

EUROPEAN PARLIAMENT

2004



2009

Committee on Civil Liberties, Justice and Home Affairs

PROVISIONAL
2005/0106(COD)

31.3.2006

*****I**

DRAFT REPORT

on the 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)
(COM(2005)0236 – C6-0174/2005 – 2005/0106(COD))

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Carlos Coelho

Symbols for procedures

- * Consultation procedure
majority of the votes cast
- **I Cooperation procedure (first reading)
majority of the votes cast
- **II Cooperation procedure (second reading)
*majority of the votes cast, to approve the common position
majority of Parliament's component Members, to reject or amend
the common position*
- *** Assent procedure
*majority of Parliament's component Members except in cases
covered by Articles 105, 107, 161 and 300 of the EC Treaty and
Article 7 of the EU Treaty*
- ***I Codecision procedure (first reading)
majority of the votes cast
- ***II Codecision procedure (second reading)
*majority of the votes cast, to approve the common position
majority of Parliament's component Members, to reject or amend
the common position*
- ***III Codecision procedure (third reading)
majority of the votes cast, to approve the joint text

(The type of procedure depends on the legal basis proposed by the Commission.)

Amendments to a legislative text

In amendments by Parliament, amended text is highlighted in ***bold italics***. Highlighting in *normal italics* is an indication for the relevant departments showing parts of the legislative text for which a correction is proposed, to assist preparation of the final text (for instance, obvious errors or omissions in a given language version). These suggested corrections are subject to the agreement of the departments concerned.

CONTENTS

	Page
DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION	5
EXPLANATORY STATEMENT	54

DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION

on the 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)
(COM(2005)0236 – C6-0174/2005 – 2005/0106(COD))

(Codecision procedure: first reading)

The European Parliament,

- having regard to the Commission proposal to the European Parliament and the Council (COM(2005)0236)¹,
 - having regard to Article 251(2) and Articles 62(2)(a) and 66 of the EC Treaty, pursuant to which the Commission submitted the proposal to Parliament (C6-0174/2005),
 - having regard to Rule 51 of its Rules of Procedure,
 - having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs and the opinion of the Committee on Budgets (A6-0000/2005),
1. Approves the Commission proposal as amended;
 2. Calls on the Commission to refer the matter to Parliament again if it intends to amend the proposal substantially or replace it with another text;
 3. Instructs its President to forward its position to the Council and Commission.

Text proposed by the Commission

Amendments by Parliament

Amendment 1 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 ***public order and internal security in the territories of the Member States and to applying the provisions of Title IV of the EC Treaty relating to the free movement of persons in those territories using information communicated via this system.***

Justification

See justification for amendment to Article 1.

¹ OJ C ... / Not yet published in OJ.

Amendment 2
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*** 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.

Amendment 3
Recital 9 a (new)

(9a) At a later stage the operational management should be the responsibility of a European Agency for the Operational Management of large-scale IT-systems.

Justification

See justification for amendment to Article 12(1).

Amendment 4
Recital 11

(11) Alerts aiming at refusing entry should not be kept longer in the SIS II than the period of refusal of entry set out in the national decision giving rise to the alert. As a general principle, they should be automatically erased from the SIS II after a maximum period of **five years**. Member States should review at least **annually** these alerts.

(11) Alerts aiming at refusing entry should not be kept longer in the SIS II than the period of refusal of entry set out in the national decision giving rise to the alert. As a general principle, they should be automatically erased from the SIS II after a maximum period of **three years**. ***That period may be extended for a further two years if the conditions for the entry of the alert continue to be fulfilled.*** Member States should review at least **every two years** these alerts.

Justification

See justifications for amendments to Article 20(5) and 20(7).

Amendment 5
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 between alerts should have no impact on the action to be taken, the conservation period or the access rights to the alerts.

Amendment 6
Recital 14

(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.

(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. ***Whenever an issue is comprehensively regulated in this Regulation, the provisions of this Regulation should take precedence over the provisions of Directive 1995/46/EC.***

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 7
Recital 16

(16) It is appropriate that national

(16) It is appropriate that national

independent supervisory authorities monitor the lawfulness of the processing of personal data by the Member States, whilst the European Data Protection Supervisor should monitor the activities of the Commission in relation to the processing of personal data.

independent supervisory authorities monitor the lawfulness of the processing of personal data by the Member States, whilst the European Data Protection Supervisor should monitor the activities of the Commission in relation to the processing of personal data, ***taking into account the limited task of the Commission with regard to the data themselves.***

Justification

The duties and powers of the European Data Protection Supervisor (EDPS) apply to the data processing activities of the Commission. The magnitude and extent of these activities therefore also determine the magnitude and extent of the EDPS's role.

Amendment 8
Recital 20

(20) The measures necessary for the implementation of this Regulation should be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission . ***deleted***

Justification

See justification for amendments to Article 35

Amendment 9
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 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 ***stipulated in this Regulation.***

Justification

The amendment seeks to clarify the text: The proposed wording 'controls on persons and objects' seems to be too vague and does not adequately reflect the content of the Regulation. 'The purposes' the amendment refers to are outlined already precisely in the Commission's

proposal (see for example Articles 15(1), 17(1), 18).

Amendment 10
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 - in accordance with this Regulation - to maintain public order and a high level of internal security in the territories of the Member States and to apply the provisions of Title IV of the Treaty establishing the European Community as regards the free movement of persons in those territories using information communicated via this system.**

Justification

The amendment reintroduces part of the current Article 93 of the Schengen Implementing Convention (SIC). This text was chosen because it reflects with greater accuracy the purpose of the SIS II.

Amendment 11
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 **in particular** 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.

Justification

The words 'in particular' are inserted in order to reflect the fact that other topics also fall within the scope of this Regulation.

Amendment 12
Article 3, paragraph 1, point (a)

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

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

Justification

The present regulation does not cover objects.

Amendment 13
Article 4 a (new)

Article 4a

Location

The main Central Schengen Information System shall be located in Strasbourg (France) and its back-up system in Sankt Johann im Pongau (Austria).

Justification

The rapporteur is of the opinion that the question of the location can be separated from the question of who will be responsible for the operational management. As to the location it appears to be the most logical choice to locate the SIS II where the current system is located and to provide for back-up facilities. The operational management of the SIS II irrespective of location has to be, however, the responsibility of the Commission until a Community agency has been set up for this purpose. See also the amendments on the operational management later.

Amendment 14
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.

Justification

One could understand the proposal of the Commission in the sense that the responsibility of the Member States is limited to 'operating' and 'maintaining'. The amendment seeks to exclude any ambiguity.

Amendment 15
Article 7, title

SIS II national office and SIRENE ***authorities***

SIS II national office and SIRENE ***authority***

Amendment 16
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 Regulation.

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

Justification

The SIS II national office will have primarily technical responsibilities and will therefore have a more technical profile than the SIRENE authorities. The amendment seeks to define these technical responsibilities in more detail. It is also added that this office shall have the central responsibility. Such a provision was foreseen in Article 108 SIC but not included by the Commission in its proposal (see also JSA, p. 14).

Amendment 17
Article 7, paragraph 2

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

2. Each Member State shall designate the **authority** which shall ensure the exchange of all supplementary information, hereinafter referred to as the "SIRENE **authority**". **Each Member State shall issue its alerts via this authority which shall also ensure** the quality of the information entered into the SIS II **and take the necessary measures to ensure compliance with the provisions of this Regulation.** For those purposes **it** shall have access to data processed in the SIS II.

