BERICHT

Gemeinsame Kontrollinstanz Schengen

Tätigkeitsbericht Dezember 2005 - Dezember 2008

INHALT

Vorwort 3

1. Einleitung 5

2. Neue Entwicklungen: SIS II 7

2.1. Migration vom SIS I+ zum SIS II 9

2.2. Erweiterung des Schengen-Raums 10

3. Kontrolltätigkeit 13

3.1. Überprüfung der Anwendung von Artikel 99 13

3.2. Überprüfung der Anwendung von Artikel 111 15

3.3. Nachkontrolle des Audits zur Anwendung von Artikel 96 19

4. Stellungnahmen der Gemeinsamen Kontrollinstanz 23

4.1. Auslegung des Artikels 111 des Schengener Durchführungsübereinkommens (SDÜ) 23

4.2. Stellungnahmen zur Anwendung des Artikels 102a (SCHAC 2501/07)/ SCHAC 2504/08 27

4.3. Stellungnahme zur Einrichtung eines der Weiterleitung von SIRENE-Nachrichten dienenden Mail-Servers als zentraler Verteiler bei der technischen Unterstützungseinheit C.SIS (SCHAC 2502/07) 29

4.4. Stellungnahme zu dem Entwurf von Durchführungsmaßnahmen einschließlich des SIRENE-Handbuchs für die zweite Generation des Schengener Informationssystems (SCHAC 2503/07) 31

4.5. Stellungnahme zu den Grundsätzen für die Zusammenarbeit zwischen den nationalen Kontrollinstanzen auf der Grundlage des SDÜ 33

4.6. Stellungnahme zum Schengener Informationssystem (SIS) und zu gewalttätigen Störern 08/10 35

5. Rechte der Betroffenen 38

6. Zukunft der gemeinsamen Überwachung 40

7. Mitglieder der Gemeinsamen Kontrollinstanz Schengen 43

8. Beobachter der Gemeinsamen Kontrollinstanz Schengen 45

Vorwort

Der Schengen-Raum kann als große Errungenschaft bei der Schaffung eines Raums ohne Grenzen in Europa betrachtet werden. Alle Menschen in diesem Raum sind von den Fragen betreffend ihre Sicherheit und die Achtung ihrer Privatsphäre und ihrer Rechte, einschließlich des Rechts auf Schutz ihrer persönlichen Daten, betroffen.

Alle nationalen Datenschutzbehörden, die in der Gemeinsamen Kontrollinstanz Schengen zusammenarbeiten, haben ihre Entschlossenheit zum Ausdruck gebracht, die Privatsphäre des Einzelnen angesichts des enormen Volumens der vom Schengener Informationssystem verarbeiteten personenbezogenen Daten zu schützen.

Während des hier erfassten Dreijahreszeitraums (Dezember 2005 - Dezember 2008) galt unser Hauptaugenmerk der korrekten Auslegung des Schengener Übereinkommens, und wir haben evaluiert, ob die Schengen-Staaten diesen Rechtsrahmen auf harmonisierte und angemessene Weise durchgeführt haben.

Die Schengen-Staaten, deren gemeinsames Ziel es ist, den Menschen durch spezifische Grenz- und andere Kontrollen im Schengen-Raum ein hohes Maß an Sicherheit zu bieten, haben darüber hinaus verschiedene neue Politiken im Bereich der Einwanderungskontrolle und der Bekämpfung der schweren Kriminalität entwickelt. Diese neuen Entwicklungen haben dazu geführt, dass die nationalen Datenschutzbehörden ihre Zusammenarbeit verbessert und Leistungsvergleiche der besten Praktiken eingeführt haben. Die Gemeinsame Kontrollinstanz (GK) hat hinsichtlich einiger dieser neuen Entwicklungen Bedenken geäußert.

Wir stehen nun vor zwei großen Herausforderungen: zum einen der Erweiterung des Schengen-Raums unter Betonung des Erfordernisses einer besseren Harmonisierung zwischen allen Schengen-Staaten und zum anderen der Entwicklung des Schengener Informationssystems der zweiten Generation (SIS II), einschließlich der komplexen Migration vom derzeitigen zum neuen System.

Der vorliegende Bericht spiegelt ferner die Arbeit aller nationalen Datenschutzbehörden und den hervorragenden Beitrag des Sekretariats zur Förderung einer besseren Harmonisierung und eines besseren Verständnisses der Mitgliedstaaten untereinander wider.

Unsere allergrößte Herausforderung wird jedoch nach wie vor sein, allen Entwicklungen bei der Bekämpfung der Kriminalität und der illegalen Einwanderung Rechnung zu tragen, und zwar durch Schaffung eines europäischen Rechtsraums, durch mehr Sicherheit für alle mittels Erkennung der Gefahren durch Terrorismus und schwere Kriminalität sowie durch ein ausgewogenes Verhältnis zwischen Sicherheit und Schutz der Privatsphäre.

Georges de LA LOYÈRE
Vorsitzender der Gemeinsamen Kontrollinstanz Schengen

1. EINLEITUNG

Die Bürger der Europäischen Union haben das Recht, uneingeschränkt von einem Land ins andere zu reisen. Obwohl dieses Recht auf die Anfänge der EU zurückgeht, wurde es durch die Abschaffung der Binnengrenzen in der EU nach dem Schengener Übereinkommen zur Realität und bot nun eine größere Freizügigkeit – ein Privileg für EU-Bürger. Es lag auf der Hand, dass angemessene Ausgleichsmaßnahmen für den Wegfall der Binnengrenzen gefunden werden mussten, damit die EU ein Raum der Freiheit, der Sicherheit und des Rechts bleiben konnte. Die Abschaffung einer Sicherungsmaßnahme führte zur Schaffung einer anderen - dem Schengener Informationssystem - zur Verarbeitung personenbezogener Daten im Hinblick auf die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung, einschließlich der nationalen Sicherheit, im Hoheitsgebiet der Schengen-Staaten und zur Anwendung des Durchführungsübereinkommens im Bereich des Personenverkehrs in diesem Hoheitsgebiet unter Verwendung von Informationen, die durch dieses System übermittelt werden. Man kann wahrscheinlich mit Recht behaupten, dass das Schengener Informationssystem der Vorgänger aller derzeitigen und künftigen großen EU-Informationssysteme war, mit denen ein Datenkontrollnetz in der EU geschaffen wurde. Das jüngste Beispiel, nämlich die durch den Prümer Vertrag eingeführten Systeme, spiegelt in starkem Maße die Konzeption und die Funktionen des Schengener Informationssystems wider, wobei hier grundsätzlich die EU-Bürger die Zielgruppe sind. In letzter Zeit sind viele Maßnahmen zur Erleichterung des Informationsaustauschs verabschiedet worden, allerdings ohne die notwendige Bewertung der bestehenden Systeme und der möglichen Auswirkungen auf den Schutz der Rechte des Einzelnen - nicht nur des Rechts auf Privatsphäre und auf Datenschutz, sondern auch des freien Personenverkehrs und des Grundsatzes der Nichtdiskriminierung.

Gemäß dem Schengener Durchführungsübereinkommen wurde die Gemeinsame Kontrollinstanz (GK) eingerichtet, ein unabhängiges Organ, welches mit der Kontrolle des zentralen Teils des Schengener Informationssystems sowie mit der Prüfung der beim Betrieb des Systems auftretenden Anwendungs- und Auslegungsschwierigkeiten betraut ist und gewährleistet, dass das System den einschlägigen Datenschutzbestimmungen entspricht.

Dieser Tätigkeitsbericht, der achte Bericht der GK, gibt einen Überblick über das Engagement und die Mitwirkung der GK an der Entwicklung des Schengener Informationssystems der zweiten Generation (SIS II), über die Funktion der GK während des Erweiterungsprozesses und ihre Initiativen für gemeinsame Tätigkeiten mit nationalen Datenschutzbehörden betreffend die vorschriftsmäßige Behandlung von personenbezogenen Daten, die im Rahmen von Ausschreibungen nach Artikel 99 des Schengener Durchführungsübereinkommens in das SIS eingegeben werden, einschließlich des Berichts über die Überprüfung der Umsetzung von Artikel 111 des Schengener Durchführungsübereinkommens.

Der vorliegende Bericht gibt auch Aufschluss über die Tätigkeiten der GK im Zusammenhang mit der Bearbeitung von Beschwerden von Personen, über die Stellungnahmen der GK zu verschiedenen Datenschutzfragen und die künftigen Perspektiven für eine gemeinsame Kontrolle des SIS.

2. NEUE ENTWICKLUNGEN: SIS II

Die Gemeinsame Kontrollinstanz, die eng an der Überwachung der Entwicklung des Schengener Informationssystems der zweiten Generation (SIS II) beteiligt gewesen ist, lieferte den EU-Institutionen Leitlinien und Hilfestellung und verfolgte dabei das Ziel, zu gewährleisten, dass das SIS II die erforderlichen Datenschutzstandards erfüllt. Im September 2006 gab die GK ihre Stellungnahme zur vorgeschlagenen Rechtsgrundlage für das SIS II ab.

