BESCHLUSS DER KOMMISSION

vom 4. Mai 2010

über den Sicherheitsplan für das zentrale SIS II und die Kommunikationsinfrastruktur

(2010/261/EU)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) [1], insbesondere Artikel 16,

gestützt auf den Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) [2], insbesondere Artikel 16,

in Erwägung nachstehender Gründe:

(1) Artikel 16 der Verordnung (EG) Nr. 1987/2006 und Artikel 16 des Beschlusses 2007/533/JI sehen vor, dass die Verwaltungsbehörde für das zentrale SIS II bzw. die Kommission für die Kommunikationsinfrastruktur die erforderlichen Maßnahmen trifft, einschließlich der Annahme eines Sicherheitsplans.

(2) Artikel 15 Absatz 4 der Verordnung (EG) Nr. 1987/2006 und Artikel 15 Absatz 4 des Beschlusses 2007/533/JI sehen vor, dass während einer Übergangszeit die Kommission für das Betriebsmanagement des zentralen SIS II zuständig ist, bis die Verwaltungsbehörde ihre Aufgaben wahrnimmt.

(3) Da die Verwaltungsbehörde noch nicht geschaffen worden ist, sollte der von der Kommission anzunehmende Sicherheitsplan während einer Übergangszeit auch auf das zentrale SIS II anwendbar sein.

(4) Die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates [3] regelt die Verarbeitung personenbezogener Daten durch die Kommission, wenn diese ihren Aufgaben beim Betriebsmanagement des SIS II nachkommt.

(5) Während der Übergangszeit, bis die Verwaltungsbehörde ihre Aufgaben wahrnimmt, hat die Kommission im Falle einer Übertragung ihrer Zuständigkeit laut Artikel 15 Absatz 7 der Verordnung (EG) Nr. 1987/2006 und Artikel 15 Absatz 7 des Beschlusses 2007/533/JI zu gewährleisten, dass sich dies nicht nachteilig auf die nach dem Gemeinschaftsrecht geltenden Kontrollmechanismen — sei es des Gerichtshofs, des Rechnungshofs oder des Europäischen Datenschutzbeauftragten — auswirkt.

(6) Die Verwaltungsbehörde sollte, sobald sie ihre Aufgaben wahrnimmt, einen eigenen Sicherheitsplan für das zentrale SIS II annehmen. Dieser Sicherheitsplan sollte daher, insoweit er sich auf das zentrale SIS II bezieht, auslaufen, sobald die Verwaltungsbehörde ihre Aufgaben wahrnimmt.

(7) Artikel 4 Absatz 3 der Verordnung (EG) Nr. 1987/2006 und Artikel 4 Absatz 3 des Beschlusses 2007/533/JI sehen vor, dass sich das zentrale SIS (CS-SIS), das für die technische Überwachung und das Management zuständig ist, in Straßburg (Frankreich) befindet, und dass sich ein Backup-CS-SIS, das alle Funktionalitäten des Haupt-CS-SIS bei einem Ausfall dieses Systems übernehmen kann, in Sankt Johann im Pongau (Österreich) befindet.

(8) Der Sicherheitsplan sollte vorsehen, dass ein Beauftragter für die Systemsicherheit sicherheitsbezogene Aufgaben wahrnimmt, die sowohl das zentrale SIS II als auch die Kommunikationsinfrastruktur betreffen, und dass zwei örtliche Sicherheitsbeauftragte sicherheitsbezogene Aufgaben wahrnehmen, die das zentrale SIS II bzw. die Kommunikationsinfrastruktur betreffen. Um im Falle von Sicherheitsvorfällen eine wirksame und rasche Reaktion und Meldung zu ermöglichen, sollte festgelegt werden, welche Aufgaben die Sicherheitsbeauftragten im Einzelnen wahrzunehmen haben.

(9) Es sollte ein Sicherheitsplan eingeführt werden, der sämtliche technischen und organisatorischen Einzelheiten nach Maßgabe dieses Beschlusses regelt.

(10) Es sollten Maßnahmen festgelegt werden, die einen ausreichenden Schutz des Betriebs des zentralen SIS II und der Kommunikationsinfrastruktur sicherstellen —

[1] ABl. L 381 vom 28.12.2006, S. 4.
[2] ABl. L 205 vom 7.8.2007, S. 63.
[3] ABl. L 8 vom 12.1.2001, S. 1.