Justification

In contrast to the technical tasks of the SIS II national office the SIRENE authority will be dealing with the content of the SIS II and have consequently a "police profile". The following modifications are proposed in comparison to the Commission's text:

- Use of the singular: Per Member State there should only be one SIRENE authority and not several.*
- That authority shall issue alerts.*
- Given the profile and tasks of the SIRENE authorities it appears appropriate to entrust them also with the responsibility to ensure compliance with the provisions of this Regulation*

Amendment 18
Article 7, paragraph 3

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

3. The Member States shall inform each other and the Commission of the office referred to in paragraph 1 and of the SIRENE **authority** referred to in paragraph 2. **The Commission shall publish the list thereof, together with the list referred to in Article 21(3).**

Justification

For transparency reasons it is preferable that the list of these authorities be published as well. Since most of this information can currently be found on the Internet, this should not pose any particular problems for Member States.

Amendment 19
Article 8, paragraph 1

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

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

Justification

The article gives a general description of the tasks of the SIRENE authorities. The part inserted by the amendment is taken from Article 92(4) SIC because it appears to be a useful clarification.

Amendment 20
Article 8, paragraph 1 a (new)

1a. Requests for supplementary information made by other Member States shall be answered as quickly as possible and at any event within 12 hours.

Justification

The reaction time can be of considerable importance for the persons concerned. Currently the

SIRENE Manual foresees a 12-hour reaction time (see part 2.2.1(a)). See also justification for amendment to Article 24(5).

Amendment 21
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, **as referred to in Articles 4(3) and 23(1), which leads to data stored on line** is at all times identical and consistent with the CS-SIS.

Justification

This is relevant only in the case of the copies referred to in the text. The amendments seek to clarify this (see also JSA p. 14).

Amendment 22
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 **as referred to in Articles 4(3) and 23(1) which leads to data stored on line** produces the same result as a search performed directly in the CS-SIS.

Justification

Since copies are used for purely technical reasons, searches other than those of the kind possible at central level should not be permitted (see also JSA, p. 15). The rapporteur considers it equally important that a search in a copy should produce the same result as a search in the central system. This is even more relevant since no searches with biometric data are foreseen.

Amendment 23
Article 9, paragraph 3 a (new)

3a. Where Member States make use of copies as referred to in Article 23(1a) they shall ensure that a search in copies of the data of the CS-SIS may be made only with the same search criteria as those used for searching the CS-SIS.

Amendment 24
Article 9(3b) (new)

3b. Each year the Member States shall carry out a 'benchmarking test' using a list of cases (data to be tested) and of the results or hits obtained by means of the CS-SIS search mechanism, which shall provide a basis for a comparison with the results obtained in each national system.

Justification

This test will serve to prove that a search carried out in each Member State's national copy produces the same results as a search carried out directly on the CS-SIS.

Amendment 25
Article 10, paragraph 1, point (aa) (new)

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

Justification

This has been considered an important safeguard for handling the potential risks related to the infrastructure of the system and ensuring a high security level for the SIS II.

Amendment 26
Article 10, paragraph 1, point (c)

(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*** between the NS and the SIS II, ***in particular by appropriate encryption techniques*** (control of ***transport***);

Justification

The modifications of the wording are largely taken from the Commission's VIS proposal which seems to be much clearer on this point. The obligation for encryption is added.

Amendment 27
Article 10, paragraph 1, point (d)

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

Justification

It is important to ensure that the purpose of data processing can also be checked.

Amendment 28

Article 10, paragraph 1, point (d a) (new)

(da) ensure that the SIS II may be accessed only by duly authorised personnel holding individual and unique user identities and confidential passwords;

Justification

These measures are recommended by the Article 29 Working Party (Article 29 WP) (p. 19) and are intended to increase the security of the system.

Amendment 29

Article 10, paragraph 1, point (d b) (new)

(db) ensure that all the authorities with a right of access to the SIS II develop profiles of personnel authorised to access SIS II and maintain an up-to-date list of that personnel, which shall be made available to the national supervisory authorities;

Justification

Both the EDPS (p. 21) and the Article 29 WP (p. 19) stressed the necessity of creating precise user profiles and a complete up-to-date list of such personnel which should be kept at the disposal of the national supervisory authorities for checks.

Amendment 30

Article 10, paragraph 2 a (new)

2a. The measures referred to in paragraphs 1 and 2 shall be in conformity with a basic IT data-security level to be

selected pursuant to Article 35.

Justification

The present legal instrument cannot and should not go into too much detail as regards security measures. However, certain amendments are proposed because they constitute necessary improvements. At the same time there is no need here to try to establish further security provisions, since such issues are dealt with in existing standards. Therefore, the rapporteur considers that a basic international European level dealing with IT data security should be identified via the comitology procedure. This will have the advantage of the reference being flexible, e.g. each time the basic standard is updated (because of new developments) the level of data security ensured by Article 10 would also rise.

Amendment 31

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 **sole** 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.**

Justification

To be able to check afterwards who consulted what data at what moment is extremely important to ensure the correct application of this Regulation. The insertions proposed aim to specify in more detail what should be logged: at national level it is important to log the accesses to the SIS II. At the same time logging the further processing of the data accessed would go too far. The possibility whereby the logs may be used for carrying out an internal audit must be specified. Finally, keeping logs also as regards the use of copies is essential in order to ensure the lawfulness of processing, for example as regards the access rights.

Amendment 32

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

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

responsible for processing the data.

competent authority and the person processing the data.

Justification

To ensure optimal use of the logs, not only operational logs (messages sent, accesses, alarms) but also history logs (containing information concerning the issue, revision and withdrawal of alerts) should be kept.

Amendment 33

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

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. It is therefore proposed to allow Member States to keep the logs for up to three years which is currently the rule in the SIC. At the same time, it is important to state exactly when this period begins. Some of these provisions are copied from Article 14 which deals with logs at the central level.

Amendment 34

Article 11, paragraph 4

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

4. The competent authorities of the Member States in charge of the supervision of the processing of data in the SIS II ***(including internal supervision carried out by the superior of the person responsible for processing the data, or in connection with legal proceedings)*** shall have the right to access the logs for the purposes of monitoring the lawfulness of data processing and to ensure the proper functioning of the system including data integrity and security.

Justification

Instead of using the expression 'in particular those' (which does not make it clear which other authorities could be involved), the other supervision possibilities should be precisely identified.

Amendment 35
Article 11 a (new)

Article 11a

Internal auditing

Each authority with a right of access to the SIS II shall have an internal monitoring service responsible for ensuring full compliance with this Regulation and reporting directly to its senior management. Each authority shall send a regular report to the national supervisory authority and shall cooperate with them.

Justification

Although the Commission proposes in Article 10(1)(h) to establish internal auditing procedures, it does not specify them. The amendment seeks to close this gap.

Amendment 36
Article 11 b (new)

Article 11b

Staff training

Before being authorised to process data stored on the SIS II, staff of the authorities with a right to access the SIS II shall receive appropriate training about data-security and data-protection rules and shall be informed of the criminal offence and penalties referred to in Article 33.

Justification

The rapporteur considers it important to explicitly mention that all staff are required to

complete security and data-privacy training and that they should be aware of the criminal offence and penalties referred to in Article 33.

Amendment 37
Article 11 c (new)

Article 11c

Informing the public

Member States shall, in cooperation with their national data protection authority, devise and implement a policy to inform the public in general about the SIS II.

Justification

There is currently a lack of information for the public about the SIS. For this reason a lot of obscure and exaggerated fears persist. The launch of SIS II should be used as an occasion for properly informing the public about the system.