Die Beiträge der GK zur Entwicklung des SIS II gehen zurück auf das Jahr 2004. In ihrer Stellungnahme vom 19. Mai 2004 zur künftigen Entwicklung des SIS II skizzierte die GK einige wichtige Anliegen und wies auf Maßnahmen hin, die ergriffen werden sollten. Im Oktober 2005 gab die GK eine Stellungnahme zur vorgeschlagenen Rechtsgrundlage für das SIS II auf der Grundlage eines Verordnungsentwurfs[1] und eines Beschlussentwurfs[2] ab, in der sie die neue Systemarchitektur in Bezug auf den bestehenden und den vorgeschlagenen neuen Datenschutzrahmen systematisch bewertete.Die GK machte zahlreiche ausführliche Anmerkungen und Vorschläge zur Verbesserung der Entwürfe. Seither wird im Rat und im Europäischen Parlament kontinuierlich über die neuen Vorschläge für die Rechtsgrundlage für das SIS II beraten, was zu vielen Abänderungen an den ursprünglichen Vorschlägen geführt hat. Die GK ging auf einige wichtige Themen im Zusammenhang mit den überarbeiteten Vorschlägen des finnischen Vorsitzes[3] vom 27. Juli 2006 über die Einrichtung, den Betrieb und die Nutzung des SIS II ein. Dadurch leistete sie aus datenschutzrechtlicher Sicht einen Beitrag zur Verbesserung der Rechtsgrundlage. In ihrer Stellungnahme begrüßte die GK, dass die Rolle des SIS II auf seine Ausgleichsfunktion begrenzt wurde, da dies als ein wichtiger Schritt zur Beschränkung des Zwecks des SIS II erschien, wie sie von der GK befürwortet wurde. Sie hob hervor, dass die beabsichtigten technischen Anforderungen, die für das SIS II entwickelt werden müssten, im Hinblick auf ihre Auswirkungen auf den Einzelnen in keinem Fall zu einer Reduzierung des Datenschutzniveaus führen dürfe.

Die GK äußerte den starken Wunsch, während des Übergangszeitraums, insbesondere angesichts der Einrichtung der Verwaltungsbehörde, einbezogen zu werden. Die GK äußerte einige Bedenken hinsichtlich der Nutzung biometrischer Daten im SIS II und begrüßte bestimmte Einschränkungen bei der Verwendung solcher Daten, wobei sie hervorhob, dass biometrische Daten lediglich als zusätzliches Werkzeug zur Überprüfung der Identität der betreffenden Person angesehen werden

1 KOM (2005) 236, 2005/0106 (COD).
2 KOM (2005) 230, 2005/0103 (CNS).
3 5709/9/06 und 5710/5/06.

könnten, wenn die zu entwickelnden technischen Qualitätsanforderungen angemessen seien und den erforderlichen Schutz böten.

Die uneingeschränkte Nutzung biometrischer Daten zu Identifizierungszwecken würde zweifellos dazu führen, dass immer mehr Behörden diese Funktionalität für verschiedene Zwecke nutzten. Eine derartige funktionale Ausweitung sollte auch unter Berücksichtigung der gewünschten Interoperabilität zwischen SIS II, VIS und Eurodac verhindert werden. Die GK empfahl in ihrer Stellungnahme, eine Bestimmung in die Vorschläge aufzunehmen, nach der die Nutzung biometrischer Daten zur Identifizierung einer Person unbedingt auf die Ausschreibungszwecke zu begrenzen sei. Die GK kam zu dem Schluss, dass biometrische Daten (Fingerabdrücke), die im SIS II verarbeitet werden, nur dazu verwendet werden sollten, die Identität der betreffenden Person zu überprüfen: beschränkt auf den Ausschreibungszweck und nicht auf andere Identifizierungsabfragen ausgeweitet. Technische Entwicklungen, die für den Abgleich "eins zu vielen" zu nutzen sind, sollten aufgrund der Besonderheit von Fingerabdrücken nicht nur höchsten Standards genügen, sondern auch die Möglichkeit eines Rechtsbehelfs für die betreffende Person umfassen. Die Inanspruchnahme eines solchen Abgleichs sollte ferner keine Option sein, die lediglich aus technischen Erwägungen gewählt wird, sondern angesichts seiner Auswirkungen auf die Rechte des Einzelnen auch eine Beurteilung der Notwendigkeit und Verhältnismäßigkeit erfordern.

Die GK bestand darauf, dass der Mechanismus gewährleisten müsse, dass die Daten präzise und rechtmäßig verarbeitet würden, damit die Rechte der Bürger gewahrt blieben. Die GK schlug auch vor, dass der Wortlaut der Vorschläge dahin gehend abgeändert werden sollte, dass strittige Fälle zwischen den Mitgliedstaaten der entsprechenden koordinierten Überwachung des SIS II unterstellt würden.

Bereits vor Beginn der Beratungen über das SIS II zeigte sich, dass der dringende Wunsch bestand, Europol und Eurojust Zugang zu einigen spezifischen Ausschreibungen zu gewähren, was zur Erfüllung ihrer Aufgaben nützlich sein könnte. Die GK hat in allen ihren Stellungnahmen davor gewarnt, dass ein solcher Zugang nicht zu einem routinemäßigen Zugang für diese Stellen führen sollte. Die Ausschreibungen, für die sie zugangsberechtigt seien, enthielten nicht notwendigerweise Informationen, die für die Ziele von Europol und Eurojust erheblich seien.

Es wurden die Verordnung (EG) Nr. 1987/2006, der Beschluss 2007/533/JI des Rates über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) und die Verordnung (EG) Nr. 1986/2006 über den Zugang von für die Ausstellung von Kfz-Zulassungsbescheinigungen zuständigen Dienststellen der Mitgliedstaaten zum Schengener Informationssystem der zweiten Generation (SIS II) angenommen, die die Rechtsgrundlagen für die SIS II-Tätigkeit bildeten; in diesen Rechtsakten wurden auch die Datenschutzbestimmungen sowie

eine Regelung für die Datenschutzüberwachung festgelegt.

2.1. Migration vom SIS I+ zum SIS II

Mit der zunehmenden Zahl von EU-Mitgliedstaaten nach der Erweiterung der Union wurde deutlich, dass das SIS so konzipiert werden muss, dass mehr als doppelt so viele Mitgliedstaaten einbezogen werden können, als dies beim derzeitigen SIS der Fall ist. Gleichzeitig beschäftigte sich die Gemeinsame Kontrollinstanz mit der Frage der Datenmigration von SIS I + zu SIS II und den Vorbereitungen hierfür. Zu diesem Zeitpunkt war es wichtig zu gewährleisten, dass während der Datenmigration von einem zum anderen System wichtige Datenschutzgrundsätze (Datenintegrität, Vertraulichkeit von Daten, Zweckbestimmung) eingehalten werden.
Die GK erhielt am 19. April 2006 ein Ersuchen des Vorsitzenden des Ausschusses "Artikel 36", die vorgeschlagenen Regeln für die Erstellung einer SIS I+-Testdatenbank zu überprüfen, um die Migration von SIS I+ zu SIS II vorzubereiten.
Obwohl die GK die Einrichtung einer SIS-II-Testdatenbank voll unterstützt hatte, merkte sie in ihrer Stellungnahme 06-05 an, dass die im Vorschlag aufgeführten Datenfelder versehentlich Daten echter Personen erstellen könnten und dass daher zusätzliche Sicherheitsmaßnahmen angewendet werden sollten. In ihrer Stellungnahme wies die GK auch darauf hin, dass die Nutzung personenbezogener Daten als Testdaten während der Entwicklung von Informationssystemen verschiedene Risiken mit sich bringe. Bei der Erstellung von Testdaten für ein Informationssystem wie das SIS II wurde allgemein akzeptiert, dass eine solche Erstellung dem Grundsatz der Datenmigration unter Wahrung der Privatsphäre folgen sollte: Entwicklung exakter Modelle ohne Zugriff auf präzise Informationen in Einzeldatensätzen, wodurch der Konflikt zwischen Privatsphäre und Datenmigration gelöst würde. Anonymisierungstechniken sollten die Verwendung von Datensätzen ohne Offenlegung der Identität ermöglichen. Die GK merkte an, dass die Datenmigration unter Wahrung der Privatsphäre auf dem Konzept basieren sollte, dass personenbezogene Daten geschützt werden könnten, wenn sie vor der Übermittlung verschlüsselt oder randomisiert werden . Durch Anwendung einer besonderen Technik könnten äußerst exakte Datenmodelle generiert werden, ohne dabei personenbezogene Daten offenzulegen. Die GK stellte fest, dass bei der Erläuterung des Vorschlags eingeräumt worden war, dass bei den zu erstellenden Testdaten echte Daten offen gelegt werden konnten. Da aufgrund des Vorschlags die Namenfelder (Vor- und Zuname) unverändert blieben und ein Austausch lediglich zwischen ähnlichen Datensätzen vorgenommen wurde, bestand ein hohes Risiko, dass Personen identifiziert werden konnten. Das Risiko sei erkannt und in den Vorschlag daher einige zusätzliche Verfahrensmaßnahmen zur begrenzten Nutzung der Testdatenbank eingeführt worden.

