

EUROPÄISCHES PARLAMENT

2004



2009

Ausschuss für bürgerliche Freiheiten, Justiz und Inneres

25.4.2006

PE 372.150v01-00

ÄNDERUNGSANTRÄGE 175-256

Entwurf eines Berichts

(PE 365.022v01-00)

Carlos Coelho

Vorschlag für einen Beschluss des Rates über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II)

Vorschlag für einen Beschluss (KOM(2005)0230 – C6-0301/2005 – 2005/0103(CNS))

Entwurf einer legislativen EntschlieÙung

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 175
Spiegelstrich 4 a (neu)

- *in Kenntnis der Stellungnahme des Europäischen Datenschutzbeauftragten vom 19. Oktober 2005 und der Stellungnahme der Artikel-29-Datenschutzgruppe vom 25. November 2005,*

Or. de

Begründung

Betonung des Datenschutzes und Hervorhebung der Stellungnahmen, die an vielen Stellen Referenzpunkte für Änderungsanträge sind.

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 176
Ziffer 4 a (neu)

4a. fordert den Rat auf, dafür zu sorgen, dass dieser Beschluss erst in Kraft tritt, wenn der Rahmenbeschluss 2005/XX/JI des Rates über den Schutz personenbezogener Daten, die

AM\612230DE.doc

PE 372.150v01-00

**im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen
verarbeitet werden, bereits in Kraft getreten ist;**

Or. de

Begründung

Es ist äußerst wichtig, dass der oben genannte Rahmenbeschluss zum Datenschutz bereits in Kraft ist vor Inkrafttreten dieses Beschlusses, um auch ein hohes Datenschutzniveau bei der Verarbeitung personenbezogener Daten des SIS II im Rahmen der 3. Säule zu gewährleisten.

Vorschlag für einen Beschluss

Vorschlag der Kommission

Änderungen des Parlaments

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 177
Erwägung 5

(5) Das SIS II sollte als Ausgleichsmaßnahme zur Wahrung eines hohen Maßes an Sicherheit in einem Raum ohne Binnengrenzkontrollen zwischen den Mitgliedstaaten beitragen, indem es die operative Zusammenarbeit zwischen Polizei- und Justizbehörden in Strafsachen unterstützt.

(5) Das SIS II sollte als Ausgleichsmaßnahme zur Wahrung eines hohen Maßes an Sicherheit in einem Raum ohne Binnengrenzkontrollen zwischen den Mitgliedstaaten beitragen, indem es die operative Zusammenarbeit zwischen Polizei- und Justizbehörden in Strafsachen unterstützt **und zur Anwendung der Bestimmungen von Titel IV des EG-Vertrags betreffend den freien Personenverkehr beiträgt.**

Or. en

Begründung

Titel IV der konsolidierten Fassung des Vertrags zur Gründung der Europäischen Gemeinschaft betrifft Visa, Asyl, Einwanderung und andere Politiken im Zusammenhang mit dem freien Personenverkehr und sollte daher in den Vorschlag aufgenommen werden.

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 178
Erwägung 5

(5) Das SIS II sollte als Ausgleichsmaßnahme **zur Wahrung eines hohen Maßes** an Sicherheit in einem Raum ohne Binnengrenzkontrollen zwischen den Mitgliedstaaten **beitragen, indem es die operative Zusammenarbeit zwischen Polizei- und Justizbehörden in Strafsachen unterstützt.**

(5) Das SIS II sollte als Ausgleichsmaßnahme **ein hohes Maß** an Sicherheit in einem Raum ohne Binnengrenzkontrollen zwischen den Mitgliedstaaten **gewährleisten.**

Or. de

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 179
Erwägung 6

(6) Die Ziele des SIS II müssen präzisiert und Vorschriften für den Betrieb und die Nutzung des Systems sowie für die Zuständigkeiten müssen festgelegt werden, einschließlich Bestimmungen über die Systemarchitektur und die Finanzierung, die in das System einzugebenden Datenkategorien, die Eingabezwecke und -kriterien, die zugriffsberechtigten Behörden und die Verknüpfung von Ausschreibungen sowie weiterer Vorschriften über die Datenverarbeitung und den Schutz personenbezogener Daten.

(6) Die Ziele des SIS II müssen präzisiert und Vorschriften für den Betrieb und die Nutzung des Systems sowie für die Zuständigkeiten müssen festgelegt werden, einschließlich Bestimmungen über die Systemarchitektur, **einen hohen Grad an Sicherheit** und die Finanzierung, die in das System einzugebenden Datenkategorien, die Eingabezwecke und -kriterien, die zugriffsberechtigten Behörden und die Verknüpfung von Ausschreibungen sowie weiterer Vorschriften über die Datenverarbeitung und den Schutz personenbezogener Daten.

Or. en

Begründung

Für die Verwaltung einer derartigen Datenbank sind klare Leitlinien erforderlich, um ein sicheres Funktionieren zu gewährleisten. Deshalb ist es notwendig, die Zuständigkeiten festzulegen.

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 180

Erwägung 7

(7) Die mit dem Betrieb des SIS II verbundenen Ausgaben sind aus dem Haushalt der Europäischen Union zu finanzieren.

(7) Die mit dem Betrieb des SIS II verbundenen Ausgaben sind aus dem Haushalt der Europäischen Union zu finanzieren. ***Sollten Mitgliedstaaten aber beschließen, die Möglichkeit zu nutzen und nationale Kopien anzulegen, sind die damit verbundenen Kosten von ihnen zu tragen.***

Or. en

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 181

Erwägung 8

(8) Es ***sollte*** ein Handbuch ***ausgearbeitet werden***, das genaue Vorschriften für den Austausch von Zusatzinformationen im Hinblick auf die aufgrund der Ausschreibung erforderlichen Maßnahmen enthält. Die nationalen Behörden jedes Mitgliedstaats sollten den Austausch dieser Informationen gewährleisten.

(8) Es ***ist notwendig***, ein Handbuch ***auszuarbeiten***, das genaue Vorschriften für den Austausch von Zusatzinformationen im Hinblick auf die aufgrund der Ausschreibung erforderlichen Maßnahmen enthält. Die nationalen Behörden jedes Mitgliedstaats sollten den Austausch dieser Informationen gewährleisten.

Or. en

Änderungsantrag von Henrik Lax

Änderungsantrag 182

Erwägung 9

(9) Die Kommission sollte für das Betriebsmanagement des SIS II verantwortlich sein und insbesondere einen reibungslosen Übergang von der Entwicklung des Systems zu seiner Inbetriebnahme sicherstellen.

(9) Die Kommission sollte ***während eines Übergangszeitraums von drei Jahren nach Inkrafttreten dieses Beschlusses*** für das Betriebsmanagement des SIS II verantwortlich sein und insbesondere einen reibungslosen Übergang von der Entwicklung des Systems zu seiner Inbetriebnahme sicherstellen.

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 183

Erwägung 9

(9) Die Kommission sollte für das Betriebsmanagement des SIS II verantwortlich sein und insbesondere einen reibungslosen Übergang von der Entwicklung des Systems zu seiner Inbetriebnahme sicherstellen.

Die Kommission sollte für das Betriebsmanagement des SIS II verantwortlich sein und insbesondere einen reibungslosen Übergang von der Entwicklung des Systems zu seiner Inbetriebnahme sicherstellen. **Die im derzeitigen SIS gespeicherten Daten können erst dann in das neue System übertragen werden, wenn das laufende System geprüft und die darin gespeicherten Daten auf ihre Integrität untersucht worden sind.**

Begründung

Die alten Daten sollten geprüft und untersucht werden, bevor sie in die neue Datenbank übertragen werden, damit sichergestellt ist, dass keine falschen oder unzuverlässigen Informationen übermittelt werden.

Änderungsantrag von Henrik Lax

Änderungsantrag 184

Erwägung 9 a (neu)

(9a) Nach dem Übergangszeitraum von drei Jahren nach Inkrafttreten dieses Beschlusses sollte das Betriebsmanagement Aufgabe einer Europäischen Agentur für das Betriebsmanagement großer IT-Systeme sein.

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 185

Erwägung 13

(13) Für jede Ausschreibungskategorie sollte eine maximale Erfassungsdauer festgelegt werden, **die nur überschritten werden darf, wenn dies zur Erreichung des Zwecks der Ausschreibung erforderlich und angemessen ist.** Generell sind Ausschreibungen aus dem SIS II zu löschen, sobald die mit der Ausschreibung beantragte Maßnahme ausgeführt ist.

(13) Für jede Ausschreibungskategorie sollte eine maximale Erfassungsdauer festgelegt werden. Generell sind Ausschreibungen aus dem SIS II zu löschen, sobald die mit der Ausschreibung beantragte Maßnahme ausgeführt ist.