Amendment 39
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 ***until the entry into force of Regulation (EC) No. XX/XXXX establishing a European Agency for the Operational Management of large-scale IT-systems.***

Justification

The rapporteur is of the opinion that in the future a Community agency should be responsible for the management of all large-scale IT systems established for the creation of an area of freedom, security and justice (which would include, for example, Eurodac, which is currently managed by the Commission, and VIS). One of the most important elements to be taken into account is the possibility of synergies between the SIS II and other systems designed to monitor persons or objects. Such an agency should be set up soon (to be decided upon by codecision) and financed out of the EU budget. The EDPS has to have the same powers to supervise the agency as to supervise the Commission. All other options are either not feasible (continuous management by the Commission) or unacceptable because of lack of democratic control (e.g. by Europol, specific Member States or an intergovernmental agency). FRONTEX would be equally problematic because allocating it such a task would modify its character as a body ensuring operational cooperation between Member States and ultimately, given its mandate, it would have an interest in gaining possible access to the system, which would violate the control principle of the separation of tasks.

Amendment 39
Article 12, paragraph 1 a (new)

1a. The Commission may entrust such management (and also budget-implementation tasks) to a national public-sector body which meets the following selection criteria:

(a) it must demonstrate that it has proven ability to operate a large-scale information system comparable to the Schengen II Information System;

(b) it must have specialist knowledge regarding the functioning and the security requirements of an information system comparable to SIS II;

(c) it must have sufficient staff with adequate professional and language skills to work in an international-cooperation environment;

(d) it must have suitable infrastructure, with particular regard to equipment relating to CITs and methods of communication;

(e) it must work within an administrative environment which enables it to perform its tasks adequately and to avoid any conflict of interests.

Justification

During the transitional period the System must be able to continue functioning, with no shortfall in terms of efficiency or results.

Amendment 40
Article 12, paragraph 1 b (new)

1b. Should the Commission delegate any of its responsibilities during the transitional period, it must be certified that such delegation of powers falls entirely within the limits laid down under the terms of the institutional system specified in the Treaty. The Commission must ensure in particular that such delegation of powers does not have a

detrimental effect on any effective control mechanism established under Community law - be it the Court of Justice, the Court of Auditors or the European Data Protection Supervisor (EDPS). In any event the EDPS shall have the right and the opportunity to perform its tasks in full - in particular the opportunity to carry out checks in situ or as necessary to exercise any other powers conferred upon it under Article 47 of Regulation (EC) No 45/2001. Before delegating any powers and at periodic intervals thereafter, the Commission shall report to the European Parliament on the terms and conditions for the delegation of powers, on the precise scope of such delegation and on the bodies to which tasks have been delegated.

Justification

If any powers are delegated it must be ensured that this does not have any detrimental effect on effective monitoring.

Amendment 41

Article 12, paragraph 1 c (new)

1c. The Commission shall ensure that at all times the best available technology, subject to a cost-benefit analysis, is used for the SIS II.

Justification

The SIS II will have an important role to play as model for other private and public databases which use biometrics. Hence there is a strategic interest in ensuring that it is an appropriate model. The amendment also clarifies that part of the operational management will be the continuous updating of the system.

Amendment 42

Article 14, paragraph 1

1. All processing operations within the SIS II shall be logged for the purposes of monitoring the lawfulness of data

1. All processing operations within the SIS II shall be logged for the purposes of monitoring the lawfulness of data

processing and ensuring the proper functioning of the system, data integrity and security.

processing, **internal auditing** and ensuring the proper functioning of the system, data integrity and security.

Justification

See justification for amendment to Article 11(1).

Amendment 43
Article 14, paragraph 2

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

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

Justification

See justification for amendment to Article 11(2).

Amendment 44
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 one **to three years from the date** of the alert to which they **refer**. **The logs that include the history of the alerts shall be erased after a period of one to three years from the date of the alerts to which they refer. Logs may be kept for longer** if they are required for monitoring procedures which have already begun.

Justification

See justification for amendment to Article 11(3).

Amendment 45
Article 14, paragraph 4

4. The competent national authorities, **in particular those** in charge of the supervision of processing data in the SIS II, shall have the right to access the logs only for the purposes of monitoring the

4. The competent national authorities in charge of the supervision of processing data in the SIS II (**including internal supervision carried out by the superior of the person responsible for processing the**

lawfulness of data processing and to ensure the proper functioning of the system, including data integrity and security..

data, or in connection with legal proceedings) shall have the right to access the logs only for the purposes of monitoring the lawfulness of data processing and to ensure the proper functioning of the system, including data integrity and security.

Justification

See justification for amendment to Article 11(4).

Amendment 46
Article 14, paragraph 5

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

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

Justification

The Commission should have access to the logs at central level in its role as 'guardian of the treaty' and not in its role as 'operational manager'. The addition proposed will ensure that there are no doubts as to what the Commission can do in case the logs show inconsistencies, such as in the case of Eurodac (where the statistics showed a high number of unexplainable special searches and the Commission was unsure of what steps it could possibly undertake).

Amendment 47
Article 14, paragraph 6

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

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

Justification

This addition is proposed by the EDPS (p. 21 of his opinion) to allow him the monitoring of the lawfulness of the data processing operations.

Amendment 48
Article 14 a (new)

Article 14a

Information campaign

At the same time as the SIS II is brought into operation, the Commission shall launch a campaign to inform the public of the objectives pursued, the data stored in, and the authorities with access to, the SIS II and the rights of individuals. Such campaigns shall be conducted regularly.

Justification

See justification for new Article 11c. A model to be followed could be the information campaign on 'Air Passenger Rights' with its posters in airports (see also http://europa.eu.int/comm/transport/air/rights/info_en.htm).

Amendment 49
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*** 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.***

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 'residence' 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 50
Article 15, paragraph 1 a (new)

1a. National alerts may be entered in the SIS II only if the decision referred to in paragraph 1 is based on the following

cases:

Justification

See previous justification.

Amendment 51

Article 15, paragraph 1, point (a), introductory sentence

(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 serious threat to public policy or **internal** security of any Member State, in particular if:

Amendment 52

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 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 **by a 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; **or**

Amendment 53

Article 15, paragraph 1, point (a), point (ii)

(ii) the third country national is the object of a restrictive measure intended to prevent entry into or transit through the territory of Member States, taken in accordance with Article 15 of the EU Treaty.

(ii) the third country national is the object of a restrictive measure intended to prevent entry into or transit through the territory of Member States, taken in accordance with Article 15 of the EU Treaty **including a travel ban issued by the Security Council of the United Nations.**

Amendment 54

Article 15, paragraph 1, point (b)

(b) if the third country national **is the subject of a re-entry ban in application of a return decision or removal order taken**

(b) if the third country national **has been subject to a removal order or a return decision which has not been rescinded or**

in accordance with Directive 2005/XX/EC[on Return] .

suspended and which may be accompanied either by a ban on admission or, where applicable, by a ban on residence for failure to comply with national regulations on the entry or residence of third country nationals.

Justification

See justification for amendment to Article 15, paragraph 1.

Amendment 55
Article 15, paragraph 1 a (new)

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

Justification

A specific paragraph on the obligation to make an individual assessment is created. This was already part of the Commission's proposal ('based on an individual assessment') but was moved towards the end to achieve more clarity.

Amendment 56
Article 15, paragraph 1 b (new)

1b. Alerts issued pursuant to Article 15(1)(1)(a)(ii) shall be entered by the Member State holding the Presidency of the mixed committee.

Justification

As regards alerts pursuant to Article 15(1)(a)(ii) or on the basis of restrictive measures such as a travel ban issued by the UN Security Council) it has to be defined which Member State enters them on behalf of all Member States.

Amendment 57
Article 16, paragraph 1, point (f a) (new)

(fa) whether the persons concerned are armed, violent or have escaped;

Justification

Such data is currently inserted in the SIS (Art. 94(3)(g)) and is foreseen in the proposed Decision. It should also be included here so that a policeman making a control is adequately alerted to the potential danger represented by the individual in question.

