Member States shall ensure that processing of SIS II data or supplementary information contrary to this Regulation 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 this end into their national law. They shall notify all their provisions of their national law applicable to the Commission by the date of the notification referred to in Article 39(2) and shall notify it without delay of any subsequent amendment affecting them. The same will apply for security breaches caused by neglect and or abuse.

Or. en

Amendment by Edith Mastenbroek

Amendment 197
Article 34, paragraph 1

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.	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***, security*** and quality of service.

Or. en

Amendment by Edith Mastenbroek

Amendment 198
Article 34, paragraph 3

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.	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 ***lawfulness of processing, the technical functioning and security of the SIS II*** and on the bilateral and multilateral exchange of supplementary information between Member States. ***It shall be examined by the European Parliament and the Council. Member States shall answer any questions raised by the institutions in that context.***

Or. en

Amendment by Edith Mastenbroek

Amendment 199
Article 34, paragraph 4

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.	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***, the lawfulness of processing, the security of the system*** 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.

Or. en

Amendment by Edith Mastenbroek

Amendment 200
Article 38, paragraph 1 a (new)

	1a. The data stored within the current SIS can only be transferred into the new system after auditing the current system and verifying the integrity of the data.

Or. en

Amendment by Edith Mastenbroek

Amendment 201
Article 38, paragraph 2

2. The remainder of the budget at the date set in accordance with Article 39 (2), which	***2.*** The remainder of the budget at the date set in accordance with Article 39 (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.	has been approved in accordance with Article 119 of the Schengen Convention, shall be ***used for auditing the current system and verifying the data in the current system. Any remainder of the budget will 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 Edith Mastenbroek

Amendment 202
Article 39, paragraph 1 a (new)

	1a. The SIS II shall start to operate only after the successful completion of a comprehensive test of the system, the security of the system and its communication infrastructure on all levels, to be conducted by the Commission together with the Member States. The Commission shall inform the European Parliament of the results thereof. In case the tests produces unsatisfactory results that period shall be extended until the correct functioning of the system can be ensured.

Or. en

Amendment by Manfred Weber

Amendment 203
Article 39, paragraph 3 a (new)

	3a. The date from which Article 16a 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 guarantee the quality of the data entered and make sure all member states are on the same technical standard and meet the legal requirements.

Amendment by Sylvia-Yvonne Kaufmann

Amendment 204
Artikel 18 Absatz 3

3. Zugriff auf Ausschreibungen nach Artikel 15 Absatz 1 Buchstabe a erhalten die für die Umsetzung der Richtlinie 2004/83/EG ***und der Richtlinie 2005/XX/EG [über Mindestnormen für Verfahren in den Mitgliedstaaten zur Zuerkennung oder Aberkennung der Flüchtlingseigenschaft]*** zuständigen Behörden, damit sie bestimmen können, ob von einem Drittstaatsangehörigen eine Gefahr für die öffentliche Ordnung oder die innere Sicherheit ausgeht.	3. Zugriff auf Ausschreibungen nach Artikel 15 Absatz 1 Buchstabe a erhalten die für die Umsetzung der Richtlinie 2004/83/EG zuständigen Behörden, damit sie bestimmen können, ob von einem Drittstaatsangehörigen eine Gefahr für die öffentliche Ordnung oder die innere Sicherheit ausgeht.

Or. de

Justification

Die im Kommissionsvorschlag genannte Richtlinie über gemeinsame Normen und Verfahren in den Mitgliedstaaten zur Rückführung illegal aufhältiger Drittstaatsangehöriger ist am 1. September 2005 von der Kommission vorgeschlagen worden. Solange die Richtlinie jedoch nicht verabschiedet ist, kann sie nicht Grundlage für die Eingabe von Daten ins SIS II sein. Dies würde insbesondere gegen Artikel 8 EKMR verstoßen, wonach ein Eingriff in die Privatsphäre gesetzlich vorgesehen sein muss. Voraussetzung hierfür sind präzise und zugängliche Gesetze. Der Einzelne muss wissen können, welche Maßnahmen eine Behörde ihm gegenüber ergreifen kann (siehe Stellungnahme des Europäischen Datenschutzbeauftragten, S. 14).