HAT FOLGENDEN BESCHLUSS ERLASSEN:

KAPITEL I

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand

(1) Dieser Beschluss regelt die Sicherheitsorganisation und -maßnahmen (Sicherheitsplan) zum Schutz des zentralen SIS II und der darin verarbeiteten Daten vor ihrer Verfügbarkeit, ihrer Integrität und ihrer Vertraulichkeit abträglichen Bedrohungen im Sinne von Artikel 16 Absatz 1 der Verordnung (EG) Nr. 1987/2006 und Artikel 16 Absatz 1 des Beschlusses 2007/533/JI über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) während einer Übergangszeit, bis die Verwaltungsbehörde ihre Aufgaben wahrnimmt.

(2) Dieser Beschluss regelt die Sicherheitsorganisation und -maßnahmen (Sicherheitsplan) zum Schutz der Kommunikationsinfrastruktur vor ihrer Verfügbarkeit, ihrer Integrität und ihrer Vertraulichkeit abträglichen Bedrohungen im Sinne von Artikel 16 der Verordnung (EG) Nr. 1987/2006 und Artikel 16 des Beschlusses 2007/533/JI über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II).

KAPITEL II

ORGANISATION, ZUSTÄNDIGKEITEN UND VORFALLMANAGEMENT

Artikel 2

Aufgaben der Kommission

(1) Die Kommission führt sämtliche in diesem Beschluss genannten Maßnahmen für die Sicherheit des zentralen SIS II durch und überwacht ihre Wirksamkeit.

(2) Die Kommission führt sämtliche in diesem Beschluss genannten Maßnahmen für die Sicherheit der Kommunikationsinfrastruktur durch und überwacht ihre Wirksamkeit.

(3) Die Kommission benennt einen ihrer Beamten als Beauftragten für die Systemsicherheit. Seine Ernennung erfolgt durch den Generaldirektor der Generaldirektion „Justiz, Freiheit und Sicherheit" der Kommission. Der Beauftragte für die Systemsicherheit nimmt insbesondere folgende Aufgaben wahr:

a) Ausarbeitung des in Artikel 7 dieses Beschlusses beschriebenen Sicherheitsplans,

b) Überwachung der Wirksamkeit der Sicherheitsverfahren für das zentrale SIS II,

c) Überwachung der Wirksamkeit der Sicherheitsverfahren für die Kommunikationsinfrastruktur,

d) Mitwirkung bei der Berichterstattung über die Sicherheit des Systems gemäß Artikel 50 der Verordnung (EG) Nr. 1987/2006 und Artikel 66 des Beschlusses 2007/533/JI,

e) Koordinierung und Unterstützung der vom Europäischen Datenschutzbeauftragten vorgenommenen Kontrollen und Prüfungen gemäß Artikel 45 der Verordnung (EG) Nr. 1987/2006 und Artikel 61 des Beschlusses 2007/533/JI sowie Meldung von Vorfällen im Sinne von Artikel 5 Absatz 2 an den Datenschutzbeauftragten der Kommission,

f) Überwachung im Hinblick auf eine ordnungsgemäße und vollständige Umsetzung dieses Beschlusses und des Sicherheitsplans durch etwaige, in gleich welcher Form an der Verwaltung des zentralen SIS II beteiligte Auftragnehmer einschließlich Unterauftragnehmer,

g) Überwachung im Hinblick auf eine ordnungsgemäße und vollständige Umsetzung dieses Beschlusses und des Sicherheitsplans durch etwaige, in gleich welcher Form an der Verwaltung der Kommunikationsinfrastruktur beteiligte Auftragnehmer einschließlich Unterauftragnehmer,

h) Pflege einer Liste der nationalen Anlaufstellen für die Sicherheit des SIS II und Verteilung der Liste an den örtlichen Sicherheitsbeauftragten für die Kommunikationsinfrastruktur,

i) Übermittlung der unter Buchstabe h genannten Liste an den örtlichen Sicherheitsbeauftragten für das zentrale SIS II.

Artikel 3

Örtlicher Sicherheitsbeauftragter für das zentrale SIS II

(1) Unbeschadet der Bestimmungen von Artikel 8 benennt die Kommission einen ihrer Beamten als örtlichen Sicherheitsbeauftragten für das zentrale SIS II. Interessenkonflikte zwischen den Pflichten des örtlichen Sicherheitsbeauftragten und sonstigen dienstlichen Pflichten sind zu vermeiden. Die Ernennung des örtlichen Sicherheitsbeauftragten für das zentrale SIS II erfolgt durch den Generaldirektor der Generaldirektion „Justiz, Freiheit und Sicherheit" der Kommission.