Amendment 58

Article 16, paragraph 1, point (i), indent 1

- a judicial or administrative decision based on a threat to public policy or **public** security including, if relevant, the decision of conviction or the restrictive measure taken in accordance with Article 15 of the EU Treaty or

- a judicial or administrative decision based on a threat to public policy or **internal** security including, if relevant, the decision of conviction or the restrictive measure taken in accordance with Article 15 of the EU Treaty or

Amendment 59

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.**

Justification

The reference is added for clarification.

Amendment 60

Article 16, paragraph 2 a (new)

2a. Other information, in particular the data listed in Article 8(1) of Directive 95/46/EC, shall not be authorised.

Justification

This provision excludes the processing of sensitive data. A provision to this end is already contained in Article 94(3) SIC. While the SIC refers to the Council of Europe Convention of 1981 the amendment uses as a reference the corresponding Community legal instrument. The addition is important, in particular, because the categories of data contain such wide concepts as 'physical characteristics not subject to frequent change'.

Amendment 61

Article 16, paragraph 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.

Justification

The Commission proposal does not include any provisions on the source or use of the biometric data. Given the particular sensitivity of biometric data, the rapporteur considers it important to close this gap.

Regarding the suggestion contained in (a): This provision tries to address the concerns expressed by the EDPS (p. 9 of his opinion) and by the Art. 29 WP (p.14) regarding the source of the biometric data.

Regarding the suggestion contained in (b): This is suggested by the Article 29 WP (p.14). The Commission itself in the LIBE meeting of 23 November 2005 also confirmed that it is not intended to search with biometric data and outlined the procedure described in the amendment as the one which will be used. This approach is outlined as well in the Commission's communication on interoperability (COM(2005)597, p. 7). See also the June 2004 Council Presidency conclusions.

Amendment 62
Article 16 b (new)

Article 16b

Minimum data for an alert to be issued

An alert may not be issued without the data referred to in Article 16(1)(i).

Justification

The reference to the decision giving rise to the alert is crucial if use is to be made by other authorities. If this information is automatically included they can quicker establish the circumstances of the case and decide on the correct action to take.

Amendment 63

Article 17, paragraph 1, point (a)

(a) authorities responsible for control of persons at the external borders of the Member States;

(a) authorities responsible for control of persons at the external borders of the Member States, ***in accordance with what was notified to the Commission pursuant to Article 34(1)(d) of Regulation XX/XXXX/EC of the European Parliament and the Council of ... establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code)***;

Justification

By referring to the Schengen Borders Code the authorities responsible are clearly defined.

Amendment 64

Article 17, paragraph 1, point (b)

(b) authorities responsible for issuing of visas

(b) authorities responsible for issuing of visas ***in accordance with the common consular instructions and Regulation (EC) No 415/2003.***

Justification

By referring to the common consular instructions and the Regulation concerning the issuing of visas at the border the authorities responsible are clearly defined.

Amendment 65

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 for the purpose of identifying a*** third country ***national*** staying illegally in the territory in order to enforce a return decision or removal order.

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

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 66 Article 18, paragraph 2

2. Access to the alerts issued in accordance with Article 15 (1) (b) shall be given to the authorities responsible for the implementation of Regulation (EC) No 343/2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national¹, for the purpose of determining whether an asylum applicant has stayed illegally in another Member State. *deleted*

Justification

Regulation 343/2003 (Dublin Regulation) provides for the criteria to determine which Member State is responsible for the examination of an asylum application. Among these criteria is the illegal stay of five months in another Member State (Art. 10(2)). The fact that a particular person was entered for the purpose of refusing entry from a particular Member State does not, however, give any indication concerning the time during which he or she stayed in that country. Access to the SIS II would therefore not give the asylum authority the information they would require. Several further steps would be necessary. In addition, the criteria of Art. 10(2) is a criteria used only if several others are not applicable (family links, visa etc.). For all these reasons it does not appear to be justified to give asylum authorities access for this purpose.

Amendment 67 Article 18 a (new)

Article 18a

Limits on access

Users may only search those data that they require for the performance of their task.

¹ OJ L 50, 25.02.03, p.1

Amendment 68
Article 20, paragraph 2

2. Alerts issued in respect of a person who has acquired citizenship of any Member State shall be erased as soon as the Member State which issued the alert becomes aware that the person has acquired such citizenship.

2. Alerts issued for the purpose of non-admission in respect of a person who has acquired citizenship of any Member State shall be erased as soon as the Member State which issued the alert ***is informed pursuant to Article 24 or*** becomes aware that the person has acquired such citizenship.

Justification

According to the report of the JSA on an inspection of the use of Article 96 alerts in the SIS 'measures should be implemented or further developed to prevent Article 96 alerts on nationals from EU Member States' (p.9 of the report), since such nationals cannot be denied entry on to the Member States' territory. Such measures are proposed in amendments to Article 24. The amendment here establishes the corresponding reference.

Amendment 69
Article 20, paragraph 3

3. Alerts issued in respect of third country nationals who become members of the family of a citizen of the Union or of other beneficiaries of Community law on the right to free movement shall be erased as soon as the Member State which entered the alert becomes aware that the person has acquired such new status.

3. Alerts issued for the purpose of non-admission in respect of third country nationals who become members of the family of a citizen of the Union or of other beneficiaries of Community law on the right to free movement shall be erased as soon as the Member State which entered the alert ***is informed pursuant to Article 24 or*** becomes aware that the person has acquired such new status.

Justification

Also as regards this group of persons there should be a mechanism to ensure that the data is kept up-to-date.

Amendment 70
Article 20, paragraph 5

5. The alerts shall automatically be erased after ***five years*** from the date of the decision referred to in Article 15 (1). The Member States having entered the data in the SIS II may decide to keep the alerts in

5. The alerts shall automatically be erased after ***three years*** from the date of the decision referred to in Article 15 (1). The Member States having entered the data in the SIS II may decide, ***following an***

the system if the conditions of Article 15 **are** fulfilled.

individual assessment, to keep the alerts in the system **for a further two years** if the conditions of Article 15 **continue to be** fulfilled. **Where a Member State decides to keep an alert in the system, it shall notify the CS-SIS thereof. Where, at the end of the five-year period, the conditions of Article 15 continue to be fulfilled, the Member State concerned shall issue a new alert.**

Justification

Instead of the review after three years like in the current SIC the Commission proposes a five year retention period with the possibility to keep it longer if requested by the issuing Member States. No justification was brought forward by the Commission for the five year period (see also EDPS, p. 15). The rapporteur proposes a three year period which can be prolonged to an absolute maximum of five years. This provision has to be read in conjunction with Article 24(7) on reviews.

Amendment 71

Article 21, paragraph 1

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

1. Data entered in the SIS II pursuant to this Regulation shall only be processed for the purposes and by the competent national authorities defined by the Member States in accordance with this Regulation. **Any other use of data which does not comply with this Regulation shall be considered as an infringement of this Regulation and as misuse under the national law of the Member State.**

Justification

The latter part of this provision is foreseen in the current SIC (Article 102(5)) but was not included by the Commission in the present proposal. It is, however, important to keep this provision.

Amendment 72

Article 21, paragraph 2

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

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

duly authorised staff.

duly authorised staff. **Such staff may only access such data as are necessary for the performance of their tasks in accordance with this Regulation. National authorities shall keep an up-to-date list of persons entitled to access the SIS II.**

Justification

The first part of the amendment is taken from the VIS proposal (COM(2004)835; see Article 4) of the Commission and is a useful supplement. The second part is recommended by the EDPS (see p. 11 of his opinion).