Diese Maßnahmen würden jedoch niemals die Weitergabe von Daten an Dritte verhindern. Die GK unterstützte die zusätzlichen Maßnahmen als eine allgemeine zusätzliche Schutzmaßnahme, hob allerdings hervor, dass sie nicht das Erfordernis ersetzen könnten, Testdaten komplett zu anonymisieren. Sie lieferte auch eine Reihe von Empfehlungen für die Entwicklung besonderer Sicherheitsmaßnahmen, die Vermeidung der Nutzung sensitiver Daten in einem Testumfeld, die Anonymisierungsmethodik, die Aufzeichnung des Zugriffs auf Testdaten, die Bereitstellung von Prüfpfaden sogar für die GK sowie Fristen für die Nutzung dieser Testdatenbank.

Im April 2008 legte die Kommission zwei Vorschläge für eine Verordnung des Rates und einen Beschluss des Rates über die Migration vom Schengener Informationssystem (SIS 1+) zum Schengener Informationssystem der zweiten Generation (SIS II) zur Festlegung des rechtlichen Rahmens für die Migration von SIS 1+ zu SIS II vor. Am 30. Juni 2008 organisierte der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments einen Runden Tisch zum Thema "Freiheit und Sicherheit im Rahmen des integrierten Schutzes an den EU-Grenzen" einschließlich einer Sitzung *"SIS II: Wann? Warum? Wie?"*. Der Vorsitzende der Gemeinsamen Kontrollinstanz Schengen nahm an der Veranstaltung teil und leistete einen Beitrag zu den Erörterungen über die datenschutzrechtlichen Auswirkungen der Migration von SIS I zu SIS II. Im Oktober 2008 nahm der Rat den Beschluss des Rates und die Verordnung des Rates über die Migration vom Schengener Informationssystem (SIS 1+) zum Schengener Informationssystem der zweiten Generation (SIS II) an.

2.2. Erweiterung des Schengen-Raums

Eines der wichtigen Ereignisse während des Zeitraums 2005-2008, das erwähnenswert ist, war die Erweiterung des Schengen-Raums, wodurch neun neue Mitgliedstaaten dem Schengen-Raum beitreten konnten und ihren Bürgern die Möglichkeit geboten wurde, uneingeschränkt die Freizügigkeit zu genießen, die Binnengrenzen zu überschreiten, ohne Pass oder Personalausweis vorzeigen zu müssen, außer für Reisen in das Vereinigte Königreich, nach Irland und Zypern sowie nach Bulgarien und Rumänien, die erst 2007 beigetreten sind. Der lange Prozess der Besuche und Folgebesuche zur Schengen-Bewertung dauerte zwei Jahre. Die Bewertung bestand insbesondere darin, zu überprüfen, ob die Begleitmaßnahmen, die die Aufhebung der Binnengrenzkontrollen ermöglichten, von den neuen Mitgliedstaaten korrekt und effizient umgesetzt wurden. Die Bewertungsbesuche betrafen folgende Bereiche: Außengrenzkontrollen, Visa, Datenschutz, polizeiliche Zusammenarbeit und Schengener Informationssystem.
Bei der Entwicklung des SIS II ging es um die Schaffung und Umsetzung neuer Systemfunktionen

(Stärkung der Sicherheit und effizientere Nutzung der Daten), aber auch darum, dass das System technisch in der Lage ist, mehr als 18 Länder zu bedienen. Die Fristen für den Start des neuen Systems und die Notwendigkeit für die neuen Mitgliedstaaten, dem System möglichst schnell beizutreten, zwangen die Mitgliedstaaten, eine rasche Alternativlösung zu finden. Im Dezember 2006 beschloss der Rat, den portugiesischen Vorschlag SISone4ALL umzusetzen, der darauf abzielte, neun der Mitgliedstaaten, die der Europäischen Union im Mai 2004 beigetreten waren, vorübergehend in das SIS 1+ zu integrieren. Durch das SISone4ALL-Projekt sollte der Prozess, der zur Aufhebung der Binnengrenzkontrollen mit den betreffenden Staaten zwischen Dezember 2007 und März 2008 führte, vereinfacht werden. Gemäß dem Beschluss 2007/471/EG des Rates vom 12. Juni 2007 konnten die Mitgliedstaaten ab dem 1. September 2007 Daten in das SIS eingeben und SIS-Daten nutzen.

Am 21. Dezember 2007 sind Estland, die Tschechische Republik, Litauen, Ungarn, Lettland, Malta, Polen, die Slowakei und Slowenien dem Schengen-Raum beigetreten. Am 30. März 2008 wurde der Erweiterungsprozess durch die Aufhebung der Kontrollen an den Luftgrenzen zwischen diesen Ländern und mit den 15 Staaten, die bereits dem Schengen-System angehörten, abgeschlossen. Auch schon vor der Erweiterung war das SIS eine der wichtigsten und größten Datenbanken für Einwanderungs- und Grenzkontrollen in der EU. Am 1. Januar 2007 betrug die Gesamtzahl der gültigen Datensätze im SIS 17 615 945.

Nachdem die neun neuen Mitgliedstaaten dem Schengen-Raum beitraten und den SIS-Betrieb am 1. Januar 2008 aufnahmen, ist diese Zahl auf 22 933 370 gültige Datensätze gestiegen. Insgesamt hat die Zahl der gültigen Datensätze in der Datenbank während dieses Zeitraums um 23 % zugenommen. Vergleicht man die Statistik vom 1. Januar 2008 mit der von 2007[1], so fand die größte Zunahme bei den Datensätzen mit personenbezogenen Daten in der Kategorie Identitätsdokumente (ausgestellte Dokumente) statt, in der ein Anstieg von 13 752 947 auf 17 876 227 (23%) zu verzeichnen war. Die Statistik sieht wie folgt aus (nach Artikeln des Schengener Übereinkommens aufgeschlüsselt):

Art. 95 (gesucht zum Zwecke der Festnahme/ Auslieferung)	+ 16%
Art. 96 (unerwünschte Drittausländer)	- 7,4%
Art. 97 (volljährige Vermisste)	+ 14%
Art. 97 (minderjährige Vermisste)	+ 6,8%
Art. 98 (Ermittlung des Wohnsitzes oder Aufenthalts)	+ 22%
Art. 99 Absatz 2 (Kontrolle/Observierung)	- 5%
Art. 99 Absatz 3 (Kontrolle/Observierung)	- 22%

[1] Dok. 5441/08 vom 30. Januar 2008; Dok. 6178/07 vom 13. Februar 2007.

Die verringerte Zahl von Ausschreibungen zu unerwünschten Drittausländern könnte durch die einfache Tatsache erklärt werden, dass aufgrund des Beitritts der neuen Mitgliedstaaten zur EU die Bürger dieser Staaten EU-Bürger geworden sind und daher die Datensätze zu diesen Personen aus dem System gelöscht worden sein dürften. Angesichts dieser Tatsache kam die Initiative der GK, das Audit zur Anwendung von Artikel 96 fortzuführen, zum rechten Zeitpunkt und die Ergebnisse waren zufrieden stellend. In den eingegangen Antworten wurde nicht über Fälle berichtet, in denen Daten von EU-Bürgern nach Artikel 96 verarbeitet wurden. Aufgrund der geringen Anzahl eingegangener Antworten liegt es allerdings auf der Hand, dass diese Arbeit in allen Schengen-Staaten durchgeführt werden muss.

Die Erweiterung brachte auch eine Zunahme der Mitgliederzahl der GK mit sich. Diese neuen Mitglieder nahmen bereits als Beobachter an der Tätigkeit der GK teil und eigneten sich dabei sehr viel Wissen zur Vorbereitung auf ihre neuen Aufgaben und Pflichten an. Durch die Gewährung dieses Beobachterstatus spielte die GK eine wichtige Rolle, indem sie das Bewusstsein der künftigen Mitglieder weckte und ihnen Wissen vermittelte, Stellungnahmen abgab und zu Fragen der Beobachter hinsichtlich unterschiedlicher Auslegungen der Bestimmungen des Schengener Übereinkommens Rat gab.

Gleichzeitig war die Erfahrung der neuen Mitglieder, die sie durch den langen Vorbereitungs- und Bewertungsprozess gewannen (Mitwirkung an den vorbereitenden Arbeiten für die nationalen SIS-Rechtsvorschriften, a priori-Audits der IT-Systeme, Beratungen mit den zuständigen Institutionen, Sensibilisierungskampagnen hinsichtlich der Rechte des Einzelnen im Rahmen des SIS, Kontrolltätigkeit in Konsulaten, bei Polizeibehörden usw.), sehr wichtig für die sogenannten "alten Mitglieder" der GK.