Or. en

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 186

Erwägung 14

(14) Ausschreibungen von Personen zwecks Verhaftung und Übergabe oder Auslieferung sowie Ausschreibungen von Personen zu ihrem Schutz oder zur Gefahrenabwehr **und von im Rahmen eines Gerichtsverfahrens gesuchten Personen** sollten höchstens 10 Jahre im SIS II gespeichert werden können, da diese Ausschreibungen zur Wahrung der öffentlichen Sicherheit im Schengener Raum wichtig sind.

(14) Ausschreibungen von Personen zwecks Verhaftung und Übergabe oder Auslieferung sowie Ausschreibungen von Personen zu ihrem Schutz oder zur Gefahrenabwehr sollten höchstens 10 Jahre im SIS II gespeichert werden können, da diese Ausschreibungen zur Wahrung der öffentlichen Sicherheit im Schengener Raum wichtig sind.

Or. en

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 187

Erwägung 14

(14) Ausschreibungen von Personen zwecks Verhaftung und Übergabe oder Auslieferung sowie Ausschreibungen von Personen zu ihrem Schutz oder zur Gefahrenabwehr und von im Rahmen eines Gerichtsverfahrens gesuchten Personen sollten höchstens **10**

(14) Ausschreibungen von Personen zwecks Verhaftung und Übergabe oder Auslieferung sowie Ausschreibungen von Personen zu ihrem Schutz oder zur Gefahrenabwehr und von im Rahmen eines Gerichtsverfahrens gesuchten Personen sollten höchstens **drei**

Jahre im SIS II gespeichert werden können, da diese Ausschreibungen zur Wahrung der öffentlichen Sicherheit im Schengener Raum wichtig sind.

Jahre im SIS II gespeichert werden können, da diese Ausschreibungen zur Wahrung der öffentlichen Sicherheit im Schengener Raum wichtig sind.

Or. de

Begründung

Im derzeitigen System ist eine Speicherungsfrist von drei Jahren vorgesehen (Artikel 112 Schengener Durchführungsübereinkommen). Die Kommission gibt keine Begründung für eine verlängerte Belassung der Ausschreibungen im System an. Es sollte daher die derzeitige Frist von drei Jahren beibehalten werden.

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 188
Erwägung 15

(15) Das SIS II sollte **die Verarbeitung biometrischer Daten ermöglichen, damit die betreffenden Personen zuverlässiger identifiziert werden können. Ebenso sollte das SIS II** die Verarbeitung von Daten von Personen ermöglichen, deren Identität missbraucht wurde; den Betroffenen sollen dadurch Unannehmlichkeiten aufgrund einer falschen Identifizierung erspart werden; dabei sind angemessene Datenschutzbestimmungen vorzusehen, insbesondere die Zustimmung der betroffenen Personen und eine strikte Beschränkung der Zwecke, zu denen diese Daten rechtmäßig verarbeitet werden können.

(15) Das SIS sollte die Verarbeitung von Daten von Personen ermöglichen, deren Identität missbraucht wurde; den Betroffenen sollen dadurch Unannehmlichkeiten aufgrund einer falschen Identifizierung erspart werden; dabei sind angemessene Datenschutzbestimmungen vorzusehen, insbesondere die Zustimmung der betroffenen Personen und eine strikte Beschränkung der Zwecke, zu denen diese Daten rechtmäßig verarbeitet werden können.

Or. de

Begründung

Siehe Begründung zu Änderungsantrag zu Artikel 39 Absatz 1 Buchstaben d und e.

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 189
Erwägung 15

(15) Das SIS II sollte die Verarbeitung biometrischer Daten ermöglichen, damit die betreffenden Personen zuverlässiger identifiziert werden können. Ebenso sollte das SIS II die Verarbeitung von Daten von Personen ermöglichen, deren Identität missbraucht wurde; den Betroffenen sollen dadurch Unannehmlichkeiten aufgrund einer falschen Identifizierung erspart werden; dabei sind angemessene Datenschutzbestimmungen vorzusehen, insbesondere die Zustimmung der betroffenen Personen und eine strikte Beschränkung der Zwecke, zu denen diese Daten rechtmäßig verarbeitet werden können.

(15) Das SIS II sollte die Verarbeitung biometrischer Daten ermöglichen, damit die betreffenden Personen zuverlässiger identifiziert werden können. ***Biometrische Daten dürfen aber nicht als Suchkriterium verwendet werden.*** Ebenso sollte das SIS II die Verarbeitung von Daten von Personen ermöglichen, deren Identität missbraucht wurde; den Betroffenen sollen dadurch Unannehmlichkeiten aufgrund einer falschen Identifizierung erspart werden; dabei sind angemessene Datenschutzbestimmungen vorzusehen, insbesondere die Zustimmung der betroffenen Personen und eine strikte Beschränkung der Zwecke, zu denen diese Daten rechtmäßig verarbeitet werden können.

Or. en

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 190 Erwägung 17

(17) Das SIS II sollte den Mitgliedstaaten die Möglichkeit bieten, Ausschreibungen miteinander zu verknüpfen. Das Verknüpfen von ***zwei oder mehr*** Ausschreibungen durch einen Mitgliedstaat sollte sich nicht auf die zu ergreifende Maßnahme, die Erfassungsdauer oder das Recht auf Zugriff auf die Ausschreibungen auswirken.

(17) Das SIS II sollte den Mitgliedstaaten die Möglichkeit bieten, Ausschreibungen miteinander zu verknüpfen. Das Verknüpfen von Ausschreibungen durch einen Mitgliedstaat sollte sich nicht auf die zu ergreifende Maßnahme, die Erfassungsdauer oder das Recht auf Zugriff auf die Ausschreibungen auswirken.

Or. en

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 191 Erwägung 18

(18) ***Die Zusammenarbeit zwischen der Europäischen Union und Drittländern oder internationalen Organisationen in Polizei-***

(18) Werden personenbezogene Daten aus dem SIS II an einen Dritten übermittelt, muss dieser Dritte die personenbezogenen

und Justizangelegenheiten sollte durch die Förderung eines wirksameren Informationsaustauschs ausgebaut werden.

Werden personenbezogene Daten aus dem SIS II an einen Dritten übermittelt, muss dieser Dritte die personenbezogenen Daten ***angemessen*** schützen und dies durch ein Abkommen garantieren.

Daten ***hochgradig*** schützen und dies durch ein Abkommen garantieren.

Or. en

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 192
Erwägung 18 a (neu)

(18a) Das SIS II darf erst dann mit anderen Datenbanken verbunden werden, wenn eine gründliche Sicherheitsanalyse durchgeführt worden ist.

Or. en

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 193
Erwägung 19

(19) Alle Mitgliedstaaten haben das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 ratifiziert. Nach Artikel 9 dieses Übereinkommens sind Ausnahmen und Einschränkungen der Rechte und Pflichten in bestimmten Grenzen möglich. Die im Zusammenhang mit der Umsetzung dieses Beschlusses verarbeiteten Daten sollten gemäß den Grundsätzen des Übereinkommens geschützt werden. Die in dem Übereinkommen verankerten Grundsätze sollten in diesem Beschluss erforderlichenfalls ergänzt oder präzisiert werden.

(19) Die Verarbeitung personenbezogener Daten im Rahmen dieses Beschlusses bemisst sich nach dem Rahmenbeschluss 2005/XX/JI des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden. Der Rahmenbeschluss muss daher in Kraft sein, bevor dieser Beschluss in Kraft tritt.

Begründung

Siehe Begründung zum Änderungsantrag zu Ziffer 4a des Entwurfs einer legislativen Entschließung.

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 194
Erwägung 22

(22) Unabhängige nationale Kontrollbehörden sollten die Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten überwachen, und der Europäische Datenschutzbeauftragte, der mit dem Beschluss 2004/55/EG des Europäischen Parlaments und des Rates vom 22. Dezember 2003 über die Nominierung für das Amt der unabhängigen Kontrollbehörde gemäß Artikel 286 des EG-Vertrags (Europäischer Datenschutzbeauftragter) ernannt wurde, sollte die Tätigkeiten der Kommission in Bezug auf die Verarbeitung personenbezogener Daten kontrollieren.

(22) Unabhängige nationale Kontrollbehörden sollten die Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten überwachen, und der Europäische Datenschutzbeauftragte, der mit dem Beschluss 2004/55/EG des Europäischen Parlaments und des Rates vom 22. Dezember 2003 über die Nominierung für das Amt der unabhängigen Kontrollbehörde gemäß Artikel 286 des EG-Vertrags (Europäischer Datenschutzbeauftragter)¹ ernannt wurde, sollte die Tätigkeiten der Kommission in Bezug auf die Verarbeitung personenbezogener Daten kontrollieren. **Die nationalen Kontrollstellen und der Europäische Datenschutzbeauftragte sollten eng zusammenarbeiten.**

Or. en

Begründung

Da es Themenstellungen mit Auswirkungen auf beide Ebenen geben wird, sollten die beiden zuständigen Stellen zusammenarbeiten.