(2) Der örtliche Sicherheitsbeauftragte für das zentrale SIS II stellt sicher, dass die in diesem Beschluss genannten Sicherheitsmaßnahmen für das Haupt-CS-SIS durchgeführt und die Sicherheitsverfahren eingehalten werden. In Bezug auf das Backup-CS-SIS stellt der örtliche Sicherheitsbeauftragte für das zentrale SIS II zudem sicher, dass mit Ausnahme der in Artikel 9 genannten Maßnahmen die in diesem Beschluss genannten Sicherheitsmaßnahmen durchgeführt und die einschlägigen Sicherheitsverfahren eingehalten werden.

(3) Der örtliche Sicherheitsbeauftragte für das zentrale SIS II kann ihm übertragene Aufgaben Untergebenen zuweisen. Interessenkonflikte zwischen diesen Aufgaben und sonstigen dienstlichen Pflichten sind zu vermeiden. Der örtliche Sicherheitsbeauftragte bzw. sein diensthabender Untergebener muss jederzeit über eine einheitliche Telefonnummer und Adresse erreichbar sein.

(4) Der örtliche Sicherheitsbeauftragte für das zentrale SIS II nimmt innerhalb der in Absatz 1 genannten Grenzen die Aufgaben wahr, die sich aus den am Standort des Haupt- bzw. Backup-CS-SIS zu ergreifenden Sicherheitsmaßnahmen ergeben; dabei handelt es sich insbesondere um

a) Aufgaben im Zusammenhang mit der Wahrung der örtlichen Betriebssicherheit (u.a. Prüfung der Firewall, regelmäßige Sicherheitsprüfung, Audits und Berichterstattung),

b) die Überwachung der Wirksamkeit des Notfallplans und die Ansetzung regelmäßiger Übungen,

c) die Dokumentierung etwaiger im zentralen SIS II aufgetretener Vorfälle mit möglichen Auswirkungen auf die Sicherheit des zentralen SIS II oder der Kommunikationsinfrastruktur und ihre Meldung an den Beauftragten für die Systemsicherheit,

d) die Benachrichtigung des Beauftragten für die Systemsicherheit, falls der Sicherheitsplan geändert werden muss,

e) die Überwachung der Umsetzung dieses Beschlusses und des Sicherheitsplans durch etwaige, in gleich welcher Form am Betriebsmanagement des zentralen SIS II beteiligte Auftragnehmer einschließlich Unterauftragnehmer,

f) die Sicherstellung, dass das Personal über seine Pflichten aufgeklärt wird und die Überwachung der Umsetzung des Sicherheitsplans,

g) die Überwachung der IT-Sicherheitsentwicklungen und die Sicherstellung einer entsprechenden Personalschulung,

h) die Zusammenstellung von Hintergrundinformationen und die Ausarbeitung von Vorgehensmöglichkeiten für die Entwicklung, die Aktualisierung und die Überprüfung des in Artikel 7 beschriebenen Sicherheitsplans.

Artikel 4

Örtlicher Sicherheitsbeauftragter für die Kommunikationsinfrastruktur

(1) Unbeschadet der Bestimmungen von Artikel 8 benennt die Kommission einen ihrer Beamten als örtlichen Sicherheitsbeauftragten für die Kommunikationsinfrastruktur. Interessenkonflikte zwischen den Pflichten des örtlichen Sicherheitsbeauftragten und sonstigen dienstlichen Pflichten sind zu vermeiden. Die Ernennung des örtlichen Sicherheitsbeauftragten für die Kommunikationsinfrastruktur erfolgt durch den Generaldirektor der Generaldirektion „Justiz, Freiheit und Sicherheit" der Kommission.

(2) Der örtliche Sicherheitsbeauftragte für die Kommunikationsinfrastruktur überwacht den Betrieb der Kommunikationsinfrastruktur und stellt sicher, dass die Sicherheitsmaßnahmen durchgeführt und die Sicherheitsverfahren eingehalten werden.

(3) Der örtliche Sicherheitsbeauftragte für die Kommunikationsinfrastruktur kann ihm übertragene Aufgaben Untergebenen zuweisen. Interessenkonflikte zwischen diesen Aufgaben und sonstigen dienstlichen Pflichten sind zu vermeiden. Der örtliche Sicherheitsbeauftragte bzw. sein diensthabender Untergebener muss jederzeit über eine einheitliche Telefonnummer und Adresse erreichbar sein.