Alle diese Aspekte sind sehr wertvoll für die gemeinsame Koordinierungsarbeit zur Förderung des tatsächlichen Schutzes der Rechte und Freiheiten des Einzelnen und der künftigen Kontrolle des SIS II.

3. KONTROLLTÄTIGKEIT

Nach Artikel 115 Absatz 3 des Schengener Durchführungsübereinkommens (SDÜ) ist die Gemeinsame Kontrollinstanz (GK) zuständig für die Prüfung der Anwendungs- oder Auslegungsfragen im Zusammenhang mit dem Funktionieren des Schengener Informationssystems, für die Prüfung von Fragen im Zusammenhang mit den von den nationalen Kontrollinstanzen unabhängig vorgenommenen Kontrollen oder mit der Ausübung des Auskunftsrechts sowie für die Erarbeitung harmonisierter Vorschläge im Hinblick auf gemeinsame Lösungen für die bestehenden Fragen. Zur praktischen Umsetzung dieser Bestimmung des SDÜ beschloss die GK, Kontrollen auf nationaler Ebene durchzuführen. Ihr offensichtlicher praktischer Nutzen bestand darin, Einblick und Wissen darüber zu gewinnen, wie die Schengen-Staaten die Artikel des SDÜ umsetzen und anwenden, und einen Überblick über die praktischen Probleme zu erhalten, die bei der Umsetzung entstehen können.

3.1. Überprüfung der Anwendung von Artikel 99

Eines der Hauptmerkmale des Schengener Informationssystems ist die gemeinsame Verantwortung für die Nutzung des Systems nach Maßgabe des Schengener Durchführungsübereinkommens und der nationalen Rechtsvorschriften. Man kann mit Recht sagen, dass die Gemeinsame Kontrollinstanz Schengen die erste Kontrollbehörde war, die gemeinsame koordinierte Kontrolltätigkeiten im Strafverfolgungsbereich im Hinblick auf die Kontrolle großer Datenbanken gefördert hat. Dieses neue Konzept der Kontrollfunktion war in der Tat erfolgreich und gab den Anstoß zu einer künftigen koordinierten Überprüfung. Dieses Überprüfungssystem trug erheblich zur Harmonisierung der Anwendung des SDÜ und der Nutzung des SIS bei.

Im Juni 2006 ersuchte die GK die nationalen Datenschutzbehörden, ein Audit der von den zuständigen Behörden ihres Landes in das Schengener Informationssystem (SIS) eingegebenen Artikel 99-Ausschreibungen vorzunehmen.

Es handelte sich um das zweite Audit, das von der GK betreffend die Anwendung eines spezifischen Artikels des SDÜ initiiert wurde (*2005 war ein Audit zu Artikel 96 SDÜ durchgeführt worden*). Oftmals ergaben sich diverse Unterschiede zwischen den Schengen-Staaten, auf deren Grundlage die GK Schlüsse ziehen und die erforderlichen Maßnahmen empfehlen konnte.

Das Audit sollte Gewissheit darüber geben, dass die Artikel-99-Daten im Einklang mit Artikel 99 sowie den Datenschutzgrundsätzen des SDÜ, des SIRENE-Handbuchs und der anzuwendenden nationalen Rechtsvorschriften verarbeitet wurden. Die für das Audit gewählte Methode ermöglichte der GK eine Beurteilung der Frage, ob Auslegungsschwierigkeiten in Bezug auf die Anwendung des Artikels 99 SDÜ bestünden.

Zu diesem Zweck hatte die GK eine von allen nationalen Datenschutzbehörden einheitlich anzuwendende einfache Audit-Methode ausgearbeitet. Ein umfassender Fragenkatalog wurde umgearbeitet. Anhand dieses Fragenkatalogs sollte ein Überblick über die einschlägigen nationalen Rechtsvorschriften der Schengen-Staaten erzielt und überprüft werden, ob alle erforderlichen Verfahren angewendet wurden, damit die für die Ausschreibungen verantwortlichen Behörden die datenschutzrechtlichen Anforderungen erfüllen. Der Fragenkatalog enthielt zudem spezifische Fragen, die klären sollten, ob die Ausschreibungen den Bestimmungen des Artikels 99 entsprachen und ob ihre Beibehaltung im SIS mit den Bestimmungen des SDÜ vereinbar war.

Die gemeinsamen Bemühungen der nationalen Datenschutzbehörden zur Überprüfung der nationalen SIS-Ausschreibungen nach Artikel 99 SDÜ in einem bestimmten Zeitraum und unter Einsatz desselben Auditmodells bestätigte einmal mehr das gemeinsame Interesse an einer ordnungsgemäßen Nutzung des SIS. Dieses zweite gemeinsame Audit war erneut ein Meilenstein in der Zusammenarbeit zwischen nationalen Datenschutzbehörden in der Europäischen Union und unterstrich die Notwendigkeit, einen Rahmen für Datenschutzinspektionen in den Bereichen zu schaffen, in denen die Zusammenarbeit zwischen Schengen-Staaten eine Verarbeitung personenbezogener Daten beinhaltet. Zugleich hat dieses Audit den nationalen Datenschutzbehörden dabei geholfen, in Erfahrung zu bringen, auf welche Weise ihr Land die Artikel-99-Ausschreibungen anwendet, was für die künftige Tätigkeit dieser Behörden sicherlich von Vorteil ist.

In Anbetracht der beim Audit zur Anwendung von Artikel 99 gewonnenen Erkenntnisse verabschiedete die GK eine Reihe von Empfehlungen. Die wesentlichen Empfehlungen lauteten wie folgt:

- Die für Artikel-99-Ausschreibungen zuständigen Behörden sollten durch Ausarbeitung förmlicher, schriftlicher und strukturierter Verfahren die Richtigkeit, Aktualität und Rechtmäßigkeit der Artikel-99-Datenbestände gewährleisten.

- Es wurde eine klare Definition der Formen von Kriminalität benötigt, die eine Artikel-99-Ausschreibung begründen könnten. Obgleich in der neuen Rechtsgrundlage für das SIS II der allgemeine Begriff "schwere Straftat" verwendet wurde, wurde empfohlen, sich auf europäischer Ebene auf eine einheitliche Auslegung des Begriffs "schwere Kriminalität" zu verständigen. Hierzu könnte das Verzeichnis der Formen schwerer Kriminalität, für die Europol zuständig ist, oder der Rahmenbeschluss des Rates über den Europäischen Haftbefehl herangezogen werden.
- Die für Artikel-99-Ausschreibungen zuständigen nationalen Behörden sollten diese Ausschreibungen alle sechs Monate einer Überprüfung unterziehen. Es sollten zusätzliche Leitlinien festgelegt werden.
- Die Liste der Behörden (einschließlich der nationalen Sicherheitsdienste) mit Zugang zu Artikel-99-Ausschreibungen sollte in allen EU-Mitgliedstaaten harmonisiert werden.
- In Fällen, in denen verschiedene Behörden für die Qualität und Integrität der Daten zuständig waren, sollte gewährleistet werden, dass sich Organisation und Verzahnung der verschiedenen Zuständigkeiten so gestalteten, dass die Richtigkeit, Aktualität und Rechtmäßigkeit der Datenbestände kontinuierlich sichergestellt und eine Überprüfung der Daten gewährleistet waren.
- Eine Ausschreibung von Personen, die mit der betroffenen Person in Verbindung stehen, war nach dem Wortlaut des Artikels 99 Absatz 2 nicht zulässig.
- Die nationalen Datenschutzbehörden sollten die Artikel-99-Ausschreibungen regelmäßig überprüfen.

3.2. Überprüfung der Anwendung von Artikel 111

Im Oktober 2006 ersuchte die Gemeinsame Kontrollinstanz Schengen die nationalen Datenschutzbehörden um Informationen zur Umsetzung und Anwendung von Artikel 111 des Schengener Durchführungsübereinkommens (SDÜ). Dies war die dritte Überprüfung, die hinsichtlich der Anwendung spezifischer Artikel des SDÜ durchgeführt wurde (*2005 wurde z.B. Artikel 96 und momentan wird Artikel 99 überprüft*). Als notwendig erwiesen hat sich diese Überprüfung im Rahmen der Untersuchung eines spezifischen Falls im Zusammenhang mit den praktischen Auswirkungen von Artikel 111, mit dem die GK befasst worden ist.