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 195
Erwägung 29

¹ ABl. L 12 vom 17.1.2004, S. 47.

(29) Es müssen Übergangsbestimmungen für SIS-Ausschreibungen nach dem Schengener Übereinkommen, die in das SIS II übertragen werden, und für Ausschreibungen im SIS II während eines Übergangszeitraums, in dem noch nicht alle Bestimmungen dieses Beschlusses anwendbar sind, festgelegt werden. Einige Bestimmungen des Schengen-Besitzstands sollten für einen begrenzten Zeitraum weiterhin Gültigkeit haben, bis die Mitgliedstaaten die Vereinbarkeit dieser Ausschreibungen mit dem neuen Rechtsrahmen überprüft haben.

(29) Es müssen Übergangsbestimmungen für SIS-Ausschreibungen nach dem Schengener Übereinkommen, die in das SIS II übertragen werden, und für Ausschreibungen im SIS II während eines Übergangszeitraums, in dem noch nicht alle Bestimmungen dieses Beschlusses anwendbar sind, festgelegt werden. ***Diese Ausschreibungen dürfen nur dann in das SIS II aufgenommen werden, wenn ihre Integrität garantiert werden kann.*** Einige Bestimmungen des Schengen-Besitzstands sollten für einen begrenzten Zeitraum weiterhin Gültigkeit haben, bis die Mitgliedstaaten die Vereinbarkeit dieser Ausschreibungen mit dem neuen Rechtsrahmen überprüft haben. ***Ausschreibungen, die damit nicht vereinbar sind, sollten gelöscht werden.***

Or. en

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 196
Erwägung 29 a (neu)

(29a) Um das einwandfreie Funktionieren des SIS II sicherzustellen, sollte das gegenwärtige SIS – im Hinblick auf die Sicherheit und Integrität der im System gespeicherten Informationen und Ausschreibungen, auf das technische System an sich und auf die Kommunikationsinfrastruktur mit den nationalen Zugangsstellen, usw. – geprüft werden. Die Ergebnisse dieser Prüfung sollten berücksichtigt werden, bevor das SIS II seinen Betrieb aufnimmt.

Or. en

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 197

Erwägung 29 b (neu)

(29b) Ein allgemeiner Sicherheitsplan sollte für das SIS II entwickelt werden, bevor das System seinen Betrieb aufnimmt. In diesem Plan sollten die physischen und verhaltensbasierten Sicherheitsaspekte des Systems auf nationaler und europäischer Ebene berücksichtigt werden. Der Plan sollte einen klaren Überblick über die Zuständigkeiten jeder betroffenen Person auf jeder Ebene geben.

Or. en

Begründung

Die Durchführung einer allgemeinen Sicherheitsanalyse umfasst mehr als die technische Absicherung des Systems. Das Verhalten der Personen, die das System betreiben, muss ebenfalls berücksichtigt werden.

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 198

Artikel 1 Absatz 1

1. Hiermit wird ein computergestütztes Informationssystem mit der Bezeichnung Schengener Informationssystem der zweiten Generation (nachstehend „SIS II“) errichtet, das den zuständigen Behörden der Mitgliedstaaten die Zusammenarbeit in Form des Austausches von Informationen **zum Zwecke von Personen- und Sachkontrollen** ermöglichen soll.

1. Hiermit wird ein computergestütztes Informationssystem mit der Bezeichnung Schengener Informationssystem der zweiten Generation (nachstehend „SIS II“) errichtet, das den zuständigen Behörden der Mitgliedstaaten die Zusammenarbeit in Form des Austausches von Informationen **zu den in diesem Beschluss genannten Zwecken** ermöglichen soll.

Or. en

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 199

Artikel 1 Absatz 2

2. *Das SIS II trägt zur Wahrung* eines hohen Maßes an Sicherheit in einem Raum ohne Binnengrenzkontrollen zwischen den Mitgliedstaaten *bei*.

2. *Ziel des SIS II ist die Gewährleistung* eines hohen Maßes an Sicherheit in einem Raum ohne Binnengrenzkontrollen zwischen den Mitgliedstaaten.

Or. de

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 200
Artikel 1 Absatz 2

2. Das SIS II trägt zur Wahrung eines hohen Maßes an Sicherheit in einem Raum ohne Binnengrenzkontrollen zwischen den Mitgliedstaaten *bei*.

2. Das SIS II trägt zur Wahrung eines hohen Maßes an Sicherheit in einem Raum ohne Binnengrenzkontrollen zwischen den Mitgliedstaaten *und zur Anwendung der Bestimmungen von Titel IV des EG-Vertrags betreffend den freien Personenverkehr* *bei*.

Or. en

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 201
Artikel 2 Absatz 2

2. Dieser Beschluss enthält außerdem Bestimmungen über die *Systemarchitektur* des SIS II, die Zuständigkeiten der Mitgliedstaaten und der Kommission, die allgemeine Datenverarbeitung, die Rechte der betroffenen Einzelpersonen und die Haftung.

2. Dieser Beschluss enthält außerdem Bestimmungen über die *System- und Sicherheitsarchitektur* des SIS II, die Zuständigkeiten der Mitgliedstaaten und der Kommission, die allgemeine Datenverarbeitung, die Rechte der betroffenen Einzelpersonen und die Haftung *im Bezug auf die Integrität des Systems*.

Or. en

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 202
Artikel 4 Absatz 1 Buchstabe b

b) einer **bis zwei** von jedem Mitgliedstaat festgelegten Zugangsstellen (nachstehend „NI-SIS“),

b) einer von jedem Mitgliedstaat festgelegten Zugangsstellen (nachstehend „NI-SIS“),

Or. de

Begründung

Solange keine überzeugende Begründung für die Notwendigkeit von zwei Zugangsstellen angeführt wird, sollte, um mögliche Missbrauchsgefahren einzudämmen, nur eine Zugangsstelle vorgesehen werden (Stellungnahme des Europäischen Datenschutzbeauftragten, S. 21).

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 203
Artikel 4 Absatz 2

2. Die nationalen Systeme der Mitgliedstaaten (nachstehend „NS“) sind über die NI-SIS mit dem SIS II verbunden.

2. Die nationalen Systeme der Mitgliedstaaten (nachstehend „NS“) sind über die NI-SIS mit dem SIS II verbunden.
Das Kommunikationssystem hat alle Sicherheitsprotokolle zu umfassen, wie dies im allgemeinen Sicherheitsplan für das SIS II angeführt ist.

Or. en

Änderungsantrag von Henrik Lax

Änderungsantrag 204
Artikel 4 a (neu)

Artikel 4a

Standort

Gemäß dem Verfahren nach Artikel 251 des Vertrags nehmen das Europäische Parlament und der Rat eine Verordnung zur Festlegung des Standorts des Zentralen Schengener Informationssystems und des Back-up-Systems an.

Or. en

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 205

Artikel 4 a (neu)

Artikel 4a

Die Europäische Agentur für das Betriebsmanagement des SIS II bestimmt, wo das CS-SIS und das Back-up-System ihren Standort haben sollen.

Or. en

Begründung

Sobald eine Entscheidung über das Betriebsmanagement getroffen wurde, muss ein Standort für das CS-SIS und sein Back-up-System gewählt werden. Die Europäische Agentur sollte das Recht haben, über den am besten geeigneten Standort zu entscheiden.

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 206

Artikel 6

Jeder Mitgliedstaat ist für den Betrieb und die Wartung seines NS und dessen Anschluss an das SIS II verantwortlich.

Jeder Mitgliedstaat ***richtet ein NS ein und*** ist für den Betrieb und die Wartung seines NS und dessen Anschluss an das SIS II verantwortlich. ***Jeder Mitgliedstaat führt die im allgemeinen Sicherheitsplan festgelegten Leitlinien durch.***

Or. en

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 207

Artikel 7 Absatz 1

1. Jeder Mitgliedstaat bestimmt eine ***Stelle***, die im Einklang mit diesem Beschluss den Zugang der zuständigen Behörden zum SIS II gewährleistet.

1. Jeder Mitgliedstaat bestimmt eine ***nationale SIS-II-Stelle***, die – ***unter der eindeutigen Verantwortlichkeit des Mitgliedstaats – als Zentrale für das nationale System zuständig und für das***

reibungslose Funktionieren und die Sicherheit des nationalen Systems verantwortlich ist und im Einklang mit diesem Beschluss den Zugang der zuständigen Behörden zum SIS II gewährleistet.

Or. en

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 208
Artikel 9 Absatz 2

2. ***Gegebenenfalls tragen die*** Mitgliedstaaten dafür Sorge, dass die Daten in den Kopien des Datenbestands der CS-SIS-Datenbank jederzeit mit dem CS-SIS-Datenbestand identisch sind und übereinstimmen.