(4) Der örtliche Sicherheitsbeauftragte für die Kommunikationsinfrastruktur nimmt die Aufgaben wahr, die sich aus den bei der Kommunikationsinfrastruktur zu ergreifenden Sicherheitsmaßnahmen ergeben; dabei handelt es sich insbesondere um:

a) sämtliche im Zusammenhang mit der Betriebssicherheit der Kommunikationsinfrastruktur stehende Aufgaben (u.a. Prüfung der Firewall, regelmäßige Sicherheitsprüfung, Audits und Berichterstattung),

b) die Überwachung der Wirksamkeit des Notfallplans und die Ansetzung regelmäßiger Übungen,

c) die Dokumentierung etwaiger in der Kommunikationsinfrastruktur aufgetretener Vorfälle mit möglichen Auswirkungen auf die Sicherheit des zentralen SIS II oder der Kommunikationsinfrastruktur und ihre Meldung an den Beauftragten für die Systemsicherheit,

d) die Benachrichtigung des Beauftragten für die Systemsicherheit, falls der Sicherheitsplan geändert werden muss,

e) die Überwachung der Umsetzung dieses Beschlusses und des Sicherheitsplans durch etwaige, in gleich welcher Form an Verwaltung und Betrieb der Kommunikationsinfrastruktur beteiligte Auftragnehmer einschließlich Unterauftragnehmer,

f) die Sicherstellung, dass das Personal über seine Pflichten aufgeklärt wird und die Überwachung der Umsetzung des Sicherheitsplans,

g) die Überwachung der IT-Sicherheitsentwicklungen und die Sicherstellung einer entsprechenden Personalschulung,

h) die Zusammenstellung von Hintergrundinformationen und die Ausarbeitung von Vorgehensmöglichkeiten für die Entwicklung, die Aktualisierung und die Überprüfung des in Artikel 7 beschriebenen Sicherheitsplans.

Artikel 5

Sicherheitsvorfälle

(1) Jedwedes Ereignis, das sich auf die Sicherheit des Betriebs des SIS II auswirkt bzw. auswirken kann, das SIS II beschädigen oder dessen Ausfall nach sich ziehen kann, ist als Sicherheitsvorfall anzusehen; dies gilt insbesondere, wenn möglicherweise ein Datenzugriff erfolgt ist oder (möglicherweise) die Verfügbarkeit, die Integrität und die Vertraulichkeit von Daten nicht mehr gewährleistet gewesen ist.

(2) Sicherheitsvorfällen ist durch eine rasche, wirksame und geeignete Reaktion nach Maßgabe des Sicherheitsplans zu begegnen. Es sind Verfahren zur Wiederherstellung der Sicherheit nach einem Vorfall vorzusehen.

(3) Informationen über Sicherheitsvorfälle, die sich auf den Betrieb des SIS II in einem Mitgliedstaat oder auf die Verfügbarkeit, die Integrität und die Vertraulichkeit der von einem Mitgliedstaat eingegebenen oder übermittelten Daten auswirken bzw. auswirken können, sind an den betreffenden Mitgliedstaat zu übermitteln. Sicherheitsvorfälle sind dem Datenschutzbeauftragten der Kommission zu melden.

Artikel 6

Vorfallmanagement

(1) Alle an der Entwicklung, an der Verwaltung und am Betrieb des SIS II beteiligten Mitarbeiter und Auftragnehmer haben etwaige von ihnen beobachtete oder vermutete Sicherheitsmängel der Kommunikationsinfrastruktur zu beachten und je nach Fall dem Beauftragten für die Systemsicherheit oder dem örtlichen Sicherheitsbeauftragten für die Kommunikationsinfrastruktur zu melden.

(2) Bei Aufdeckung eines Vorfalls, der sich auf die Sicherheit des SIS II auswirkt oder auswirken könnte, informiert der örtliche Sicherheitsbeauftragte für die Kommunikationsinfrastruktur so rasch wie möglich den Beauftragten für die Systemsicherheit sowie gegebenenfalls die nationale Anlaufstelle für die Sicherheit des SIS II (falls eine solche Stelle in dem betreffenden Mitgliedstaat existiert) in schriftlicher Form bzw. — in dringenden Fällen — über sonstige Kommunikationskanäle. Der betreffende Bericht hat eine Beschreibung des Sicherheitsvorfalls, der Gefahrenstufe, der möglichen Folgen und der bereits ergriffenen oder zu ergreifenden Gefahrenminderungsmaßnahmen zu umfassen.

(3) Etwaige Beweise für den Sicherheitsvorfall sind unverzüglich vom örtlichen Sicherheitsbeauftragten für die Kommunikationsinfrastruktur sicherzustellen. So weit es die geltenden Datenschutzbestimmungen zulassen, sind diese Beweise dem Beauftragten für die Systemsicherheit auf Antrag vorzulegen.