Amendment 73

Article 21, paragraph 3

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

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

Justification

As to the first part of the amendment: it is not only important that Member States transmit 'an up-to-date list' but also that they indicate any changes made to it.

As to the second part of the amendment: in the interests of transparency and supervision it is important to ensure not only that the annually published list can be consulted but also that it is valid at all times. Simply publishing a list on its website should not constitute a heavy burden for the Commission.

Amendment 74

Article 23, paragraph 1

1. Except for the copy of data of the CS-

1. Except for the copy of data of the CS-

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

SIS referred to in Article 4 (3), the data processed in the SIS II may only be copied for technical purposes, provided that such copying is necessary for the competent national authorities to access the data in accordance with this Regulation **and provided that all provisions of this Regulation are applied also in respect of these copies.**

Justification

Member States according to Article 4(3) would be allowed to have one national copy of the data as a backup. The data contained in this national copy must be updated by the central system. Since some Member States appear to require more than one national copy, provision should be made for this but only on condition that these are constantly on-line, i.e. their content is at all times the same as the one in the central system. Another condition is that all other rules of this Regulation are applied to them in identical fashion.

Amendment 75

Article 23, paragraph 1 a (new)

1a) Copying for technical purposes as referred to in the first paragraph which leads to data stored off-line shall cease to be possible one year after the start of operations of the Visa Information System. Until this date Member States shall keep an up-to-date inventory of these copies, make this available to national data protection supervisory authorities and ensure that all provisions of this Regulation are applied also in respect of these copies.

Justification

Copies which are not constantly on-line, like CDs, should however be phased out. Currently these are mainly used by consulates in third countries. With the start of operations of the VIS all of these consulates will have to be equipped, however, with an adequate IT infrastructure. There will therefore not be a need anymore for using CDs, which raise numerous security problems (they can be stolen; not up-to-date data is used when issuing visas etc.). In the meantime safeguards for their use have to be established (see also JSA, p. 13).

Amendment 75

Article 24, paragraph 1

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

1. The Member State entering the data in the SIS II shall be responsible for ensuring that that data is processed lawfully and, in particular, that it is accurate and up-to-date. ***To this end, authorities responsible for alerts issued in respect of third country nationals for the purpose of refusing entry shall develop formal and written procedures.***

Justification

In an inspection into Article 96 alerts the JSA asked the question whether there was a formal description of the procedure to process these data in the SIS and to ensure that data were accurate, up to date and lawful. The outcome revealed that in many cases such procedures were lacking. The JSA recommended therefore the development of such procedures (JSA report on Article 96 alerts p. 6 and 9).

Amendment 77

Article 24, paragraph 3

3. If a Member State, which did not enter the data, has evidence suggesting that data is incorrect or has been unlawfully processed in the SIS II, it shall inform the Member State which entered the data by exchanging supplementary information at the earliest opportunity and ***if possible*** not later than 10 days after the evidence comes to its attention. The Member State which entered the data shall check it and, if necessary, modify, add to, correct or erase it. The detailed rules for this exchange of supplementary information shall be adopted in accordance with the procedure defined in Article 35 (3) and inserted in the SIRENE Manual.

3. If a Member State, which did not enter the data, has evidence suggesting that data is incorrect or has been unlawfully processed in the SIS II, it shall inform the Member State which entered the data by exchanging supplementary information at the earliest opportunity and not later than 10 days after the evidence comes to its attention. The Member State which entered the data shall check it and, if necessary, modify, add to, correct or erase it. The detailed rules for this exchange of supplementary information shall be adopted in accordance with the procedure defined in Article 35 (3) and inserted in the SIRENE Manual.

Justification

It is very important for the effective functioning of the SIS II that data is accurate and lawfully processed. Member States should therefore remedy problems quickly. The wording 'if possible' could prevent this from taking place in time. Ten days is a reasonable period which should be respected.

Amendment 78

Article 24, paragraph 4

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

4. If Member States are unable to reach agreement within two months about the correction of the data, **they shall** submit the case to the European Data Protection Supervisor who shall **jointly with the national supervisory authorities involved** act as mediator.

Justification

As to the first part of the amendment: according to the current Schengen Implementing Convention it was an obligation to submit such problems to the JSA. As the JSA writes: 'In view of the interests at stake for the data subject, the obligation to submit the dispute on data quality to the supervisor should remain.' (p. 17 of their opinion).

As to the second part: since the EDPS and national supervisory authorities should bear "joint responsibility" for the supervision of SIS II (see proposed Article 31b) they should also deal with such conflicts jointly.

Amendment 79

Article 24, paragraph 4 a (new)

4a. Each Member State shall, through the exchange of supplementary information, inform immediately the Member State responsible, if a person entered into the SIS II pursuant to Article 15 has acquired its nationality or has become through family connections a beneficiary of the Community law on the right to free movement.

Justification

According to the report of the JSA on an inspection of the use of Article 96 alerts in the SIS 'measures should be implemented or further developed to prevent Article 96 alerts on nationals from EU Member States' (p.9 of the report). This amendment seeks to ensure that information about a change of status of a person is transmitted to the Member State which had entered an alert. See also JSA, p. 22.

Amendment 80

Article 24, paragraph 5

5. The Member States shall exchange supplementary information in order to distinguish accurately between alerts in the SIS II related to persons with similar characteristics. The **detailed** rules for this exchange of supplementary information

5. The Member States shall exchange supplementary information in order to distinguish accurately between alerts in the SIS II related to persons with similar characteristics. The rules for this exchange of supplementary information **are that**

shall be adopted in accordance with the procedure defined in Article 35 (3) and inserted in the SIRENE Manual.

before an alert is entered the following procedure shall be followed:

(a) if processing a request for entering a new alert reveals that there is already an individual in the SIS II with the same mandatory identity description elements (surname, given name, date of birth) a check must be run before the new alert is approved;

(b) the SIRENE authority shall contact the requesting department to clarify whether the alert is on the same person or not;

(c) if the cross-check reveals that the person in question is indeed one and the same, the SIRENE authority shall apply the procedure for entering multiple alerts as referred to in paragraph 6. If the outcome of the check is that there are in fact two different people, the SIRENE authority approves the request for entering another alert by adding the necessary elements to avoid any misidentifications.

Justification

The present proposal of the Commission repeals Regulation 378/2004 (see Article 37 of the present Regulation) which provides for the modification of the SIRENE Manual by comitology. Instead all references to the SIRENE Manual in the present Regulation contain a cross-reference to the comitology committee provided for in Article 35. Thereby Regulation 378/2004 is de facto included in the present text. In its opinion (P5_TA(2003)0391 and 392 adopted on 23.9.2003) about the Greek initiatives which led to the adoption of Regulation 378/2004 Parliament requested that sensitive parts of the SIRENE Manual should not be modified by comitology but by the legislative procedure. Consequently several parts of the current SIRENE Manual are inserted in the present legal text.

Amendment 81

Article 24, paragraph 5a (new)

5a. The Member States shall exchange supplementary information if a person claims not to be the person wanted by an alert. If the outcome of the check is that there are in fact two different persons this person shall be informed about the provisions referred to in Article 25.

Justification

In the proposal of the Commission there is no provision for the case where somebody is checked but claims not to be this person (Article 25 deals with cases where the misuse of an identity is known; Article 24(5) deals with the measures prior to the entry of an alert).

Amendment 82

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 **every two years** 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).**

Justification

As to the first part of the amendment: In order to avoid an overly bureaucratic approach it is proposed to have a review every two years. The two year period would constitute a compromise between the one year period proposed by the Commission and the three year period currently foreseen in Article 112(1) SIC.