2. ***Die*** Mitgliedstaaten ***tragen*** dafür Sorge, dass die Daten in den Kopien des Datenbestands der CS-SIS-Datenbank jederzeit mit dem CS-SIS-Datenbestand identisch sind und übereinstimmen.

Or. en

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 209
Artikel 9 Absatz 3

3. ***Gegebenenfalls tragen die*** Mitgliedstaaten dafür Sorge, dass eine Abfrage in Kopien des CS-SIS-Datenbestands zu demselben Ergebnis führt wie eine direkte Abfrage im CS-SIS.

3. ***Die*** Mitgliedstaaten ***tragen*** dafür Sorge, dass eine Abfrage in Kopien des CS-SIS-Datenbestands zu demselben Ergebnis führt wie eine direkte Abfrage im CS-SIS.

Or. en

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 210
Artikel 9 Absatz 3 a (neu)

3a. Die Mitgliedstaaten stellen sicher, dass die auf die Daten in den Kopien

zugreifenden Behörden nur diejenigen Informationen, Ausschreibungen und Verknüpfungen abrufen können, die sie einsehen dürfen.

Or. en

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 211
Artikel 9 Absatz 3 b (neu)

3b. Die Mitgliedstaaten führen ein detailliertes Protokoll über die Personen, die auf die Kopien zugreifen, die Zahl der bestehenden Kopien und wo sich die Kopien befinden.

Or. en

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 212
Artikel 10

Sicherheit **und Geheimhaltung**

Sicherheit

1. **Die Mitgliedstaaten, die Zugriff auf die im SIS II verarbeiteten Daten haben, treffen die erforderlichen Maßnahmen, um:**

-1. Die Mitgliedstaaten führen die im Sicherheitsplan nach Absatz 1 angenommenen Leitlinien für die Sicherheit durch.

1. **Der gemeinsame Sicherheitsplan beinhaltet die Maßnahmen, die die Mitgliedstaaten treffen müssen, wenn sie auf die im SIS II verarbeiteten Daten zugreifen, um:**

(-a) die Infrastruktur und die Standorte der Zugangsstellen (NI-SIS) sowie die Kommunikationsinfrastruktur zwischen den NI-SIS und dem C-SIS physisch zu schützen;

(-aa) permanent ein hohes Sicherheitsniveau zu gewährleisten mittels Überwachung und durch einen klaren Überblick über die für die Sicherheit

(a) Unbefugten den Zugang zu Anlagen, in denen NI-SIS- und NS-Datenverarbeitungsvorgänge durchgeführt werden, zu verwehren (Zutrittskontrollen);

(b) den unbefugten Zugriff auf SIS-II-Daten und Datenträger und das unbefugte Lesen, Kopieren, Ändern oder Löschen dieser Daten und Datenträger zu verhindern (Datenträgerkontrolle);

(c) zu verhindern, dass auf für die Übertragung zwischen dem NS und dem SIS II bestimmte SIS-II-Daten unbefugt zugegriffen werden kann oder diese Daten unbefugt gelesen, kopiert, geändert oder gelöscht werden können (Übertragungskontrolle);

(d) sicherzustellen, dass nachträglich überprüft und festgestellt werden kann, welche SIS-II-Daten wann und von wem erfasst wurden (Datenerfassungskontrolle);

(e) die unbefugte Verarbeitung von SIS-II-Daten im NS und die unbefugte Änderung oder Löschung von im NS erfassten SIS-II-Daten zu verhindern (Dateneingabekontrolle);

Verantwortlichen, durch die Benennung eines Sicherheitsmanagers, der die Risiken ermittelt, eines Informationsmanagers, der die Daten auf ihre Integrität prüft, und eines Netzwerk-Managers, der für die Sicherheit des Netzes und der Kommunikationsinfrastruktur zuständig ist. Diese Manager sind gegenüber den Mitgliedstaaten rechenschaftspflichtig.

(a) Unbefugten den Zugang zu Anlagen, in denen NI-SIS- und NS-Datenverarbeitungsvorgänge durchgeführt werden, zu verwehren (Zutrittskontrollen **und Kontrollen in der Anlage**);

(b) den unbefugten Zugriff auf SIS-II-Daten und Datenträger und das unbefugte Lesen, Kopieren, Ändern oder Löschen dieser Daten und Datenträger zu verhindern (Datenträgerkontrolle);

(c) zu verhindern, dass **während der Datenübertragung bzw.** auf für die Übertragung zwischen dem NS und dem SIS II bestimmte SIS-II-Daten unbefugt zugegriffen werden kann oder diese Daten unbefugt gelesen, kopiert, geändert oder gelöscht werden können (Übertragungskontrolle);

(d) sicherzustellen, dass nachträglich überprüft und festgestellt werden kann, welche SIS-II-Daten wann und von wem erfasst wurden (Datenerfassungskontrolle);

(e) die unbefugte Verarbeitung von SIS-II-Daten im NS und die unbefugte Änderung oder Löschung von im NS erfassten SIS-II-Daten **dadurch** zu verhindern, **dass nur befugtes Personal mit individuellen und einmaligen Nutzeridentitäten und geheimen Passwörtern Zugang erhält** (Dateneingabekontrolle);

(ea) sicherzustellen, dass jede Behörde mit einem Zugriffsrecht auf das SIS II Profile des Personals erstellt, das zu den Räumlichkeiten bzw. zum SIS II Zugang hat. Es wird eine ständig aktualisierte Liste dieses Personals geführt und den nationalen Kontrollstellen zur Verfügung

(f) sicherzustellen, dass Zugriffsberechtigte bei der Nutzung des NS nur Zugriff auf SIS-II-Daten für ihren Zuständigkeitsbereich haben (Zugriffskontrolle);

(g) zu gewährleisten, dass überprüft und festgestellt werden kann, welchen Behörden in den NS erfasste SIS-II-Daten mit Datenübertragungsgeräten übermittelt werden können (Übermittlungskontrolle);

(h) die Wirksamkeit der **in diesem Absatz genannten** Sicherheitsmaßnahmen zu kontrollieren (Eigenkontrolle).

2. Die Mitgliedstaaten treffen für den Austausch und die Weiterverarbeitung von Zusatzinformationen Sicherheits- und Geheimhaltungsmaßnahmen, die den in Absatz 1 genannten Maßnahmen entsprechen.

3. Die berufliche Schweigepflicht bzw. eine vergleichbare Geheimhaltungspflicht gilt für alle Personen und Stellen, die mit SIS-II-Daten und Zusatzinformationen arbeiten müssen.

Die Geheimhaltungspflicht besteht auch nach dem Ausscheiden dieser Personen aus dem Amt oder Dienstverhältnis oder der Beendigung der Tätigkeit dieser Stellen weiter.

gestellt;

(f) sicherzustellen, dass Zugriffsberechtigte bei der Nutzung des NS nur Zugriff auf SIS-II-Daten für ihren Zuständigkeitsbereich haben (Zugriffskontrolle);

(g) zu gewährleisten, dass übergeprüft und festgestellt werden kann, welchen Behörden im NS erfasste SIS-II-Daten durch Datenübertragungsgeräte **unter Verwendung von Verschlüsselungstechniken** übermittelt werden können (Übermittlungskontrolle);

(h) die Wirksamkeit der Sicherheitsmaßnahmen zu kontrollieren (Eigenkontrolle).

Or. en

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 213
Artikel 10 a (neu)

Artikel 10a

Vertraulichkeit

1. Die berufliche Schweigepflicht bzw. eine vergleichbare Geheimhaltungspflicht gilt für alle Personen und Stellen, die mit SIS-II-Daten und Zusatzinformationen arbeiten müssen.

2. Die Geheimhaltungspflicht besteht auch nach dem Ausscheiden dieser Personen aus dem Amt oder Dienstverhältnis oder der Beendigung der Tätigkeit dieser Stellen weiter.

Or. en

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 214
Artikel 10 Absatz 1 Buchstabe h a (neu)

ha) bei Systemabstürzen die sofortige Wiederherstellung der Daten zu gewährleisten sowie die Datenintegrität bereits gespeicherter Daten sicherzustellen.

Or. de

Begründung

Es ist notwendig, auch Regelungen für technische Notfälle zu schaffen. Da Systemabstürze nicht ausgeschlossen werden können, ist es unerlässlich, Vorkehrungen für solche Fälle zu treffen (siehe Stellungnahme der Artikel-29-Datenschutzgruppe vom 23. Juni 2005 zum VIS, S. 22)

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 215
Artikel 11 Absatz 1

1. Jeder Mitgliedstaat protokolliert jeglichen Datenaustausch mit dem SIS II **und die Weiterverarbeitung der betreffenden Daten**, damit die Rechtmäßigkeit der Datenverarbeitung kontrolliert werden kann, und **gewährleistet somit** das einwandfreie Funktionieren des NS sowie die Datenintegrität und -sicherheit.