(4) Im Sicherheitsplan sind geeignete Rückmeldungsverfahren vorzusehen, durch die sichergestellt wird, dass der Beauftragte für die Systemsicherheit und der örtliche Sicherheitsbeauftragte für die Kommunikationsinfrastruktur nach Behandlung und Abstellung eines Vorfalls über die Art und die Behandlung des Vorfalls sowie über die betreffenden Ergebnisse informiert werden.

(5) Die Absätze 1 bis 4 sind *mutatis mutandis* auf Vorfälle im zentralen SIS II anwendbar. In diesem Rahmen ist jede in den Absätzen 1 bis 4 erfolgende Bezugnahme auf den örtlichen Sicherheitsbeauftragten für die Kommunikationsinfrastruktur als Bezugnahme auf den örtlichen Sicherheitsbeauftragten für das zentrale SIS II zu betrachten.

KAPITEL III

SICHERHEITSMASSNAHMEN

Artikel 7

Sicherheitsplan

(1) Der Generaldirektor der Generaldirektion „Justiz, Freiheit und Sicherheit“ erlässt einen verbindlichen Sicherheitsplan nach Maßgabe dieses Beschlusses und aktualisiert und überprüft diesen regelmäßig. Der Sicherheitsplan hat detaillierte Verfahren und Maßnahmen zum Schutz vor der Verfügbarkeit, der Integrität und der Vertraulichkeit der Kommunikationsinfrastruktur abträglichen Bedrohungen vorzusehen und eine Notfallplanung einzuschließen, damit eine ausreichende Sicherheit im Sinne dieses Beschlusses sichergestellt ist. Der Sicherheitsplan hat im Einklang mit diesem Beschluss zu stehen.

(2) Der Sicherheitsplan hat sich auf eine Risikobewertung zu gründen. Die im Sicherheitsplan vorgesehenen Maßnahmen müssen den ermittelten Risiken angemessen sein.

(3) Die Risikobewertung und der Sicherheitsplan sind zu aktualisieren, wenn technologische Änderungen, neue Bedrohungen oder sonstige Umstände dies erforderlich machen. Unabhängig davon ist der Sicherheitsplan alljährlich zu überprüfen, um sicherzustellen, dass er nach wie vor in geeigneter Weise der jüngsten Risikobewertung, der neuesten technologischen Entwicklung und den aktuellen Bedrohungen und sonstigen maßgeblichen Umständen Rechnung trägt.

(4) Der Sicherheitsplan wird vom Beauftragten für die Systemsicherheit in Absprache mit dem örtlichen Sicherheitsbeauftragten für das zentrale SIS II und dem örtlichen Sicherheitsbeauftragten für die Kommunikationsinfrastruktur ausgearbeitet.

(5) Die Absätze 1 bis 4 sind *mutatis mutandis* auf den Sicherheitsplan für das zentrale SIS II anwendbar. In diesem Rahmen ist jede in den Absätzen 1 bis 4 erfolgende Bezugnahme auf den örtlichen Sicherheitsbeauftragten für die Kommunikationsinfrastruktur als Bezugnahme auf den örtlichen Sicherheitsbeauftragten für das zentrale SIS II zu betrachten.

Artikel 8

Umsetzung der Sicherheitsmaßnahmen

(1) Die Umsetzung der in diesem Beschluss und im Sicherheitsplan vorgesehenen Aufgaben und Anforderungen einschließlich der Benennung eines örtlichen Sicherheitsbeauftragten kann per Auftrag oder Delegation privaten oder öffentlichen Einrichtungen anvertraut werden.

(2) In diesem Fall stellt die Kommission im Wege einer rechtsverbindlichen Vereinbarung sicher, dass die Anforderungen dieses Beschlusses und des Sicherheitsplans in vollem Umfang erfüllt werden. Falls die Aufgabe der Benennung eines örtlichen Sicherheitsbeauftragten im Rahmen eines Auftrags oder einer Delegation umgesetzt wird, stellt die Kommission im Wege einer rechtsverbindlichen Vereinbarung sicher, dass sie bezüglich der als örtlicher Sicherheitsbeauftragter zu benennenden Person zu Rate gezogen wird.

Artikel 9

Kontrolle des Zugangs zu Datenverarbeitungseinrichtungen

(1) Zum Schutz von Bereichen, in denen sich Datenverarbeitungseinrichtungen befinden, sind Sicherheitszonen mit geeigneten Sperren und Zugangskontrollen einzurichten.