Das SDÜ enthält Bestimmungen sowohl über die Verarbeitung personenbezogener Daten als auch über die Rechte der Personen, deren personenbezogene Daten im SIS verarbeitet werden. Nach Artikel 109 SDÜ sollte sich das Recht, über in dem System gespeicherte Daten Auskunft zu erhalten, nach dem nationalen Recht der Vertragspartei des SDÜ richten, in deren Hoheitsgebiet eine Person das Auskunftsrecht beansprucht. Es sei darauf hingewiesen, dass nach dieser Bestimmung im nationalen Recht festgelegt werden kann, dass die in Artikel 114 Absatz 1 SDÜ vorgesehene nationale Kontrollinstanz entscheiden kann, ob und in welcher Weise der betroffenen Person Auskunft erteilt wird. Artikel 109 regelt auch Fälle, in denen eine natürliche Person das Auskunftsrecht in einem Schengen-Vertragsstaat beanspruchen will, der die Ausschreibung nicht selber veranlasst hat. In diesem Fall darf der Schengen-Staat, der die Ausschreibung nicht veranlasst hat, Auskunft zu diesen Daten nur erteilen, wenn er vorher dem ausschreibenden Schengen-Staat Gelegenheit zur Stellungnahme gegeben hat. Artikel 114 Absatz 2 räumt dem Einzelnen das Recht ein, die Kontrollinstanzen nach Artikel 114 Absatz 1 SDÜ zu ersuchen, die im SIS zu seiner Person gespeicherten Daten sowie deren Nutzung zu überprüfen. Dieses Recht richtet sich, wie bereits erwähnt, nach dem nationalen Recht des Schengen-Staates, in dem der Antrag gestellt wird. Wurden die Daten durch einen anderen Schengen-Staat eingegeben, so sollte die Kontrolle in enger Abstimmung mit der Kontrollinstanz dieses Staates erfolgen.

Nach Artikel 109 Absatz 2 SDÜ ist das Auskunftsrecht kein absolutes Recht und demzufolge sollte einer Person, die um Auskunft über zu ihrer Person im SIS gespeicherte Daten ersucht, die Auskunftserteilung verweigert werden, wenn dies zur Durchführung einer rechtmäßigen Aufgabe im Zusammenhang mit der Ausschreibung oder zum Schutz der Rechte und Freiheiten Dritter unerlässlich ist. Darüber hinaus ist es nach Artikel 109 Absatz 2 verboten, Auskunft über zum Zwecke der verdeckten Registrierung nach Artikel 99 SDÜ gespeicherte Daten zu erteilen.

Artikel 106 Absatz 1 führt das "Besitzerprinzip" für das SIS ein. Zwar werden in allen Schengen-Staaten personenbezogene Daten im Zusammenhang mit Ausschreibungen verarbeitet, doch dies bedeutet nicht, dass von einem Staat eingegebene Daten von einem anderen Schengen-Staat geändert werden dürfen. Es findet zwar das nationale Recht des verarbeitenden Staates Anwendung, doch ist nach der einschlägigen Bestimmung im SDÜ lediglich eine Änderung oder Löschung der Daten durch den ausschreibenden Staat zulässig.

Artikel 111 gibt weitere Garantien für die Rechte des Einzelnen. Nach Artikel 111 Absatz 1 hat jeder das Recht, im Hoheitsgebiet jeder Vertragspartei des SDÜ eine Klage wegen einer seine Person betreffenden Ausschreibung insbesondere auf Berichtigung, Löschung, Auskunftserteilung oder Schadensersatz vor dem nach nationalem Recht zuständigen Gericht oder der zuständigen

Behörde zu erheben. Nach Absatz 2 dieses Artikels sollten sich die Vertragsparteien des SDÜ verpflichten, unanfechtbare Entscheidungen der Gerichte oder Behörden nach Absatz 1 dieses Artikels zu vollziehen.

Entsprechend dem "Besitzerprinzip" und der Verpflichtung nach Artikel 111 Absatz 2, unanfechtbare Entscheidungen zu vollziehen, werden diese Entscheidungen vom ausschreibenden Schengen-Staat vollstreckt.

Wird jemand beim Betrieb des nationalen Bestandes des SIS geschädigt, so haften darüber hinaus die Vertragsparteien des SDÜ nach nationalem Recht. Diese Bestimmung des Artikels 116 SDÜ gilt auch für Schäden, die die ausschreibende Vertragspartei durch unrichtig oder unrechtmäßig gespeicherte Daten verursacht.

Mit dieser Überprüfung sollte kontrolliert werden, ob alle Schengen-Staaten Artikel 111 konsequent anwenden, dabei die Rechte der betreffenden Einzelpersonen wahren und ihnen eine faire und gleiche Behandlung zuteil werden lassen.

Dieser Überblick über die Gerichte und zuständigen Behörden zeigte, dass im Schengen-Raum ganz unterschiedliche Behörden für Entscheidungen im Zusammenhang mit Artikel 111 zuständig sind. Nur in einem Mitgliedstaat lag die Zuständigkeit für den Erlass unanfechtbarer Entscheidungen bei der Datenschutzbehörde (Österreich). In anderen Schengen-Staaten gab es eine geteilte Zuständigkeit zwischen Datenschutzbehörden und Gerichten, oder die diesbezügliche Zuständigkeit lag bei einem bestimmten Gericht.
In Bezug auf Ausschreibungen anderer Schengen-Staaten ging aus den meisten Antworten hervor, dass es ein formelles Verfahren für die Konsultation des ausschreibenden Staates bzw. für dessen offiziellen Streitbeitritt gab. Dies war jedoch nicht in allen Schengen-Staaten der Fall oder zumindest war das Verfahren nicht obligatorisch.

Was die Beteiligung der nationalen Datenschutzbehörden an einem Gerichtsverfahren anbelangt, so zeigten die Ergebnisse, dass nicht alle nationalen Datenschutzbehörden formell beteiligt oder unterrichtet wurden.

Es wurden 17 Fälle gemeldet, in denen Artikel 111 zur Anwendung gelangt ist.
Was die Vollstreckung von Entscheidungen anbelangt, so wurden – mit Ausnahme Portugals – keine spezifischen Verfahren zur Kontrolle der Vollstreckung angegeben. Generell muss sich die betroffene Person vergewissern, dass die Entscheidung vollstreckt wurde.

Die gemeinsamen Anstrengungen, die die nationalen Datenschutzbehörden unternommen haben, um die im Rahmen von Artikel 111 SDÜ geübte nationale Praxis über einen gewissen Zeitraum anhand eines einheitlichen Modells zu überprüfen, machten nochmals deutlich, dass die ordnungsgemäße Nutzung des SIS allen ein gemeinsames Anliegen ist. Diese dritte gemeinsame Aktion unterstrich die Notwendigkeit einer engen Zusammenarbeit zwischen den nationalen Datenschutzbehörden im Schengen-Raum und die Notwendigkeit weiterer Investitionen in die Zusammenarbeit zwischen den Schengen-Staaten, wenn dies für den Schutz der Rechte des Einzelnen unerlässlich ist.

Mit Artikel 111 SDÜ wird der Schutz des Rechts der betroffenen Person auf Berichtigung, Löschung oder Auskunft über sie betreffende Informationen im SIS einen wichtigen Schritt vorangebracht, da die Möglichkeit vorgesehen wird, eine Klage vor einem Gericht oder der zuständigen nationalen Behörde jedes Schengen-Staates zu erheben. Die Überprüfung zeigte, dass diese Bestimmung aufgrund einzelstaatlicher Rechtsvorschriften unterschiedlich umgesetzt wird.

Ein Eckpfeiler für den Schutz der Rechte der betroffenen Person ist die Vollstreckung der unanfechtbaren Entscheidung durch den ausschreibenden Schengen-Staat. Überaus wichtig ist hier das System zur Vollstreckung unanfechtbarer Entscheidungen und dessen Anwendung in der Praxis. Zwar liegen nur sehr wenige Statistiken vor, doch die Analyse der vorgelegten Fälle und insbesondere der Fälle, mit denen die GK befasst wurde, lassen begründete Zweifel daran aufkommen, ob Artikel 111 Absatz 2 SDÜ in der Praxis funktioniert.

Keiner der teilnehmenden Schengen-Staaten berichtete von einem Verfahren zur Kontrolle der Vollstreckung von unanfechtbaren Entscheidungen. Die zuständigen Behörden waren meist nicht an der Vollstreckung unanfechtbarer Entscheidungen beteiligt. Dies kann auf die unterschiedlichen rechtlichen Rahmenbedingungen der einzelnen Schengen-Staaten zurückzuführen sein. Die betroffene Person ist jedoch damit überfordert, in der Praxis auf eigene Initiative kontrollieren zu müssen, ob eine unanfechtbare Entscheidung vom ausschreibenden Schengen-Staat vollstreckt wurde.

In Anbetracht der Ergebnisse des Audits zu Artikel-111-Ausschreibungen gab die GK folgende Empfehlungen ab:

- Die Schengen-Staaten sollten ihre innerstaatlichen Verfahren überprüfen, um sich zu vergewissern, ob die von Artikel 111 gebotenen Garantien gewährleistet waren.