1. Jeder Mitgliedstaat protokolliert jeglichen **Zugriff auf die im SIS II gespeicherten Daten und jeglichen** Datenaustausch mit dem SIS II, damit die Rechtmäßigkeit der Datenverarbeitung kontrolliert werden kann, **zum Zweck der internen Kontrolle und um** das einwandfreie Funktionieren des NS sowie die Datenintegrität und -sicherheit **zu gewährleisten. Mitgliedstaaten, die auf Kopien nach Artikel 4 Absatz 3 oder Kopien nach Artikel 42 zurückgreifen, protokollieren zu den gleichen Zwecken alle Verarbeitungsvorgänge im Rahmen**

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 216
Artikel 11 Absatz 2

2. Die Protokolle enthalten insbesondere das Datum und die Uhrzeit der Datenübermittlung, die für die Abfrage verwendeten Daten, die Datenübermittlung sowie den Namen der zuständigen Behörde und der *mit der* Datenverarbeitung *betrauten* Person.

2. Die Protokolle enthalten insbesondere *den Verlauf der Ausschreibungen*, das Datum und die Uhrzeit der Datenübermittlung, die für die Abfrage verwendeten Daten, *den Bezug auf* die übermittelten Daten sowie den Namen der zuständigen Behörde und der *die* Datenverarbeitung *durchführenden* Person.

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 217
Artikel 11 Absatz 3

3. Die Protokolle werden in geeigneter Weise vor unbefugtem Zugriff geschützt und nach einer Frist von *einem Jahr* gelöscht, wenn sie nicht für ein bereits eingeleitetes Kontrollverfahren benötigt werden.

3. Die Protokolle werden in geeigneter Weise vor unbefugtem Zugriff geschützt und nach einer Frist von *zwei Jahren* gelöscht, wenn sie nicht für ein bereits eingeleitetes Kontrollverfahren benötigt werden.

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 218
Artikel 11 Absatz 3

3. Die Protokolle werden in geeigneter Weise vor unbefugtem Zugriff geschützt und nach einer Frist von *einem Jahr* gelöscht, wenn sie *nicht* für ein bereits eingeleitetes Kontrollverfahren benötigt werden.

3. Die Protokolle werden in geeigneter Weise vor unbefugtem Zugriff geschützt und nach einer Frist von *drei Jahren nach der Löschung der Ausschreibung, auf die sie sich beziehen*, gelöscht. *Protokolle können*

länger gespeichert werden, wenn sie für ein bereits eingeleitetes Kontrollverfahren benötigt werden.

Or. de

Begründung

Unter Bezugnahme auf den Änderungsantrag des Berichterstatters zu Artikel 11 Absatz 3 soll ein verbindlicher Zeitraum von drei Jahren festgelegt werden, in dem die Protokolle aufbewahrt werden müssen. Dies ist angemessen in Anbetracht der Bedeutung, die diese Protokolle für die Überprüfung des rechtmäßigen Zugriffs und damit auch für den Rechtsschutz der Betroffenen haben.

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 219
Artikel 11 Absatz 4 a (neu)

4a. Jede Behörde mit einem Zugangsrecht zum SIS II verfügt über eine Struktur für internes Monitoring, um die vollständige Einhaltung dieses Beschlusses sicherzustellen. Jede Behörde erstattet der nationalen Kontrollstelle regelmäßig Bericht.

Or. en

Änderungsantrag von Henrik Lax

Änderungsantrag 220
Artikel 12 Absatz 1

1 ***Die*** Kommission ***ist*** für das Betriebsmanagement des SIS II zuständig.

1. ***Bis zum Inkrafttreten der Verordnung Nr. XX/XXXX/EG zur Errichtung einer Europäischen Agentur für das Betriebsmanagement großer IT-Systeme ist die Kommission während eines Übergangszeitraums von drei Jahren nach Inkrafttreten des vorliegenden Beschlusses für das Betriebsmanagement des SIS II zuständig.***

Or. en

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 221

Artikel 12 Absatz 1

1. Die Kommission ist für das Betriebsmanagement des SIS II zuständig.

1. Die Kommission ist für das Betriebsmanagement des SIS II **und insbesondere für den reibungslosen Übergang vom derzeitigen zum neuen System** zuständig. **Die im derzeitigen SIS gespeicherten Daten können erst dann in das neue System übertragen werden, wenn das laufende System geprüft und die darin gespeicherten Daten auf ihre Integrität untersucht worden sind.**

Or. en

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 222

Artikel 13

Sicherheit **und Geheimhaltung**

Die Kommission wendet in Bezug auf den Betrieb des SIS II Artikel 10 sinngemäß an.

Sicherheit

- 1. Die Kommission erstellt einen gemeinsamen Sicherheitsplan für das SIS II-System. Der Sicherheitsplan beinhaltet Verpflichtungen für die Mitgliedstaaten und die Kommission.**
- 2. Die Kommission teilt den Mitgliedstaaten die spezifischen Sicherheitsleitlinien mit und stellt sicher, dass sie sie in vollem Umfang anwenden.**
- 3. Der gemeinsame Sicherheitsplan sieht unter anderem vor, dass die Kommission die erforderlichen Maßnahmen trifft, um:**
 - (a) die Infrastruktur und den Standort des C-SIS sowie die Kommunikationsinfrastruktur zwischen den NI-SIS und dem C-SIS physisch zu schützen;**
 - (b) permanent ein hohes Sicherheitsniveau zu gewährleisten mittels Überwachung und**

durch einen klaren Überblick über die für die Sicherheit Verantwortlichen, durch die Benennung eines Sicherheitsmanagers, der die Risiken ermittelt, eines Informationsmanagers, der die Daten auf ihre Integrität prüft, und eines Netzwerk-Managers, der für die Sicherheit des Netzes und der Kommunikationsinfrastruktur zuständig ist. Die Manager sind gegenüber der Kommission rechenschaftspflichtig, die letztendliche Verantwortung trägt die Kommission aber selbst;

(c) Unbefugten den Zugang zu Anlagen, in denen C-SIS-Datenverarbeitungsvorgänge durchgeführt werden, zu verwehren (Zutrittskontrollen und Kontrollen in der Anlage);

(d) den unbefugten Zugriff auf SIS-II-Daten und -Datenträger und das unbefugte Lesen, Kopieren, Ändern oder Löschen dieser Daten und Datenträger zu verhindern (Datenträgerkontrolle);

(e) zu verhindern, dass während der Datenübertragung bzw. auf für die Übertragung zwischen den N-SIS und dem C-SIS bestimmte C-SIS-Daten unbefugt zugegriffen werden kann oder diese Daten unbefugt gelesen, kopiert, geändert oder gelöscht werden können (Übertragungskontrolle);

(f) nur befugtem Personal mit individuellen und einmaligen Nutzeridentitäten und geheimen Passwörtern Zugang zum C-SIS zu gewähren;

(g) Profile des Personals zu erstellen, das zu den Räumlichkeiten bzw. zum C-SIS-System Zugang hat. Es wird eine ständig aktualisierte Liste dieses Personals geführt und dem Europäischen Datenschutzbeauftragten zur Verfügung gestellt;

(h) sicherzustellen, dass befugte Personen nur zum C-SIS-System Zugang haben, nicht aber auf die Daten selbst zugreifen können (Zugriffskontrolle);

(j) sicherzustellen, dass der Datenfluss im Netz verschlüsselt ist;

(k) die Wirksamkeit der Sicherheitsmaßnahmen zu überwachen (Eigenkontrolle).

4. Der gemeinsame Sicherheitsplan umfasst alle Maßnahmen nach Artikel 10.

Or. en

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 223
Artikel 13 a (neu)

Artikel 13a

Vertraulichkeit

1. Die berufliche Schweigepflicht bzw. eine vergleichbare Geheimhaltungspflicht gilt für alle Personen und Stellen, die mit SIS-II-Daten und Zusatzinformationen arbeiten müssen.

2. Die Geheimhaltungspflicht besteht auch nach dem Ausscheiden dieser Personen aus dem Amt oder Dienstverhältnis oder der Beendigung der Tätigkeit dieser Stellen weiter.

Or. en

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 224
Artikel 14 Absatz 3

3. Die Protokolle werden in geeigneter Weise vor unbefugtem Zugriff geschützt und nach einer Frist von **einem Jahr** nach Löschung der Ausschreibung, auf die sie sich beziehen, gelöscht, wenn sie **nicht** für ein bereits eingeleitetes Kontrollverfahren benötigt werden.

3. Die Protokolle werden in geeigneter Weise vor unbefugtem Zugriff geschützt und nach einer Frist von **drei Jahren** nach Löschung der Ausschreibung, auf die sie sich beziehen, gelöscht. **Protokolle können länger gespeichert werden**, wenn sie für ein bereits eingeleitetes Kontrollverfahren benötigt werden.

Begründung

Siehe Begründung zum Änderungsantrag zu Artikel 11 Absatz 3.