As to the second part of the amendment: The JSA has pointed out in their opinion that in a number of Member States the retention period is 'routinely renewed' (p. 11 of their opinion). Such an approach would seem to contradict the principle that there should be an individual assessment of each case to see whether the alert should remain in the system. The JSA also suggested adding the requirement proposed here that the reviews be documented (p. 12 of their opinion).

Amendment 83

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

Amendment 84

Article 26, paragraph 3 a (new)

3a. All links shall have clear operational requirements.

Amendment 85
Article 26, paragraph 4

4. When a Member State considers that the creation of a link between alerts is incompatible with its national law or international obligations, it **may** take the necessary measures to ensure there can be no access to the link **from its national territory**.

4. When a Member State considers that the creation **by another Member State** of a link between alerts is incompatible with its national law or international obligations, it **shall** take the necessary measures to ensure there can be no access to the link **by its national authorities**.

Amendment 86
Article 27, paragraph 1

1. Member States shall keep a copy of the decisions referred to in Article 16 (1) (i) to support the exchange of supplementary information.

1. Member States shall keep a copy of the decisions referred to in Article 16 (1) (i) to support the exchange of supplementary information **at the SIRENE authority**.

Justification

It is important to specify where the information is to be kept.

Amendment 87
Article 27, paragraph 2

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

2. The supplementary information transmitted by another Member State shall be used only for the purpose for which it was transmitted. It shall only be kept in national files as long as the alert to which it relates is kept in the SIS II. Member States may keep this information for a longer period, **but not for longer than is necessary** to achieve the purpose for which it was transmitted. In any event, the supplementary information shall be erased at the latest one year after the related alert has been erased from the SIS II.

Justification

The amendments seeks to make it clear that the data can be kept only for the time which is deemed strictly necessary for the achievement of the objectives.

Amendment 88
Article 28

An individual whose data is to be processed in the SIS II for the purpose of refusing entry shall be informed of:

An individual whose data is to be processed in the SIS II for the purpose of refusing entry shall be informed ***in writing*** of:

Justification

It is important to specify that the information should be given in writing. Addresses etc should not be communicated orally.

Amendment 89
Article 28, point (ca) (new)

(ca) the data conservation period.

Justification

This addition is suggested by the EDPS because it would contribute to ensuring fair treatment of the data subject (p. 17 of his opinion).

Amendment 90
Article 28, point (e a) (new)

(ea) the existence of the right referred to in Article 15(3);

Justification

This addition is suggested by the EDPS (p. 17 of his opinion) and the Art. 29 WP (p. 16).

Amendment 91
Article 28, point (e b) (new)

(eb) the existence of the right to remedies referred to in Article 30;

Justification

This addition is suggested by the EDPS because it should contribute to ensuring fair treatment of the data subject (p. 17 of his opinion).

Amendment 92
Article 28, point (e c) (new)

(ec) the address of the national data protection supervisory authority.

Justification

This addition is suggested by the Art. 29 WP (p. 16 of their opinion).

Amendment 93
Article 28, subparagraph 1 a (new)

This information shall be given:

(a) together with the re-entry ban in application of a return decision or a removal order or a sentence pursuant to Article 15(1)(a)(i); or

(b) by any authority with the right of access which enters into contact with the third country national;

(c) in any case at the border in case of a refusal of entry.

Justification

In order for the right of information to be effective it has to be possible to give the information. The amendment seeks to outline when the information should be given and by doing so closes a gap in the Commission's proposal.

Amendment 94
Article 29, paragraph 3

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

3. The personal data shall be communicated to the individual concerned as soon as possible and in any event not later than 60 days from the date on which he applies for access. ***If national law provides for a shorter delay, the latter***

shall be respected.

Justification

There is a risk of contradictions between the delays provided for in this Regulation and national procedures which are still valid. The amendment seeks to solve this possible conflict in the interest of the person concerned (EDPS, p. 17).

Amendment 95
Article 29, paragraph 3 a (new)

3a. Whenever a person requests data relating to him or her, the responsible authority shall send a copy of the request to the competent national supervisory authority.

Justification

It is important that the national data protection authorities are informed about such requests. This allows them to have an overview about the requests.

Amendment 96
Article 29, paragraph 4

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

4. The individual shall be informed about the follow-up given to the exercise of his rights of rectification and erasure as soon as possible and in any event not later than **3** months from the date on which he applies for rectification or erasure.

Justification

The JSA outlines that given the interest at stake a 6 months time limit is too long. They propose a limit of three months. See JSA, p. 18.

Amendment 97
Article 30

Any person ***in the territory of any Member State*** shall have the right to bring an action or a complaint before the courts of that Member State if he is refused the right of access to or the right to rectify or erase data relating to him or the right to obtain

Any person shall have the right to bring an action or a complaint before the courts of that Member State if he is refused the right of access to or the right to rectify or erase data relating to him or the right to obtain information or reparation in connection

information or reparation in connection with the processing of his personal data contrary to this Regulation.

with the processing of his personal data contrary to this Regulation.

Where an action or a complaint is lodged with a court in a Member State which is not responsible for entering the alert, that Member State shall cooperate with the Member State responsible for entering the alert.

The Member States shall mutually abide by the final decisions taken by the courts in other Member States.

Justification

As the EDPS outlines, such a territorial limitation is not justified and might make the right to remedies ineffective because most of the persons concerned will not be on the territory since they have been refused entry at the border (EDPS p. 18). See also Art. 29 WP p. 16 and JSA, p. 19. The second of the new paragraphs added to the existing text is taken from Article 111(2) of the Schengen Convention.

Amendment 98 Article 31, title

Data protection authorities

National supervisory authorities

Amendment 99 Article 31, paragraph 1

1. ***Each*** Member State ***shall require that the authorities designated pursuant to Article 28(1) of Directive 95/46/EC to monitor independently the lawfulness of the processing of SIS II personal data on its territory, including the exchange and further processing of supplementary information.***

1. ***The authority or authorities designated in each Member State and endowed with the powers referred to in Article 28 of Directive 95/46/EC shall monitor independently the lawfulness of the processing of SIS II personal data on and from their territory, including the exchange and further processing of supplementary information.***

Justification

This provision should not address Member States but independent supervisory authorities. Article 28 of Directive 95/46/EC and current practice also take account of federal states with more than one supervisory authority. It is also clarified that national data protection authorities have all the powers given to them by Article 28 of the Directive (EDPS p. 19). Furthermore the word 'from' is added to take account of the situation that national processing

will regularly make use of the central system. The lawfulness of this processing should be subject to supervision by national supervisory authorities where necessary in cooperation with EDPS.

Amendment 100
Article 31, paragraph 1 a (new)

1a. The authority or authorities referred to in paragraph 1 shall ensure that at least every four years an audit of the data processing operations in the national part of SIS II is carried out according to international auditing standards.

Justification

It should be ensured that SIS II, both at national and European level, is regularly subject to audits according to high and similar standards, either by or on behalf of the competent supervisory authorities. Audits are even more important considering the probably wide use made of national copies.

Amendment 101
Article 31, paragraph 1 b (new)

1b. Member States shall ensure that the authority or authorities referred to in paragraph 1 have sufficient resources to fulfil the tasks entrusted to them by this Regulation.

Justification

Essential is that supervision works. Without sufficient resources it will not work. Unfortunately, currently many authorities are under-resourced (see the first report on the implementation of the Data Protection Directive (95/46/EC) (COM(2003)265)).