(2) Innerhalb der Sicherheitszonen sind Sicherheitsbereiche zum Schutz der physischen Bestandteile (Sachanlagen) einschließlich Hardware, Datenträger, Konsolen und Pläne und sonstige Dokumente über das SIS II sowie der Büroräume und sonstigen Arbeitsplätze des mit dem Betrieb des SIS II befassten Personals. Diese Bereiche sind durch geeignete Zugangskontrollen zu schützen, so dass nur befugtem Personal Zugang gewährt wird. Sämtliche in Sicherheitsbereichen durchgeführten Arbeiten unterliegen den ausführlichen Sicherheitsbestimmungen, die im Sicherheitsplan festgelegt wurden.

(3) Für die physische Sicherheit von Büro- und sonstigen Räumen sowie Einrichtungen sind geeignete Sicherheitsvorkehrungen vorzusehen und zu treffen. Zugangspunkte wie Liefer- und Ladezonen und sonstige Punkte, an denen Unbefugte die betreffenden Gebäude oder Bereiche betreten könnten, sind zu kontrollieren und nach Möglichkeit von Datenverarbeitungseinrichtungen zu isolieren, um jedweden unerlaubten Zugriff zu vermeiden.

(4) Für die Sicherheitszone ist ein dem bestehenden Risiko angemessener physischer Schutz vor Beschädigung durch eine Naturkatastrophe oder eine vom Menschen verursachte Katastrophe zu konzipieren und anzuwenden.

(5) Ausrüstung ist vor physischen Bedrohungen, Umweltbedrohungen und unerlaubtem Zugriff zu schützen.

(6) Falls der Kommission die betreffenden Informationen vorliegen, fügt sie der in Artikel 2 Absatz 2 Buchstabe f genannten Liste eine Anlaufstelle für die Überwachung der Umsetzung dieses Artikels am Standort des Backup-CS-SIS hinzu.

Artikel 10

Kontrolle von Datenträgern und anderen wichtigen Komponenten

(1) Wechseldatenträger, die Daten enthalten, sind vor Zugriff durch Unbefugte, vor Missbrauch und vor Zerstörung zu schützen, und ihre Lesbarkeit ist während der gesamten Lebensdauer der Daten sicherzustellen.

(2) Nicht mehr benötigte Datenträger sind nach Maßgabe der im Sicherheitsplan festzulegenden ausführlichen Verfahrensbestimmungen sicher zu entsorgen.

(3) Durch Bestandsaufnahmen ist sicherzustellen, dass Informationen über den Speicherort, die geltende Vorhaltezeit und die Zugangsermächtigungen verfügbar sind.

(4) Es sind alle wichtigen Komponenten der Kommunikationsinfrastruktur zu ermitteln, damit sie ihrer Bedeutung entsprechend geschützt werden können. Ferner ist ein aktuelles Verzeichnis der einschlägigen IT-Ausrüstung zu führen.

(5) Es muss eine auf dem neuesten Stand befindliche Dokumentation der Kommunikationsinfrastruktur verfügbar sein. Die Dokumentation ist vor Zugriff durch Unbefugte zu schützen.

(6) Die Absätze 1 bis 5 sind *mutatis mutandis* auf das zentrale SIS II anwendbar. In diesem Rahmen ist jede Bezugnahme auf die Kommunikationsinfrastruktur als Bezugnahme auf das zentrale SIS II zu betrachten.

Artikel 11

Speicherkontrolle

(1) Es sind geeignete Maßnahmen zu treffen, die eine ordnungsgemäße Datenspeicherung sicherstellen und unerlaubten Zugriff auf die Daten verhindern.

(2) Sämtliche Ausrüstungsgegenstände, die Speichermedien enthalten, sind vor ihrer Entsorgung zu prüfen, um sicherzustellen, dass sensible Daten gelöscht oder vollständig überschrieben wurden oder sicher zu vernichten.

Artikel 12

Passwortkontrolle

(1) Passwörter sind sicher aufzubewahren und vertraulich zu behandeln. Bei Verdacht, dass ein Passwort offengelegt worden ist, ist das Passwort unverzüglich zu ändern oder das betreffende Konto zu deaktivieren. Es sind persönliche, eindeutige Benutzerkennungen zu verwenden.

(2) Im Sicherheitsplan sind geeignete An- und Abmeldeverfahren vorzusehen, um jedweden Zugang durch Unbefugte zu verhindern.