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 225
Artikel 14 Absatz 3

3. Die Protokolle werden in geeigneter Weise vor unbefugtem Zugriff geschützt und nach einer Frist von **einem Jahr nach Löschung der Ausschreibung, auf die sie sich beziehen**, gelöscht, wenn sie nicht für ein bereits eingeleitetes Kontrollverfahren benötigt werden.

3. Die Protokolle werden in geeigneter Weise vor unbefugtem Zugriff geschützt und nach einer Frist von **zwei Jahren** gelöscht, wenn sie nicht für ein bereits eingeleitetes Kontrollverfahren benötigt werden.

Or. en

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 226
Artikel 18 Absatz 2

2. Das Europäische Polizeiamt (Europol) hat Zugriff auf die in den Ausschreibungen zwecks Verhaftung enthaltenen Daten, wenn dies für die Erfüllung seiner Aufgaben gemäß des Übereinkommens vom 26. Juli 1995 über die Errichtung eines Europäischen Polizeiamts ("Europol-Übereinkommen") **nötig** ist.

2. Das Europäische Polizeiamt (Europol) hat Zugriff auf die in den Ausschreibungen zwecks Verhaftung enthaltenen Daten **zum Zweck der Verhaftung**, wenn **und soweit** dies für die Erfüllung seiner Aufgaben gemäß des Übereinkommens vom 26. Juli 1995 über die Errichtung eines Europäischen Polizeiamts ("Europol-Übereinkommen") **notwendig** ist.

Or. de

Begründung

Grundsatz der Zweckbindung: Es muss sichergestellt werden, dass Europol nur Zugriff auf in Ausschreibungen enthaltene Daten hat, die es benötigt, um seine Aufgaben gemäß dem „Europol-Übereinkommen“ zu erfüllen. Dies soll mit dieser Änderung deutlicher gemacht werden.

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 227
Artikel 18 Absatz 3

3. Eurojust hat Zugriff auf die in den Ausschreibungen zwecks Verhaftung enthaltenen Daten und auf die in Artikel 16 und 17 genannten Daten, wenn dies für die Erfüllung ihrer Aufgaben gemäß dem Beschluss 2002/187/JI **nötig** ist.

3. Eurojust hat Zugriff auf die in den Ausschreibungen zwecks Verhaftung enthaltenen Daten und auf die in Artikel 16 und 17 genannten Daten **zum Zweck der Verhaftung**, wenn **und soweit** dies für die Erfüllung ihrer Aufgaben gemäß dem Beschluss 2002/187/JI **notwendig** ist.

Or. de

Begründung

Grundsatz der Zweckbindung: Es muss sichergestellt werden, dass Eurojust nur Zugriff auf in Ausschreibungen enthaltene Daten hat, die es benötigt, um seine Aufgaben gemäß dem Beschluss 2002/187/JI zu erfüllen. Dies soll mit dieser Änderung deutlicher gemacht werden.

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 228
Artikel 19 Absatz 2

2. Ausschreibungen zwecks Verhaftung und die in den Artikeln 16 und 17 genannten ergänzenden Daten werden **10** Jahre nach Erlass der Ausschreibungsentscheidung automatisch gelöscht. **Der Mitgliedstaat, der Daten in das SIS II eingegeben hat, kann beschließen, diese im System zu belassen, wenn dies für den Zweck, zu dem die Daten eingegeben wurden, erforderlich ist.**

2. Ausschreibungen zwecks Verhaftung und die in den Artikeln 16 und 17 genannten ergänzenden Daten werden **drei** Jahre nach Erlass der Ausschreibungsentscheidung automatisch gelöscht. **Sind nach Ablauf der drei Jahre die Bedingungen von Artikel 15 weiterhin erfüllt, veranlasst der Mitgliedstaat, der die Ausschreibung ursprünglich veranlasst hatte, eine neue Ausschreibung.**

Or. de

Begründung

Die Kommission gibt keine Begründung für eine verlängerte Belassung der Ausschreibungen im System an. Es sollte daher die in Artikel 112 Schengener Durchführungsübereinkommen vorgesehene Frist von drei Jahren beibehalten werden. Darüber hinaus ist es vorzugswürdig, dass bei weiterem Vorliegen der Ausschreibungsbedingungen eine neue Ausschreibung vorgenommen werden muss.

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 229

Artikel 23 Absatz 1

1. Mitgliedstaaten schreiben **im SIS II Vermisste oder Personen aus, die zu ihrem eigenen Schutz oder zur Gefahrenabwehr** auf Ersuchen der zuständigen Verwaltungs- oder Justizbehörde **vorläufig** in Gewahrsam genommen werden müssen.

1. Mitgliedstaaten schreiben auf Ersuchen der zuständigen Verwaltungs- oder Justizbehörde **Vermisste oder Personen im SIS II aus, die zu ihrem eigenen Schutz oder zur Gefahrenabwehr** in Gewahrsam genommen werden müssen.

Or. en

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 230

Artikel 25 Absatz 2

2. Die in Absatz 1 genannten Ausschreibungen werden **10** Jahre nach Erlass der der Ausschreibung zugrunde liegenden Entscheidung automatisch gelöscht. **Der Mitgliedstaat, der die Ausschreibung in das SIS II eingegeben hat, kann beschließen, diese im System zu belassen, wenn dies für den Zweck, zu dem die Ausschreibung eingegeben wurde, erforderlich ist.**

2. Die in Absatz 1 genannten Ausschreibungen werden **drei** Jahre nach Erlass der der Ausschreibung zugrunde liegenden Entscheidung automatisch gelöscht. **Sind nach Ablauf der drei Jahre die Bedingungen von Artikel 23 weiterhin erfüllt, veranlasst der Mitgliedstaat, der die Ausschreibung ursprünglich veranlasst hatte, eine neue Ausschreibung.**

Or. de

Begründung

Siehe Begründung zum Änderungsantrag zu Artikel 19 Absatz 2.

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 231

Artikel 28 Absatz 3

3. Eurojust hat Zugriff auf die in den Ausschreibungen gemäß Artikel 27 enthaltenen Daten, wenn dies für die Erfüllung ihrer Aufgaben gemäß dem

3. Eurojust hat Zugriff auf die in den Ausschreibungen gemäß Artikel 27 enthaltenen Daten **zu den in den Ausschreibungen genannten Zwecken**, wenn **und soweit** dies für die Erfüllung ihrer

Begründung

Daten sollen nur zu den in den Ausschreibungen genannten und nicht zu sonstigen Zwecken verwendet werden. Siehe auch Begründung zum Änderungsantrag zu Artikel 18 Absatz 3.

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 232
Artikel 29 Absatz 2

2. Die in Absatz 27 genannten Ausschreibungen werden **10** Jahre nach Erlass der der Ausschreibung zugrunde liegenden Entscheidung automatisch gelöscht. **Der Mitgliedstaat, der die Ausschreibung in das SIS II eingegeben hat, kann beschließen, diese im System zu belassen, wenn dies für den Zweck, zu dem die Ausschreibung eingegeben wurde, erforderlich ist.**

2. Die in Absatz 27 genannten Ausschreibungen werden **drei** Jahre nach Erlass der der Ausschreibung zugrunde liegenden Entscheidung automatisch gelöscht. **Sind nach Ablauf der drei Jahre die Bedingungen von Artikel 27 weiterhin erfüllt, veranlasst der Mitgliedstaat, der die Ausschreibung ursprünglich veranlasst hatte, eine neue Ausschreibung.**

Begründung

Siehe Begründung zum Änderungsantrag zu Artikel 19 Absatz 2.

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 233
Artikel 31 Absatz 1

1. Auf Ersuchen der zuständigen Justiz- oder Verwaltungsbehörde schreiben die Mitgliedstaaten zur Strafverfolgung und zur Abwehr von Gefahren für die öffentliche Sicherheit im SIS II Personen oder Fahrzeuge, Wasserfahrzeuge, Luftfahrzeuge und Container zur **verdeckten Registrierung oder zur gezielten** Kontrolle aus, wenn:

1. Auf Ersuchen der zuständigen Justiz- oder Verwaltungsbehörde schreiben die Mitgliedstaaten zur Strafverfolgung und zur Abwehr von Gefahren für die öffentliche Sicherheit im SIS II Personen oder Fahrzeuge, Wasserfahrzeuge, Luftfahrzeuge und Container zur Kontrolle **oder Durchsuchung** aus, wenn:

(a) konkrete Anhaltspunkte dafür vorliegen, dass der Betroffene in erheblichem Umfang außergewöhnlich schwere Straftaten plant oder begeht, oder

(b) die Gesamtbeurteilung des Betroffenen, insbesondere aufgrund der bisher von ihm begangenen Straftaten, erwarten lässt, dass er auch künftig außergewöhnlich schwere Straftaten begehen wird.