Amendment 102
Article 31, paragraph 2

2. The European Data Protection Supervisor shall monitor that the personal data processing activities of the Commission are carried out in accordance with this Regulation. ***deleted***

(See amendment for Article 31 a)

Amendment 103

Article 31, paragraph 3

3. The national supervisory authorities and the European Data Protection Supervisor shall cooperate actively with each other. The European Data Protection Supervisor shall convene a meeting for that purpose at least once a year. *deleted*

(See amendment for Article 31 b)

Amendment 104
Article 31 a (new)

Article 31a

The European Data Protection Supervisor

1. The European Data Protection Supervisor shall monitor that the personal data processing activities of the Commission are carried out in accordance with this Regulation. The duties and powers referred to in Article 46 and 47 of Regulation (EC) No. 45/2001 shall apply accordingly.

2. The European Data Protection Supervisor shall ensure that at least every four years an audit of the Commission's data processing activities is carried out according to international auditing standards. The report of the audit shall be sent to the European Parliament, the Council, the Commission and the national supervisory authorities referred to in Article 31. The Commission shall be given an opportunity to make comments before the report is adopted.

Justification

The duties and powers of the EDPS are derived from Regulation 45/2001 which applies to processing activities of the Commission (see Recital 15). At the same time they are also limited by the extent of the activities of the Commission. This is made clear by the word 'accordingly' and the proposed addition to recital 16.

Amendment 105
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 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.***

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 106
Article 33

Sanctions

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.

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 ***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.***

Amendment 107
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 ***lawfulness of processing and the*** functioning of the SIS II against objectives, in terms of output, cost-effectiveness and quality of service.

Justification

The Commission's rule is not limited to the operational management but the Commission is at the same time the guardian of the treaty. In this role the Commission has to ensure that such monitoring systems are in place. The choice of method is, however, left to the Commission.

Amendment 108
Article 34, paragraph 2 a (new)

2a. Each year the Commission shall publish statistics showing the number of

records per alert, the number of hits per alert and how many times the SIS II was accessed, respectively given as a total and for each Member State.

Justification

At the moment certain limited statistics are published in the Council register (see for example Council doc. 5239/06) while more detailed statistics are not published. For transparency reasons the annual publication of statistics is important.

Amendment 109

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 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.***

Justification

The Commission's rule is not limited to the operational management but the Commission is at the same time the guardian of the treaty. It is essential that the Commission accepts this role and reports also about the compliance with legal requirements (see EDPS p. 20). In order to obtain the necessary information for doing so the Commission can rely on its sources it uses like in any Community policy area (complaints from citizens, Member States, own initiative etc) and on the logs stored at central level (see also amendment to Article 14(5)). The latter part of the amendments seeks to ensure that democratic control can be effective.

Amendment 110

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

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.

shall include the examination of results achieved against objectives, ***the lawfulness of processing*** 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.

Justification

See justification for amendment to Article 34(3).

Amendment 111
Article 34, paragraph 5

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

5. Member States shall provide the Commission with the information necessary to draft the reports referred to in paragraphs ***2a***, 3 and 4.

Justification

This addition is a necessary consequence of the amendment proposed to Article 34, paragraph 2a (new).

Amendment 112
Article 35, paragraph 1

1. The Commission shall be assisted by a Committee.

1. The Commission shall be assisted by a Committee, ***hereinafter "the Committee"***. ***It shall be composed of the representatives of the Member States and chaired by the representative of the Commission.***

Justification

The right of the Council, as legislator, to partly delegate its implementing powers to the Commission, has been recognized by the European Court of Justice since 1970 (decision Koster 25/70). The Court of Justice decision also required that such a delegation should specify the principles as well as the conditions for its exercise (as setting-up Committees of Member States' representatives to assist the Commission) and eventually the power 'to call-back' the delegation.

These principles have been inserted in Article 202 TEC. The Council however 'forgot' in implementing the Article 202 (in the Comitology Decision 1999/468) to recognize the same right of 'call-back' in acts decided by codecision for the European Parliament.

In order to have the benefit of this right, the European Parliament would have to insert it in the initial decision foreseeing the delegation of implementing powers. This is the purpose of the amendments to Article 35. Instead of making reference to the Articles of the Decision 1999/468, the amendments reproduce their content when it comes to the role of the Council, and propose similar prerogatives for the European Parliament (including the power to 'call back').

Amendment 113
Article 35, paragraph 2

2. Where reference is made to this paragraph, the advisory procedure laid down in Article 3 of Decision 1999/468/EC shall apply, in compliance with Article 7 (3) thereof. *deleted*

Justification

See justification for amendment to Article 35, paragraph.

Amendment 114
Article 35, paragraph 3

3. Where reference is made to this paragraph, the regulatory procedure laid down in Article 5 of Decision 1999/468/EC shall apply, in compliance with Article 7(3) thereof. *deleted*

The period provided for in Article 5(6) of Decision 1999/468/EC shall be three months.

Justification

See justification for amendment to Article 35, paragraph 1.

Amendment 115
Article 35, paragraph 4, point (a) (new)

(a) Where this Regulation imposes procedural requirements for the adoption of implementing measures, the

representative of the Commission shall submit a draft of those measures to the Committee and to the European Parliament.

The Committee shall deliver its opinion on the draft within a time-limit which the chairman may lay down according to the urgency of the matter which shall not be less than one month. The opinion shall be delivered by the majority laid down in Article 205(2) of the Treaty. The votes of the representatives of the Member States within the Committee shall be weighted in the manner set out in that Article. The chairman shall not vote.

Amendment 116

Article 35, paragraph 4, point (b) (new)

(b) The Commission shall adopt the measures envisaged if they are in accordance with the opinion of the Committee and of no objection has been raised in the meantime by the competent committee of the European Parliament.

Amendment 117

Article 35, paragraph 4, point (c) (new)

(c) Where the measures envisaged are not in accordance with the opinion of the Committee, or if no opinion is delivered, or an objection has been raised by the competent committee of the European Parliament, the Commission shall, without delay, submit to the Council and to the European Parliament a proposal relating to the measures to be taken.

Amendment 118

Article 35, paragraph 4, point (d) (new)

(d) If, within a period which may not exceed three months from the referral, the proposal has not been rejected either by

the European Parliament, by an absolute majority of its members, or by the Council, acting by qualified majority, it shall be adopted by the Commission. Otherwise the Commission shall submit an amended proposal or present a legislative proposal on the basis of the Treaty.

Amendment 119

Article 35, paragraph 4, point (e) (new)

(d) Without prejudice to any implementing measures already adopted, application of the provisions of the Regulation which provide for the adoption of technical rules and decisions shall cease four 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 relevant provisions, in accordance with the procedure laid down in Article 251 of the Treaty, and, with that aim in view, shall review those provisions prior to expiry of the four-year period.

Amendment 120

Article 35, paragraph 4, point (f) (new)

(f) The authorities referred to in Article 31 and 31a shall be consulted on the draft measures prior to adoption.

Justification

The JSA argued that data protection supervisors should be assigned a formal advisory role in the committee (JSA, p. 10).

Amendment 121

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, 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.

EXPLANATORY STATEMENT

I. Introduction

The SIS II¹ is of very high importance for the EU, in particular to allow for the enlargement of the Schengen area to the new Member States to take place as soon as possible. The rapporteur is fully aware of the political importance and the resulting time pressure. He therefore reconfirms his willingness to try to achieve in a constructive way a first reading agreement with all three proposals as a package.

II. General approach

The rapporteur applied a series of guiding principles when preparing the amendments to the Commission's proposals. First of all, the traditional position of Parliament as expressed in recent years was incorporated. Secondly, amendments are proposed and proposals of the Commission supported which ensure that the SIS II is firmly embedded in the Community's and Union's legal framework. Thirdly, a 'bigger system' requires 'bigger safeguards'. Consequently amendments for improved data protection standards are put forward. A sense of priority for data protection has to be displayed. Fourthly, the idea 'to go back to the old text' as requested by many Member States in the Council was carefully examined. Text from the current Schengen Implementing Convention (SIC) was introduced wherever it appeared better and more complete.