- Unanfechtbare Entscheidungen nach Artikel 111 müssen von allen Schengen-Staaten gleichermaßen vollstreckt werden.
- Nach Artikel 111 ergangene unanfechtbare Gerichtsentscheidungen müssen den nationalen Datenschutzbehörden übermittelt werden. Zur Durchsetzung dieses Erfordernisses kann es innerstaatlicher Vorschriften bedürfen.
- In allen Schengen-Staaten war ein innerstaatliches Verfahren zur Kontrolle der Vollstreckung von nach Artikel 111 ergangenen unanfechtbaren Entscheidungen erforderlich. Zu diesem Zweck mussten die jeweiligen Datenschutzbehörden miteinander in Kontakt stehen. Es kann nicht Aufgabe des Einzelnen sein, die Vollstreckung einer ihn betreffenden Entscheidung in einem anderen Schengen-Staat zu kontrollieren.
- Die nationalen Datenschutzbehörden sollten in dieser Hinsicht zusammenarbeiten. Die für die Zusammenarbeit zwischen den nationalen Kontrollbehörden geltenden Grundsätze müssen aktualisiert werden.

3.3. Nachkontrolle des Audits zur Anwendung von Artikel 96

Einer der wichtigsten Aspekte der Kontrolltätigkeit ist die regelmäßige Nachkontrolle, um zu gewährleisten, dass die ausgesprochenen Empfehlungen von der kontrollierten Stelle auch praktisch umgesetzt werden und so eine bessere Einhaltung der Bestimmungen erreicht wird.

Auf Initiative der GK kontrollierten die nationalen Datenschutzbehörden aller Schengen-Staaten die Nutzung der Ausschreibungen nach Artikel 96 im Schengener Informationssystem während des Zeitraums 2004-2005.

In Anbetracht der Tatsache, dass eine Ausschreibung zur Einreiseverweigerung für eine Person schwerwiegende Folgen haben kann, sowie der bei den Kontrollen festgestellten Probleme verständigte sich die GK auf eine Nachkontrolle zu der Frage, wie die Ergebnisse des Berichts auf nationaler Ebene umgesetzt und welche Verbesserungen erzielt wurden.

Die Nachkontrolle ergab, dass als Reaktion auf die Ergebnisse des Berichts die folgenden Schritte auf nationaler Ebene unternommen worden waren: In einigen Mitgliedstaaten wurden keine Probleme festgestellt, während in anderen Ländern sehr erfolgreiche Folgemaßnahmen ergriffen wurden. Bezüglich der Vorgehensweise bei der Bearbeitung von Fällen und der diesbezüglichen Kontrollverfahren, über die im Zusammenhang mit Artikel 96 SDÜ berichtet werden musste, waren interne Leitlinien erstellt worden, und besonderes Augenmerk war auf die Umsetzung einer der Empfehlungen des Berichts zu Artikel 96 gelenkt worden - *Maßnahmen sollten umgesetzt oder*

weiter entwickelt werden, um Ausschreibungen nach Artikel 96 zu Staatsangehörigen aus EU-Mitgliedstaaten zu verhindern. Im Anschluss an die Nachkontrollen wurden keine Ausschreibungen zu Staatsangehörigen der EU-Mitgliedstaaten mehr gefunden. Ein sehr positives Ergebnis dieser Nachkontrollen war die aktive Sensibilisierungskampagne, die eine Reihe von Mitgliedstaaten durchgeführt hatten, um Personen über ihre Rechte zu informieren, so wie sie im SDÜ festgelegt sind.
Dies war ein erneuter Beweis dafür, wie wichtig die Arbeit ist, die die GK zusammen mit den nationalen Datenschutzbehörden leistet, und zeige auch, wie sehr sich letztere ihren Werten, nämlich die Rechte und Freiheiten der Personen zu schützen, verpflichtet fühlen.

Die künftigen Bestimmungen über Ausschreibungen betreffend unerwünschte Drittstaatsangehörige, die im Rechtsrahmen für das SIS II festgelegt wurden, werden vor Eingabe einer Ausschreibung eine individuellere Bewertung und mehr Verantwortung voraussetzen.

In Artikel 24 Absatz 1 der 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] sind die Kriterien für die Eingabe einer Ausschreibung in das SIS II vorgesehen: Die Daten zu Drittstaatsangehörigen, die zur Einreise- oder Aufenthaltsverweigerung ausgeschrieben sind, werden aufgrund einer nationalen Ausschreibung eingegeben, die auf einer Entscheidung der zuständigen Verwaltungsbehörden oder Gerichte beruht, wobei die Verfahrensregeln des nationalen Rechts zu beachten sind; diese Entscheidung ergeht auf der Grundlage einer *umfassenden individuellen Bewertung* ergehen. Dies bedeutet, dass die Entscheidung, die Ausschreibung einzugeben, nicht automatisch in das System eingegeben werden kann. In seinem Urteil vom 31. Januar 2006 (*Kommission der Europäischen Gemeinschaften gegen Königreich Spanien*) betonte der Europäische Gerichtshof, dass für jeden individuellen Fall eine Einzelfallbewertung erforderlich sei, und vertrat die Auffassung, *dass ein Vertragsstaat die Ausschreibung eines Drittstaatsangehörigen, der mit einem Staatsangehörigen eines Mitgliedstaats verheiratet ist, erst dann vornehmen kann, wenn er festgestellt hat, dass die Anwesenheit dieser Person (…) eine tatsächliche, gegenwärtige und hinreichend schwere Gefährdung darstellt, die ein Grundinteresse der Gesellschaft berührt* [2]. Der Gerichtshof war der Auffassung, dass die Verweigerung des Sichtvermerks nicht auf dem bloßen Bestehen einer Ausschreibung im SIS oder einer vorherigen strafrechtlichen Verurteilung bestehen darf. Der Gerichtshof befand, dass *eine strafrechtliche Verurteilung daher nur insoweit berücksichtigt werden darf, als die ihr zugrunde liegenden Umstände ein persönliches Verhalten erkennen lassen, das eine gegenwärtige Gefähr-*

[1] ABl. L 381 vom 28.12.2006, S. 4.
[2] ABl. C 86 vom 8.4.2006, S. 3.

dung der öffentlichen Ordnung darstellt[1]. Aufgrund dieser Entscheidung des Gerichtshofs und der Bestimmungen über den Rechtsrahmen für das SIS II erhalten die nationalen Behörden mehr Verantwortung, wenn es darum geht, Entscheidungen zu treffen, die negative Folgen für den Einzelnen implizieren können, damit von Anfang an auf nationaler Ebene internationale Datenschutzgrundsätze eingehalten werden.

Ein weitere wichtige Änderung findet sich in Artikel 42 der Verordnung, nämlich das Recht der Drittstaatsangehörigen, die Gegenstand einer Ausschreibung nach der Verordnung sind, gemäß den Artikeln 10 und 11 der Richtlinie 95/46/EG informiert zu werden. Hierbei handelt es sich um eine wichtige Verbesserung im Vergleich zur bisherigen Situation, so wie sie durch das Schengener Durchführungsübereinkommen festgelegt wurde.

Gleichzeitig geben neue EU-Initiativen, bei denen es um die Verarbeitung personenbezogener Daten von Drittstaatsangehörigen geht, Anlass zu gewissen Bedenken hinsichtlich ihrer Auswirkungen auf das Recht der betroffenen Personen auf Privatsphäre. Nach Auffassung der Europäischen Kommission sollte die gemeinsame Politik der Union zur Unterstützung der Bemühungen der Mitgliedstaaten stetig ausgeweitet und verstärkt werden, um neuen Bedrohungen, Verlagerungen des Migrationsdrucks und etwaigen Defiziten zu begegnen, wobei die neuen Technologien umfassend und verhältnismäßig zu nutzen sind[2]. Nach Ansicht der Kommission könnte die Union die Einführung eines effizienten Instruments in Betracht ziehen, um Personen, die die genehmigte Aufenthaltsdauer überschreiten, zu ermitteln, da derzeit keine Daten über grenzüberschreitende Bewegungen von Drittstaatsangehörigen erfasst werden. Daten zu Drittstaatsangehörigen (Einreiseverweigerungen) werden derzeit im Rahmen von Ausschreibungen nach Artikel 96 verarbeitet, obwohl keine Daten hinsichtlich der Dauer des überschrittenen Zeitraums verarbeitet werden. Da dies nicht ausreichend sein dürfte, werden mögliche Instrumente empfohlen, die bei Drittstaatsangehörigen Anwendung finden würden, die in einen an der Schengen-Zusammenarbeit beteiligten Mitgliedstaat oder einen mit dieser Zusammenarbeit assoziierten Staat einreisen; derartige Instrumente könnten Folgendes umfassen:

- Erleichterung des Grenzübertritts für Bona-fide-Reisende;
- eventuelle Erfassung der Ein- und Ausreise und
- Prüfung der Einführung eines Systems zur elektronischen Erteilung von Reisebewilligungen (Electronic System of Travel Authorisation – ESTA).