Amendment by Sylvia-Yvonne Kaufmann

Amendment 205
Artikel 20 Absatz 5

5. Die Ausschreibungen werden ***fünf*** Jahre nach Erlass einer Entscheidung nach Artikel 15 Absatz 1 automatisch gelöscht. ***Die Mitgliedstaaten, die die Daten in das SIS II eingegeben haben, können beschließen, die Ausschreibungen im System zu belassen, wenn die Bedingungen von Artikel 15 erfüllt sind.***	5. Die Ausschreibungen werden ***drei*** Jahre nach Erlass einer Entscheidung nach Artikel 15 Absatz 1 automatisch gelöscht. ***Sind nach Ablauf der drei Jahre die Bedingungen von Artikel 15 weiterhin erfüllt, veranlasst der Mitgliedstaat, der die Ausschreibung ursprünglich veranlasst hat, eine neue Ausschreibung.***

Or. de

Justification

Die Kommission gibt keine Begründung für eine verlängerte Belassung der Ausschreibungen im System. Es sollte daher die derzeitig im Schengener Durchführungsübereinkommen vorgesehene Frist von drei Jahren beibehalten werden. Darüber hinaus ist es vorzugswürdig, dass bei weiterem Vorliegen der Ausschreibungsbedingungen nach Artikel 15 eine neue Ausschreibung vorgenommen werden muss.

Amendment by Sylvia-Yvonne Kaufmann

Amendment 206
Artikel 26 Absatz 1

1. Ein Mitgliedstaat kann nach Maßgabe des innerstaatlichen Rechts von ihm im SIS II eingegebene Ausschreibungen miteinander verknüpfen. Durch eine solche Verknüpfung werden zwei oder mehr Ausschreibungen miteinander verbunden.	1. Ein Mitgliedstaat kann nach Maßgabe des innerstaatlichen Rechts von ihm ***nach Artikel 15*** im SIS II eingegebene Ausschreibungen miteinander verknüpfen. Durch eine solche Verknüpfung werden zwei oder mehr Ausschreibungen miteinander verbunden. ***Die Verknüpfung mit Ausschreibungen, die nicht unter Artikel 15 fallen, ist nicht möglich.***

Or. de

Justification

Verknüpfungen sind ein typisches Mittel polizeilicher Fahndungssysteme. Daher sollte ein solcher Mechanismus im SIS II restriktiv angewandt werden. Verknüpfungen sollten sich innerhalb der jeweiligen Ausschreibungsziele halten; die Verknüpfung von Ausschreibungen, die unterschiedlichen Zwecken dienen ("Verweigerung der Einreise" nach Artikel 15 Absatz 1 dieser Verordnung, "Verhaftung und Übergabe mit Europäischem Haftbefehl" nach Artikel

15, "Sachfahndungsausschreibungen zur Sicherstellung oder Beweissicherung in Strafverfahren" nach Kapitel VIII des Kommissionsvorschlags für einen Beschluss des Rates über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) KOM(2005)0236), sollten ausgeschlossen werden.

Amendment by Sylvia-Yvonne Kaufmann

Amendment 207
Artikel 26 Absatz 2 a (neu)

2a. Verknüpfungen dürfen keinesfalls zur Folge haben, dass Behörden Zugriff auf Daten erhalten, zu denen sie keine Zugangsberechtigung haben.

Or. de

Justification

Es muss gewährleistet werden, dass durch Verknüpfungen keine Ausweitung von Zugangsrechten geschaffen wird (Stellungnahme der Artikel-29-Datenschutzgruppe, S. 17).

Amendment by Sylvia-Yvonne Kaufmann

Amendment 208
Artikel 26 Absatz 4 a (neu)

4a. Verknüpfungen müssen sofort gelöscht werden, sobald eine der verknüpften Ausschreibungen aus dem System gelöscht wurde.

Or. de

Justification

Da Verknüpfungen eine eigene Datenkategorie darstellen, besteht die Gefahr, dass eine Ausschreibung, die als solche bereits gelöscht ist, als verknüpfte Datenkategorie weiter besteht (Gemeinsames Kontrollgremium Schengen, S. 9). Aus Gründen der Rechtssicherheit müssen Verknüpfungen umgehend gelöscht werden, sobald eine der verknüpften Ausschreibungen gelöscht wurde.