III. Issues for the present Regulation and the Decision

III.1 Technical copies

Following a careful assessment the rapporteur is ready to accept national copies (Art. 4(3)). He also accepts technical copies (Art. 23) but only under the condition that these are constantly on-line and therefore at all times contain identical data as the central system and the national copies. Copying for technical purposes which leads to data stored off-line (for example on CDs) must end one year after the start of operations of the VIS. In the meantime, adequate safeguards have to be introduced (for example the keeping of an inventory of off-line copies). It is equally important that a search in a copy can only be made by using the same search criteria as in the central system and that a search in a copy produces the same result as a search in the central system (see amendments to Art. 9 and 23).

III.2 Data quality

The quality of the SIS II data is of paramount importance to ensure the effectiveness of the system. Up until today there have been numerous complaints about the quality of data in the SIS. The data of EU citizens or family members of EU citizens constitutes a particular

¹ For a general description of the current SIS and a first analysis of the Commission's proposals the rapporteur would like to refer to two working documents presented to the Committee on 23.11.2005: PE364.657V02-00; PE364.674V02-00

problem. A series of suggestions aiming to further improve data quality are introduced in Art. 24. These include the introduction of formal and written procedures to ensure that data is lawfully processed, accurate and up-to-date, the obligation to submit disputes about the accuracy of data to the data protection authorities, the obligation to inform the Member States immediately of the change of status of a person subject to an alert and the documentation of reviews. Furthermore, an obligation to exchange supplementary information is introduced for cases in which a person claims not to be the person wanted by an alert. Finally, the review period is prolonged from one to two years which appears to be more realistic. The rapporteur is afraid that overly ambitious obligations risk to be implemented in an improper way.

III.3 Biometric data

The Commission proposes the inclusion of biometrics without any further specification as to the source of the biometric data and its use. In his proposed Art. 16a new the rapporteur introduces certain basic rules to close this gap: Firstly, the biometric data entered into SIS II has to pass a quality check according to a standard to be established by comitology in order to reduce the risk of errors. Secondly, a search with biometrics should be excluded at this initial stage of the system.

III.4 Interlinking

Like biometrics the interlinking of alerts is a new element of SIS II in comparison to the current system which will enhance the system's capacities. In the future it will be possible to link, for example, the alert of a stolen car with the alert of a person wanted for arrest. If a policeman then discovers the stolen car he will have grounds to believe that the person wanted for arrest was or still is in the immediate vicinity of this car. It is, however important to underline that links should only be made if they have clear operational requirements (see amendment to Art. 26).

III.5 Communication with the public

A major problem with the current SIS is the lack of information to the public. For this reason a lot of obscure and exaggerated fears persist. Citizens are mostly not informed about their rights in relation to the system (for example the right to request information and its correction). The launch of SIS II should be used as an occasion for properly informing the public about the system. This should be done by the Commission and the Member States and be financed out of the SIS II budget. Such campaigns should be repeated on a regular basis. A model to be followed could be the information campaign on 'Air Passenger Rights' with its posters in airports. The rapporteur expects a clear commitment from the Commission and the Member States on this issue.

III.6 Supervision

New proposals for the system of supervision had to be found in order to reconcile the current system including the Joint Supervisory Authority (JSA) with the realities of a modified legal and institutional context. To this end the rapporteur had a series of meetings with representatives of the JSA and the European Data Protection Supervisor (EDPS) in order to find a mutually satisfactory solution. This solution is now brought forward in the amendments to Art. 31, 31a new and 31b new. The main element of this system is the concept of joint

responsibility. The nature of the SIS II requires close cooperation between supervisors which is best achieved in this way. The proposals are supplemented by a more detailed description of the tasks of supervision which is based on Art. 115 SIC and current practice. Finally, the rapporteur wishes to stress that the Commission's role is not limited to the operational management but that the Commission is at the same time the guardian of the Treaty and therefore also a supervisor. It is essential that the Commission accepts this role because it constitutes a key element for an effective supervision. Amendments concerning this role of the Commission are introduced to Art. 14 and 34.

III. 7 Location and future management

The rapporteur was initially ready to exclude the issue of location and future management from the debate about the legislative framework. Since the Member States in the Council, however, raised this issue and attached great importance to it, the rapporteur has no objection to including it in this legislative instrument.

As far as the physical location is concerned, the rapporteur has no objections against the sites of Strasbourg and Sankt Johann im Pongau (see amendment to Art. 4a new). The operational management of the SIS II at these locations has to be, however, the sole responsibility of the Commission.

The rapporteur is of the firm opinion that in the future a community agency¹ should be responsible for the management of all large-scale IT systems established for the creation of an area of freedom, security and justice (i.e. also for Eurodac which is currently managed by the Commission and for the VIS).²

IV. The present Regulation

IV. 1 Art. 15

Serious problems were identified with the data of the current Art. 96 alerts for the purpose of refusing entry and need to be addressed. The rapporteur therefore welcomes the Commission's proposal on this Article. He proposes some amendments to Article 15 which aim to further improve the text. He would like to strengthen, for example, the notions that alerts have to be based on an individual assessment and that alerts will have to be harmonised at SIS II alert level.

IV.2 Access rights

The rapporteur basically agrees with the access rights to the various authorities as proposed by the Commission. Some amendments are proposed to Art. 17 and 18 essentially clarifying which the authorities concerned are. In Art. 18(1) the rapporteur makes clear that police authorities should like today have the right to access the alerts for the purpose of refusing entry because it has to be acknowledged that such persons can be on the territory of the Member States.

¹ This was always requested by Parliament (see recommendation on SIS II adopted on 20.11.2003).

² See the justification for the amendment to Art. 12 for a more detailed explanation.

The rapporteur does, however, not agree with the proposed access to asylum authorities for the purpose of determining the Member State responsible for an asylum application (amendment to Art. 18(2)). The justification for such an access is too farfetched. In addition, the rapporteur is of the opinion that the access for asylum authorities for the purpose of determining whether an asylum seeker constitutes a 'threat to public order or internal security' (Art. 18(3)) and thereby - indirectly - for the examination of an asylum application should be clarified by referring to the precise grounds as given in the qualifications directive.

The publication - also on the internet - of an up-to-date list of the authorities with access is very important for transparency reasons and supervision (see amendments to Art. 21(3)).

IV. 3 Conservation periods

The rapporteur proposes a three year retention period in accordance with the three year period currently foreseen for the review of Article-96 alerts (Art. 112(1) SIC). There should, however, be the possibility to prolong the period by two more years following an individual assessment. If the conditions are still met after five years a new alert should be entered. Together with the review of the data foreseen in Art. 24(7) this would mean that alerts would be checked after two, three and five years. The rapporteur is of the opinion that this is necessary to ensure the quality of the data in the SIS II.

IV.4 Comitology

The rapporteur follows the present line of the LIBE committee in proposing an alternative committee procedure which would put Parliament and Council on a more equal level. The rapporteur is fully aware of the ongoing interinstitutional discussions on this matter but will keep these amendments (to Art. 35) until a satisfactory solution is found. In addition, certain parts of the SIRENE manual are introduced in the text of the Regulation because the SIRENE manual is subject to the comitology procedure and in the opinion of the rapporteur does in parts not represent purely technical implementing measures. Finally, the rapporteur proposes to give the data protection authorities the possibility to deliver opinions on draft implementing measures.