[1] ABl. C 86 vom 8.4.2006, S. 3.
[2] KOM(2008) 69 endg. vom 13.2.2008.

Auch wenn der Prozess erst am Anfang steht, wurde in den Schlussfolgerungen des Rates über die Entwicklung des Visa-Informationssystems (VIS)[1] bereits die von der Kommission vorgelegte Durchführbarkeitsstudie begrüßt, in der die in den Leitlinien enthaltenen Ziele für das Visa-Informationssystem bestätigt und die Kommission ersucht wird, ihre vorbereitenden Arbeiten für die Entwicklung des VIS in Zusammenarbeit mit den Mitgliedstaaten auf der Grundlage einer zentralisierten Systemarchitektur fortzusetzen und dabei die Option einer mit dem SIS II gemeinsamen technischen Plattform zu berücksichtigen, wobei die Daten im selben System gespeichert werden und dieselben Endnutzer auf sie Zugriff haben. Für den Fall, dass wenn beide Systeme auf einer gemeinsamen technischen Plattform eingerichtet werden, könnte dies bedeuten, dass technische Maßnahmen/Möglichkeiten für eine Interoperabilität zwischen dem SIS II und dem VIS gegeben wären.

Obgleich noch nicht erwiesen ist, ob dieses neue System einen Mehrwert für die EU-Außengrenzen im Vergleich zu den bestehenden EU-Systemen (SIS) bietet, liegt es auf der Hand, dass dieses größere, komplexe und vernetzte Datenverarbeitungsmodell ernste Auswirkungen auf die Privatsphäre jedes Einzelnen haben und erhebliche Anstrengungen von Seiten der nationalen und europäischen Datenschutzbehörden erfordern wird, um einen angemessenen und wirksamen Schutz der Rechte des Einzelnen zu gewährleisten. Der Preis für diese Initiativen könnte wie folgt beschrieben werden: "Die Modernisierung der Einwanderungspolitik auf Kosten ihrer Dehumanisierung ist die Folge einer Asymmetrie in der politischen Entwicklung, bei der die Kontrolle von Migranten ohne eine entsprechende Weiterentwicklung ihrer Rechte ausgeweitet wird."[2]

[1] Dok. 6535/04 vom 20. Februar 2004.

[2] Alice Garside (2006): The political genesis and legal impact of proposals for the SIS II: what cost for data protection and security in the EU? Sussex Migration Working Paper no. 30.

4. STELLUNGNAHMEN DER GEMEINSAMEN KONTROLLINSTANZ

4.1. Auslegung des Artikels 111 des Schengener Durchführungsübereinkommens (SDÜ)

Im Juni 2006 wurde die Gemeinsame Kontrollinstanz von der österreichischen Datenschutzkommission darum ersucht, nach Artikel 115 Absatz 3 SDÜ zu prüfen, ob Schwierigkeiten im Zusammenhang mit der Anwendung von Artikel 111 SDÜ aufgetreten sind, und Vorschläge im Hinblick auf die Lösung jeglichen festgestellten Problems zu unterbreiten. In Anbetracht der Umstände, die zu dem Ersuchen Veranlassung gegeben hatten, hat die GK auch geprüft, welche Auswirkungen der Zusammenfall von Verfahren für die Anwendung von Artikel 111 hat.

Seit Einrichtung des Schengener Informationssystems unterrichten sich die Vertragsparteien des SDÜ gegenseitig über ihre Ausschreibungen zu einzelnen Personen. Im SDÜ sind die Gründe und Voraussetzungen für diese Ausschreibungen sowie die zu treffenden Maßnahmen festgelegt. Eines der wichtigsten Ergebnisse, die mit diesem Übereinkommen erzielt wurden, besteht wohl darin, dass die an das SIS angebundenen Staaten verpflichtet sind, auf die Ausschreibung eines anderen Staates hin (unmittelbar) tätig zu werden.

In Artikel 104 Absatz 2 ist präzise festgelegt, in welchem Verhältnis das einzelstaatliche Recht der Mitgliedstaaten und das SDÜ zueinander stehen: *"Soweit dieses Übereinkommen keine besondere Regelung enthält, findet das nationale Recht der jeweiligen Vertragspartei auf die in ihrem nationalen Teil des SIS gespeicherten Daten Anwendung."*
In Fällen, in denen das einzelstaatliche Recht anderweitige Bestimmungen enthält, sind also die einschlägigen Bestimmungen des Übereinkommens maßgebend.

Ein Beispiel hierfür ist das so genannte "Besitzerprinzip" in Artikel 106 Absatz 1: *"Die Änderung, Ergänzung, Berichtigung oder Löschung der Daten darf nur durch die ausschreibende Vertragspartei vorgenommen werden."*
Obwohl in allen Schengen-Staaten personenbezogene Daten im Zusammenhang mit Ausschreibungen verarbeitet werden, bedeutet dies nicht, dass von einem Staat eingegebene Daten von anderen Schengen-Staaten geändert werden dürfen. Es findet zwar das nationale Recht des verarbeitenden Staates Anwendung, doch ist nach der einschlägigen Bestimmung im SDÜ lediglich eine Änderung oder Löschung der Daten durch den ausschreibenden Staat zulässig.

Mit der Einrichtung des SIS wurde auch die Rechtsstellung der betroffenen Personen harmonisiert. Es wurden Rechte für die betroffenen Personen verbrieft, einschließlich Bestimmungen, um zu verhindern, dass sich die betroffenen Personen bei der Ausübung ihrer Rechte verfahrensrechtlichen "Hindernissen" gegenübersehen. Der alleinige Umstand, dass sich eine betroffene Person nicht in das Schengen-Gebiet begeben kann, sollte sie nicht daran hindern, ein Verfahren anzustrengen. Das Übereinkommen erkennt die Rechtsstellung der betroffenen Personen an, verpflichtet sie jedoch nicht dazu, in dem ausschreibenden Staat ein (Gerichts-)Verfahren betreffend eine Ausschreibung anzustrengen. Es bleibt der betroffenen Person überlassen, im Schengen-Staat ihrer Wahl ein entsprechendes Verfahren einzuleiten. Die Schengen-Staaten haben damit klar zum Ausdruck gebracht, dass sie auf eine harmonisierte Anwendung der geltenden Datenschutzbestimmungen vertrauen.

Die Rechte der betroffenen Person sind in Artikel 109 Absatz 1 – Auskunftsrecht – und in Artikel 110 – Recht, unrichtige Daten berichtigen oder unrechtmäßig gespeicherte Daten löschen zu lassen – verankert.
Diese Rechte richten sich nach dem Recht des Schengen-Staates, in dem sie geltend gemacht werden (Artikel 109 Absatz 1). Wurden die Daten von einem anderen Schengen-Staat in das SIS eingestellt, so wird diesem Gelegenheit zur Stellungnahme gegeben, bevor eine Entscheidung ergeht.

Die betroffene Person hat außerdem das Recht, den nationalen Datenschutzbeauftragten eines Schengen-Staates um Überprüfung der zu seiner Person gespeicherten Daten zu ersuchen (Artikel 114 Absatz 2). Wurden die Daten von einem anderen Schengen-Staat in das SIS eingestellt, so koordiniert der nationale Datenschutzbeauftragte die Kontrolle im Benehmen mit dem nationalen Datenschutzbeauftragten des Schengen-Staates, der die Ausschreibung veranlasst hat.

Der betroffenen Person wird auch das Recht zugestanden, eine Klage wegen einer sie betreffenden Ausschreibung auf Berichtigung, Löschung, Auskunftserteilung oder Schadensersatz vor dem nach nationalem Recht zuständigen Gericht oder der zuständigen Behörde zu erheben (Artikel 111 Absatz 1).
Nach Artikel 111 Absatz 2 sind die Schengen-Staaten verpflichtet, unanfechtbare Entscheidungen der Gerichte oder Behörden nach Absatz 1 dieses Artikels zu vollziehen.

Da das Übereinkommen ein System vorsieht, um die Rechte der betroffenen Personen zu schützen, und insbesondere aufgrund des "Besitzerprinzips", muss es einen Mechanismus geben, der sicher-

stellt, dass unanfechtbare Entscheidungen von Gerichten oder Behörden nach Artikel 111 Absatz 1 auch von anderen Schengen-Staaten vollzogen werden. Andernfalls wären die grundlegenden Datenschutzrechte, die das SDÜ der betroffenen Person einräumt, nicht in ausreichendem Maße gewährleistet.

Eine der Voraussetzungen für das Inkrafttreten des Übereinkommens ist, dass der teilnehmende Staat in seinem nationalen Recht die erforderlichen Maßnahmen zur Gewährleistung eines Datenschutzstandards trifft, der zumindest dem entspricht, der sich aus der Verwirklichung der Grundsätze des Übereinkommens des Europarates über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 ergibt, und dabei die Empfehlung R (87) 15 des Ministerausschusses des Europarates über die Nutzung personenbezogener Daten im Polizeibereich vom 17. September 1987 beachtet.