Artikel 13

Zugangskontrolle

(1) Im Sicherheitsplan ist ein förmliches An- und Abmeldeverfahren einzuführen, über das Mitarbeitern zu den Zwecken des Betriebsmanagements der Zugang zu Hard- und Software des SIS II erteilt bzw. entzogen werden kann. Die Zuteilung und Verwendung entsprechender Anmeldeinformationen (Passwort oder dergleichen) ist über ein im Sicherheitsplan festzulegendes förmliches Verfahren zu kontrollieren.

(2) Der Zugang zu Hard- und Software des SIS II am zentralen SIS

i) ist auf befugte Personen zu beschränken,

ii) ist auf die Fälle zu begrenzen, in denen ein legitimer Zweck nach Artikel 45 der Verordnung (EG) Nr. 1987/2006 und Artikel 61 des Beschlusses 2007/533/JI oder nach Artikel 50 Absatz 2 der Verordnung (EG) Nr. 1987/2006 und Artikel 66 Absatz 2 des Beschlusses 2007/533/JI verfolgt wird,

iii) darf, was seine Dauer und seinen Umfang anbelangt, nicht über das für die Zwecke des Zugangs erforderliche Maß hinausgehen und

iv) darf nur nach Maßgabe eines im Sicherheitsplan festzulegenden Zugangskontrollverfahrens erfolgen.

(3) Am zentralen SIS dürfen ausschließlich die vom örtlichen Sicherheitsbeauftragten für das zentrale SIS II zugelassenen Konsolen und Softwareanwendungen verwendet werden. Die Verwendung von Systemprogrammen, mit denen System- und Softwareeinstellungen überschrieben werden können, ist einzuschränken und zu kontrollieren. Es sind Verfahren zur Kontrolle der Softwareinstallation vorzusehen.

Artikel 14

Kommunikationskontrolle

Die Kommunikationsinfrastruktur ist zu überwachen, um die Verfügbarkeit, die Integrität und die Vertraulichkeit des Informationsaustausches zu gewährleisten. Zum Schutz der über die Kommunikationsinfrastruktur übertragenen Daten sind kryptografische Mittel einzusetzen.

Artikel 15

Kontrolle der Dateneingabe

Die Benutzerkonten der zum Zugriff auf die Software des SIS II vom zentralen SIS berechtigten Personen ist vom örtlichen Sicherheitsbeauftragten für das zentrale SIS II zu überwachen. Die Nutzung dieser Konten ist einschließlich Dauer und Benutzerkennung zu erfassen.

Artikel 16

Transportkontrolle

(1) Im Sicherheitsplan sind geeignete Maßnahmen festzulegen, durch die vermieden wird, dass personenbezogene Daten bei der Übertragung zum oder vom SIS II oder während des Transports von Datenträgern von Unbefugten gelesen, kopiert, verändert oder gelöscht werden können. Ferner ist im Sicherheitsplan festzulegen, welche Versand- bzw. Transportarten zulässig und welche Haftungsbestimmungen beim Transport und bei der Ankunft von Datenträgern am Zielort zu beachten sind. Die Datenträger dürfen keine anderen als die zu übermittelnden Daten enthalten.

(2) Von Dritten erbrachte Dienstleistungen, die den Zugriff auf Daten, die Verarbeitung und Übermittlung von Daten oder die Verwaltung von Datenverarbeitungseinrichtungen einschließen oder durch die zusätzliche Erzeugnisse oder Dienstleistungen für Datenverarbeitungseinrichtungen bereitgestellt werden, müssen ausreichende integrierte Sicherheitskontrollen beinhalten.

Artikel 17

Sicherheit der Kommunikationsinfrastruktur

(1) Die Kommunikationsinfrastruktur ist in geeigneter Weise zu verwalten und zu kontrollieren, um sie vor Bedrohungen zu schützen und um ihre Sicherheit sowie die des zentralen SIS II einschließlich der darüber ausgetauschten Daten sicherzustellen.

(2) Die für sämtliche Netzdienste geltenden Anforderungen in Bezug auf Sicherheitsmerkmale, Dienstgüte und Verwaltung sind in der Netzdienstevereinbarung mit dem Dienstanbieter festzulegen.

(3) Neben den Zugangspunkten zum SIS II sind auch etwaige zusätzliche von der Kommunikationsinfrastruktur genutzte Dienste zu schützen. Die betreffenden Maßnahmen sind im Sicherheitsplan festzulegen.