(a) konkrete Anhaltspunkte dafür vorliegen, dass der Betroffene in erheblichem Umfang außergewöhnlich schwere Straftaten plant oder begeht, **wie dies in Artikel 2 des Europol-Übereinkommens und seinem Anhang definiert ist**, oder

(b) die Gesamtbeurteilung des Betroffenen, insbesondere aufgrund der bisher von ihm begangenen Straftaten, erwarten lässt, dass er auch künftig außergewöhnlich schwere Straftaten **nach der Definition von Artikel 2 des Europol-Übereinkommens und seinem Anhang** begehen wird.

Or. en

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 234 Artikel 33 Absatz 3

3. Europol hat Zugriff auf die in den Ausschreibungen gemäß Artikel 31 genannten Daten, wenn dies zur Erfüllung seiner Aufgaben gemäß dem Europol-Übereinkommen notwendig ist.

3. Europol hat Zugriff auf die in den Ausschreibungen gemäß Artikel 31 genannten Daten **zu den in den Ausschreibungen genannten Zwecken**, wenn **und soweit** dies zur Erfüllung seiner Aufgaben gemäß dem Europol-Übereinkommen notwendig ist.

Or. de

Begründung

Daten sollen nur verwendet werden zu den in den Ausschreibungen genannten und nicht zu sonstigen Zwecken. Siehe auch Begründung zum Änderungsantrag zu Artikel 18 Absatz 2.

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 235 Artikel 37 Absatz 3

3. Europol hat Zugriff auf die in den Ausschreibungen im Sinne des Artikels 35 enthaltenen Daten, wenn dies zur Durchführung seiner Aufgaben gemäß dem

3. Europol hat Zugriff auf die in den Ausschreibungen im Sinne des Artikels 35 enthaltenen Daten **zu den in den Ausschreibungen genannten Zwecken**,

Europol-Übereinkommen notwendig ist.

wenn **und soweit** dies zur Durchführung seiner Aufgaben gemäß dem Europol-Übereinkommen notwendig ist.

Or. de

Begründung

Daten sollen nur verwendet werden zu den in den Ausschreibungen genannten und nicht zu sonstigen Zwecken. Siehe auch Begründung zum Änderungsantrag zu Artikel 18 Absatz 2.

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 236
Artikel 39 Absatz 1 Buchstaben d und e

**d) Lichtbilder,
e) Fingerabdrücke,**

entfällt

Or. de

Begründung

Die Benutzung biometrischer Daten ist technisch noch nicht ausgereift. Ein fehlerhaftes Funktionieren von SIS II kann aber weit reichende Folgen für den Betroffenen haben. Dies gilt erst Recht für die Benutzung dieser Daten in einer derart großen Datenbank. Nach dem derzeitigen Stand der Technik kann die Funktionssicherheit bei der zu erwartenden großen Datenmenge im SIS II nicht gewährleistet werden. Darüber hinaus hat es auch kein impact assessment bezüglich der Verwendung biometrischer Daten gegeben.

Änderungsantrag von Henrik Lax

Änderungsantrag 237
Artikel 39 a (neu)

Artikel 39a

Besondere Regelungen für Fotos und Fingerabdrücke

1. Fotos und Fingerabdrücke im Sinne von Artikel 16 Absatz 1 Buchstaben d und e dürfen nur in den folgenden Fällen verwendet werden:

a) Fotos und Fingerabdrücke dürfen in den Ausschreibungen nach Absatz 1 nur nach

einer besonderen Qualitätskontrolle enthalten sein, damit sichergestellt wird, dass sie dem Mindestqualitätsstandard für Daten entsprechen, der nach Maßgabe des Artikels 35 festzulegen ist;

b) Fotos und Fingerabdrücke dürfen nur verwendet werden, um die Identifizierung eines Drittstaatsangehörigen anhand einer alphanumerischen Abfrage zu bestätigen;

c) Fingerabdrücke dürfen verwendet werden, um einen Drittstaatsangehörigen zu identifizieren, wenn dieser keine Ausweise oder Reisedokumente mit sich führt.

Or. en

Änderungsantrag von Manfred Weber

Änderungsantrag 238
Artikel 39 a (neu)

Artikel 39a

Ab einem gemäß Artikel 65 festzulegenden Zeitpunkt können auch Fingerabdrücke und Fotos zur Abfrage und Ermittlung, ob eine Person im SIS II ausgeschrieben ist, verwendet werden.

Or. en

Begründung

Dadurch soll eine Abfrage anhand biometrischer Daten ermöglicht werden, wenn die rechtlichen und technischen Voraussetzungen erfüllt sind.

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 239
Artikel 39 a (neu)

Artikel 39a

Die Suche mit biometrischen Daten ist in jedem Fall ausgeschlossen.

Begründung

Siehe Begründung zum Änderungsantrag zu Artikel 39 Absatz 1 Buchstaben d und e. Dieser Änderungsvorschlag versteht sich als Ergänzung zum Änderungsvorschlag des Berichterstatters Coelho zu Artikel 39 a (neu).

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 240
Artikel 40 Absatz 1 a (neu)

1a. Alle Bestimmungen nach Artikel 10 und Artikel 13 sind auf diesen Artikel in vollem Umfang anwendbar.

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 241
Artikel 40 Absatz 3

3. Der Zugriff auf die SIS-II-Daten wird nur im Rahmen der Zuständigkeiten der nationalen Behörde und nur bevollmächtigten Bediensteten gewährt.

3. Der Zugriff auf die SIS-II-Daten wird nur im Rahmen der Zuständigkeiten der nationalen Behörde und nur bevollmächtigten Bediensteten gewährt.
Diese Bediensteten dürfen nur diejenigen Daten abfragen, die sie für die Erfüllung ihrer Aufgaben gemäß dem vorliegenden Beschluss benötigen. Die nationalen Behörden führen eine aktuelle Liste der Personen mit Recht auf Zugriff zum SIS II. Dies gilt auch für Europol und Eurojust und ihre Bediensteten.

Begründung

Die ersten beiden Sätze des Änderungsantrags übernehmen den Änderungsantrag 100 des Berichterstatters zu Artikel 40 Absatz 3. Europol und Eurojust müssen in diesem Zusammenhang denselben Regelungen unterworfen sein wie die Mitgliedstaaten.

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 242

Artikel 43 Absatz 7

7. Die im SIS II gespeicherten Daten werden mindestens einmal jährlich von dem ausschreibenden Mitgliedstaat überprüft. Mitgliedstaaten steht es frei, kürzere Prüffristen festzulegen.

7. Die im SIS II gespeicherten Daten werden mindestens einmal jährlich von dem ausschreibenden Mitgliedstaat überprüft. Mitgliedstaaten steht es frei, kürzere Prüffristen festzulegen. **Die Mitgliedstaaten dokumentieren die Überprüfungen einschließlich der Gründe für die weitere Aufbewahrung der Daten sowie Statistiken über den prozentualen Anteil der Ausschreibungen, die gemäß Artikel 19 Absatz 2, Artikel 25 Absatz 2, Artikel 29 Absatz 2, Artikel 34 Absatz 3 und Artikel 28 Absatz 4 gespeichert und neu eingetragen werden.**

Or. en

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 243

Artikel 46 Absatz 1

1. Ein Mitgliedstaat kann nach Maßgabe des innerstaatlichen Rechts von ihm im SIS II eingegebene Ausschreibungen miteinander verknüpfen. Durch eine solche Verknüpfung werden zwei oder mehr Ausschreibungen miteinander verbunden.

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

Or. de

Begründung

Verknüpfungen sind ein typisches Mittel polizeilicher Fahndungssysteme. Daher sollte ein solcher Mechanismus im SIS II restriktiv angewandt werden. Verknüpfungen sollten sich innerhalb der jeweiligen Ausschreibungsziele halten; die Verknüpfung von Ausschreibungen, die unterschiedlichen Zwecken dienen („Verhaftung und Übergabe mit Europäischem Haftbefehl“ nach Artikel 15, „Sachfahndungsausschreibungen zur Sicherstellung oder

Beweissicherung in Strafverfahren" nach Kapitel VIII dieses Beschlusses, „Verweigerung der Einreise" nach Artikel 15 Absatz 1 des Kommissionsvorschlags für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) KOM(2005)0236)) sollten ausgeschlossen werden.

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 244
Artikel 46 Absatz 2 a (neu)

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

Or. de

Begründung

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

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 245
Artikel 46 Absatz 3

3. Die Verknüpfung beeinträchtigt nicht die in diesem Beschluss festgelegten Zugriffsrechte. Behörden, die auf bestimmte Ausschreibungskategorien keinen Zugriff haben, erhalten keinen Zugang zu den Verknüpfungen zu diesen Kategorien.

3. Die Verknüpfung beeinträchtigt nicht die in diesem Beschluss festgelegten Zugriffsrechte. Behörden, die auf bestimmte Ausschreibungskategorien keinen Zugriff haben, erhalten keinen Zugang zu den Verknüpfungen zu diesen Kategorien ***und können auch keine Verknüpfung zu einer Ausschreibung einsehen, zu der sie keinen Zugriff haben.***

Or. en

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 246
Artikel 46 Absatz 4 a (neu)

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

Or. de

Begründung

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

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 247 Artikel 48

1. Soweit nicht ausdrücklich im EU-Recht vorgesehen, dürfen personenbezogene

Daten, die im SIS II gemäß diesem Beschluss verarbeitet werden, keinem Drittstaat und keiner internationalen Organisation übermittelt oder ihnen zur Verfügung gestellt werden.

2. Abweichend von Absatz 1 dürfen personenbezogene Daten **auf der Grundlage eines Abkommens der Europäischen Union über die justizielle Zusammenarbeit mit Genehmigung des Mitgliedstaats, der die Daten in das SIS II eingegeben hat**, an Drittstaaten oder internationale Organisationen übermittelt werden, wenn **diese einen äquivalenten Schutz der übermittelten personenbezogenen Daten gewährleisten.**

1. **Personenbezogene** Daten, die im SIS II gemäß diesem Beschluss verarbeitet werden, **dürfen keiner nicht-staatlichen Stelle**, keinem Drittstaat und keiner internationalen Organisation übermittelt oder ihnen zur Verfügung gestellt werden.

2. Abweichend von Absatz 1 dürfen personenbezogene Daten an Drittstaaten oder internationale Organisationen übermittelt werden, wenn:

a) diese Datenübermittlung durch ein EU-Gesetz ausdrücklich vorgesehen oder gestattet wird;

b) der Drittstaat oder die internationale Organisation, an die die betreffenden Daten übermittelt werden sollen, ein angemessenes Datenschutzniveau gewährleistet;

c) die Übertragung zu dem Zweck, zu dem die fraglichen Daten erhoben wurden, notwendig ist.

2a. Die Übertragung erfolgt gemäß Artikel 15 des Rahmenbeschlusses XX des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden].

Or. en

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 248
Artikel 48 a (neu)

Artikel 48a

Das SIS II darf erst dann mit anderen Datenbanken verbunden werden, wenn eine gründliche Sicherheitsanalyse durchgeführt worden ist.

Or. en

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 249
Artikel 54 Absatz 2

2. Ist der gemäß Absatz 1 in Anspruch genommene Mitgliedstaat nicht der Mitgliedstaat, der die Daten in das SIS II eingegeben hat, erstattet letzterer auf Ersuchen den bereits gezahlten Schadenersatz, es sein denn, von dem beklagten Mitgliedstaat wurden die Daten in Verletzung dieses Beschlusses genutzt.

2. Ist der gemäß Absatz 1 in Anspruch genommene Mitgliedstaat nicht der Mitgliedstaat, der die Daten in das SIS II eingegeben hat, erstattet letzterer auf Ersuchen den bereits gezahlten Schadenersatz, es sein denn, von dem beklagten Mitgliedstaat wurden die Daten in Verletzung dieses Beschlusses genutzt. ***Es darf nur in einem einzigen Mitgliedstaat Klage erhoben werden.***

Or. en

Begründung

Um ein „Shopping“ zu verhindern, darf es nicht möglich sein, in mehr als einem Mitgliedstaat eine Schadenersatzklage zu erheben.

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 250

Artikel 55

Sanktionen

Jeder Mitgliedstaat stellt sicher, dass eine mit diesem Beschluss unvereinbare Verarbeitung von SIS-II-Daten oder Zusatzinformationen mit wirksamen, angemessenen und abschreckenden Sanktionen nach innerstaatlichem Recht geahndet wird.

Sanktionen *und Straftaten*

Jeder Mitgliedstaat stellt sicher, dass eine mit diesem Beschluss unvereinbare Verarbeitung von SIS-II-Daten oder Zusatzinformationen mit wirksamen, angemessenen und abschreckenden Sanktionen nach innerstaatlichem Recht geahndet wird. ***Schwere Verstöße gelten als Straftat. Die Mitgliedstaaten erlassen entsprechende Vorschriften in ihrem nationalen Recht. Sie teilen der Kommission alle einschlägigen Vorschriften des nationalen Rechts bis zu dem nach Artikel 65 Absatz 2 festzulegenden Zeitpunkt mit und setzen sie unverzüglich über alle nachfolgenden Änderungen in Kenntnis, die damit in Verbindung stehen. Dies gilt auch für Sicherheitsverstöße, die auf Nachlässigkeit und/oder Missbrauch zurückzuführen sind.***

Or. en

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 251

Artikel 64 Absatz 1 a (neu)

1. Die im derzeitigen SIS gespeicherten Daten können erst dann in das neue System übertragen werden, wenn das laufende System geprüft und die darin gespeicherten Daten auf ihre Integrität untersucht worden sind.

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 252

Artikel 64 Absatz 2

2. Die zum gemäß Artikel 65 Absatz 2 festgelegten Zeitpunkt nicht in Anspruch genommenen Beträge des gemäß Artikel 119 des Schengener Übereinkommens angenommenen Haushalts werden an die Mitgliedstaaten zurückgezahlt. Die zurückzuzahlenden Beträge werden auf der Grundlage der Beiträge der Mitgliedstaaten nach Maßgabe des Beschlusses des Exekutivausschusses vom 14. Dezember 1993 bezüglich der Finanzregelung für die Einrichtung und den Betrieb des Schengener C.SIS berechnet.

2. Die zum gemäß Artikel 65 Absatz 2 festgelegten Zeitpunkt nicht in Anspruch genommenen Beträge des gemäß Artikel 119 des Schengener Übereinkommens angenommenen Haushalts werden **für die Überprüfung des laufenden Systems und die Kontrolle der im derzeitigen System gespeicherten Daten verwendet. Alle ausstehenden Beträge werden** an die Mitgliedstaaten zurückgezahlt. Die zurückzuzahlenden Beträge werden auf der Grundlage der Beiträge der Mitgliedstaaten nach Maßgabe des Beschlusses des Exekutivausschusses vom 14. Dezember 1993 bezüglich der Finanzregelung für die Einrichtung und den Betrieb des Schengener C.SIS berechnet.

Änderungsantrag von Tatjana Ždanoka

Änderungsantrag 253

Artikel 65 Absatz 1 Einleitung

1. Dieser Beschluss tritt am zwanzigsten Tag nach seiner Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

1. Dieser Beschluss tritt am zwanzigsten Tag nach seiner Veröffentlichung im Amtsblatt der Europäischen Union in Kraft, **sofern der Rahmenbeschluss zum Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden– Datenschutz im dritten Pfeiler (KOM(2005)475), in Kraft getreten ist.**

Änderungsantrag von Sylvia-Yvonne Kaufmann

Änderungsantrag 254
Artikel 65 Absatz 1 Unterabsatz 2

Er gilt ab dem von der Kommission gemäß den Absätzen 2 und 3 festzusetzenden Zeitpunkt.

Er gilt ab dem von der Kommission gemäß den Absätzen 2 und 3 festzusetzenden Zeitpunkt, ***nicht jedoch bevor der Rahmenbeschluss 2005/XX/JI des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, in Kraft getreten ist.***

Or. de

Begründung

Siehe Begründung zum Änderungsantrag zu Spiegelstrich 1a zum Entwurf einer legislativen Entschließung.

Änderungsantrag von Edith Mastenbroek

Änderungsantrag 255
Artikel 65 Absatz 1 a (neu)

1a. Das SIS II nimmt erst nach erfolgreichem Abschluss eines von der Kommission gemeinsam mit den Mitgliedstaaten durchzuführenden umfassenden Tests des Systems, der Sicherheit des Systems und der Kommunikationsinfrastruktur auf allen Ebenen seinen Betrieb auf. Die Kommission informiert das Europäische Parlament über die Ergebnisse dieses Tests. Falls der Test kein zufrieden stellendes Ergebnis liefert, wird dieser Zeitraum verlängert, bis das ordnungsgemäße Funktionieren des Systems sichergestellt werden kann.

Or. en

Änderungsantrag von Manfred Weber

Änderungsantrag 256
Artikel 65 Absatz 4 a (neu)

3a. Der Zeitpunkt, ab dem Artikel 39a gilt, wird festgelegt, wenn:

a) die erforderlichen Durchführungsbestimmungen erlassen wurden und

b) alle Mitgliedstaaten die Kommission darüber in Kenntnis gesetzt haben, dass sie die notwendigen technischen und rechtlichen Vorkehrungen für die Verwendung von Fingerabdrücken und/oder Fotos zur Abfrage getroffen haben.

Or. en

Begründung

Dient der Kohärenz mit Artikel 16a und um die biometrische Abfrage zu ermöglichen, wenn die Voraussetzungen dafür erfüllt sind.