Artikel 18

Überwachung

(1) Die Protokolldateien, in denen die in Artikel 18 Absatz 1 der Verordnung (EG) Nr. 1987/2006 und in Artikel 18 Absatz 1 des Beschlusses 2007/533/JI genannten Informationen über jedweden Zugriff auf das zentrale SIS und jeden darüber erfolgenden Austausch von personenbezogenen Daten aufgezeichnet werden, sind sicher aufzubewahren und müssen während der in Artikel 18 Absatz 3 der Verordnung (EG) Nr. 1987/2006 und Artikel 18 Absatz 3 des Beschlusses 2007/533/JI genannten Frist vom Standort des Haupt-CS-SIS und des Backup-CS-SIS zugänglich sein.

(2) Die Verfahrensvorschriften für die Überwachung der Datenverarbeitungseinrichtungen und die Erfassung etwaiger dabei auftretender Fehler sind im Sicherheitsplan festzulegen, und die Überwachungsergebnisse sind regelmäßig zu prüfen. Erforderlichenfalls sind geeignete Maßnahmen zu treffen.

(3) Die Protokollierungseinrichtungen und die Protokolldateien sind vor Manipulation und unbefugtem Zugriff zu schützen, damit die für die Vorhaltefrist geltenden Anforderungen in Bezug auf die Datensammlung und -vorhaltung eingehalten werden.

Artikel 19

Kryptografische Maßnahmen

Falls es zum Schutz von Informationen erforderlich ist, ist auf kryptografische Maßnahmen zurückzugreifen. Der Einsatz derartiger Maßnahmen einschließlich der dabei verfolgten Zwecke und geltenden Bedingungen bedarf der vorherigen Genehmigung durch den Beauftragten für die Systemsicherheit.

KAPITEL IV

PERSONALSICHERHEIT

Artikel 20

Personalprofile

(1) Im Sicherheitsplan sind die Aufgaben und die Zuständigkeiten der zum Zugang zum zentralen SIS II berechtigten Personen festzulegen.

(2) Im Sicherheitsplan sind die Aufgaben und die Zuständigkeiten der zum Zugang zur Kommunikationsinfrastruktur berechtigten Personen festzulegen.

(3) Die Sicherheitsaufgaben und -befugnisse der mit dem Betriebsmanagement befassten Kommissionsbediensteten, Auftragnehmer und sonstigen Mitarbeiter sind zu definieren, zu dokumentieren und den betreffenden Personen mitzuteilen. Bei Kommissionspersonal sind diese Aufgaben und Befugnisse in der Tätigkeitsbeschreibung und in den Zielen festzuhalten, bei Auftragnehmern in den betreffenden Verträgen bzw. Dienstgütevereinbarungen.

(4) Mit Personen, die keinen Vorschriften für den öffentlichen Dienst in der Europäischen Union oder einem Mitgliedstaat unterliegen, sind Vertraulichkeits- bzw. Geheimhaltungsvereinbarungen zu schließen. Mitarbeiter, die mit SIS-II-Daten umgehen sollen, müssen sicherheitsüberprüft oder nach Maßgabe der ausführlichen, im Sicherheitsplan festzulegenden Verfahrensverfahren zertifiziert sein.

Artikel 21

Information des Personals

(1) Alle Mitarbeiter und Auftragnehmer sind ihren Aufgaben entsprechend zu schulen (Sicherheitsbewusstsein, rechtliche Anforderungen, politische Strategien und Verfahren).

(2) Ferner ist im Sicherheitsplan festzulegen, welchen Pflichten Mitarbeiter und Auftragnehmer beim Ablauf ihres Beschäftigungs- bzw. Vertragsverhältnisses in Bezug auf einen etwaigen Arbeitsplatzwechsel oder die Beendigung des Arbeitsverhältnisses unterliegen und welche Verfahrensvorschriften für die Hardwarerückgabe und den Entzug von Zugangsrechten gelten.

KAPITEL V

SCHLUSSBESTIMMUNG

Artikel 22

Anwendbarkeit

(1) Dieser Beschluss wird an dem vom Rat gemäß Artikel 55 Absatz 2 der Verordnung (EG) Nr. 1987/2006 und Artikel 71 Absatz 2 des Beschlusses 2007/533/JI festgelegten Zeitpunkt wirksam.

(2) Artikel 1 Absatz 1, Artikel 2 Absatz 1, Artikel 2 Absatz 3 Buchstabe b, d, f und i, Artikel 3, Artikel 6 Absatz 5, Artikel 7 Absatz 5, Artikel 9 Absatz 6, Artikel 10 Absatz 6, Artikel 13 Absätze 2 und 3, Artikel 15, Artikel 18 und Artikel 20 Absatz 1 gelten, bis die Verwaltungsbehörde ihre Aufgaben aufnimmt.

Brüssel, den 4. Mai 2010

Für die Kommission

Der Präsident

José Manuel BARROSO