Alle Schengen-Staaten haben die erforderlichen datenschutzrechtlichen Vorschriften erlassen; diese werden jedoch mitunter auf unterschiedliche Weise umgesetzt. Es gibt Staaten, in denen Fragen bezüglich der Rechte der betroffenen Person vornehmlich durch unmittelbare Kontakte zwischen dieser Person und der für den nationalen Teil des SIS verantwortlichen Behörde geklärt werden. In anderen Staaten spielen die nationalen Aufsichtsbehörden eine wichtige Rolle als zwischengeschaltete Stelle zwischen dieser Behörde und betroffenen Personen.

Das SDÜ trägt diesen Unterschieden in einigen spezifischen Bestimmungen betreffend die Rechte der betroffenen Person Rechnung (z.B. Artikel 109). In Ermangelung einer Regelung zur Verbindung der Schengen- und der einzelstaatlichen Bestimmungen findet jedoch die Schengen-Bestimmung Anwendung, die eine besondere Regelung vorsieht (Artikel 104 Absatz 2).
Dies ist der Fall, wenn eine Klage im Sinne des Artikels 111 Absatz 1 bei einem nationalen Gericht oder einer zuständigen Behörde eines anderen als des für die Ausschreibung zuständigen Staates erhoben wird und diese Ausschreibung gleichzeitig in dem für die Ausschreibung zuständigen Staat ebenfalls Gegenstand eines Gerichtsverfahrens ist. In Artikel 111 ist diese Sachlage nicht geregelt. Unter Berücksichtigung des besonderen grundlegenden Charakters von Artikel 111 kann berechtigterweise der Schluss gezogen werden, dass in diesem Fall Artikel 111 maßgebend ist.

In der Praxis dürfte dies keine Schwierigkeiten bereiten, da bei den innerstaatlichen Verfahren aller Mitgliedstaaten der Grundsatz anerkannt wird, dass alle beteiligten Parteien gehört werden. Bei einem Verfahren im Sinne des Artikels 111 ergeht in der Praxis keine unanfechtbare Entscheidung, ohne dass der ausschreibende Staat gehört wird. Das Gericht oder die Behörde im Sinne des

Artikels 111 wird zweifellos dem Umstand Rechnung tragen, dass ein anderes Rechtsverfahren läuft.
Lagen diesbezüglich keine Informationen vor oder ist im Falle des Vorliegens von Informationen keine andere Entscheidung ergangen, so sind die Schengen-Staaten aufgrund des besonderen Charakters von Artikel 111 gezwungen, die unanfechtbare Entscheidung zu vollziehen. Zu bemerken ist ferner, dass für den Fall, dass eine solche Entscheidung zur Löschung der Schengen-Ausschreibung führt, es dem ausschreibenden Staat freisteht, eine nationale Ausschreibung in seine nationalen Systeme aufzunehmen. Ähnlich verhält es sich bei Artikel 25 SDÜ: Erteilt ein Schengen-Staat einem zur Einreiseverweigerung ausgeschriebenen Drittausländer einen Aufenthaltstitel, so sollte der ausschreibende Staat die Ausschreibung zurückziehen, jedoch den Drittstaatsangehörigen gegebenenfalls in seine nationale Ausschreibungsliste aufnehmen.

Obgleich Artikel 111 SDÜ den Begriff "unanfechtbare Entscheidung" nicht eindeutig bestimmt, sollte nach Meinung einiger Autoren der Begriff "*unanfechtbare Entscheidung"* nicht zu eng ausgelegt werden. Der Begriff würde demnach nicht nur Entscheidungen der höchsten (Verwaltungs-, Zivil- oder Straf-)Gerichte erfassen. Die Tatsache, dass Artikel 111 SDÜ und Artikel 43 der SIS-II-Verordnung auch auf Entscheidungen nationaler Datenschutzbehörden verwiesen, bedeute, dass eine Entscheidung als unanfechtbar betrachtet werden sollte, insoweit sie vollstreckbar sei und keine der Parteien Beschwerde gegen sie eingelegt habe." [1]

Ungeachtet der verschiedenen Auslegungsmöglichkeiten im Hinblick auf den Begriff "unanfechtbare Entscheidung" je nach den unterschiedlichen Rechtssystemen und rechtlichen Verfahren kam die GK in ihrer Stellungnahme zu dem Schluss, dass unanfechtbare Entscheidungen von Gerichten oder Behörden im Sinne von Artikel 111 betreffend eine von einer anderen Vertragspartei eingestellten Ausschreibung von der anderen Vertragspartei stets vollzogen werden sollten.

In Anbetracht des Urteils des Gerichtshofs (*Kommission der Europäischen Gemeinschaften gegen Königreich Spanien*)[1] und der Parallele, die zwischen der Verpflichtung der Schengen-Staaten zur Anerkennung und zum Vollzug der Entscheidung eines anderen Schengen-Staates zur Verweigerung der Einreise bzw. eines Visums und der Verpflichtung und Anerkennung der unanfechtbaren Entscheidung eines Gerichts oder einer Behörde zur Löschung einer SIS-Ausschreibung gezogen werden kann, wurden in der Praxis in einigen Fällen Entscheidungen nationaler Gerichte oder Behörden zur Löschung von Ausschreibungen nicht vollzogen – mit den entsprechenden negativen Folgen für die betreffende Person.

[1] Evelien Brouwer, "The Other Side of Moon. The Schengen Information System and Human Rights: A Task for National Courts", CEPS Working Document No. 288/April 2008.

4.2. Stellungnahmen zur Anwendung des Artikels 102a (SCHAC 2501/07)/ SCHAC 2504/08

Nach Artikel 102a Absatz 4 legt der Rat jedes Jahr, nachdem er die Stellungnahme der GK über die Anwendung dieses Artikels – insbesondere die anzuwendenden Datenschutzbestimmungen – eingeholt hat, dem Europäischen Parlament einen Bericht vor.

Aufgrund eines Ersuchens des Vorsitzenden der Gruppe "SIS/SIRENE" vom 31. Mai 2007 hat die GK im Juni 2007 eine Stellungnahme verabschiedet.
Durch Artikel 102a des SDÜ erhalten die in den Mitgliedstaaten für die Ausstellung von Zulassungsbescheinigungen für Fahrzeuge zuständigen Stellen erstmals Zugriff auf bestimmte im Schengener Informationssystem gespeicherte Daten. Dies gilt für Daten über gestohlene, unterschlagene oder sonst abhanden gekommene Kraftfahrzeuge, Anhänger und Wohnwagen sowie über Zulassungsbescheinigungen für Fahrzeuge und Kfz-Kennzeichenschilder.
Nach dem Beschluss 2006/228/JI dürfen Daten zu diesen Fahrzeugscheinen und Kfz-Kennzeichen seit dem 31. März 2006 im Schengener Informationssystem verarbeitet werden.

Aus dem Bericht ging eindeutig hervor, dass die durchgängige Anwendung von Artikel 102a noch nicht in allen Mitgliedstaaten gewährleistet war. Aufgrund dessen wurde in der Stellungnahme schwerpunktmäßig auf bestimmte Datenschutzaspekte im Zusammenhang mit der Anwendung eingegangen.
Da für das erste Jahr keine deutlich erkennbaren Ergebnisse vorlagen, konnte die GK nur schließen, dass die Kontrolle der Nutzung von Daten in Bezug auf Sachen, wie sie in Artikel 102a geregelt ist, nicht im Einklang mit Artikel 103 erfolgt war und dass der Rat eingehender prüfen sollte, ob die Mitgliedstaaten ihren Verpflichtungen gemäß Artikel 103 in Bezug auf Artikel 102a nachkommen.

Da eine strikte Anwendung von Artikel 103 nicht nur für den Zugang von Kfz-Zulassungsstellen wichtig war, gab die GK an, sie werde die nationalen Datenschutzbehörden ersuchen, darüber Auskunft zu geben, in welcher Weise Artikel 103 in ihren Ländern angewendet wird.

Der Berichtsentwurf enthielt die Bemerkung, Zulassungsbescheinigungen für Fahrzeuge und Kfz-Kennzeichenschilder seien keine personenbezogenen Daten. Die GK wies darauf hin, dass diese Bemerkung und der Kontext, in dem sie steht, sich nicht mit dem vereinbaren lassen, was als personenbezogene Daten betrachtet wird.

[1] ABl. C 86 vom 8.4.2006, S. 3.

Nach der allgemeinen Definition für personenbezogene Daten, wie sie in allen einschlägigen Rechtsakten im Datenschutzbereich verwendet wird, gelten als personenbezogene Daten "*alle Informationen über eine bestimmte oder bestimmbare natürliche Person; als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann".*

Die GK wies darauf hin, dass die nationalen Datenschutzbehörden Zulassungsbescheinigungen für Fahrzeuge und Kfz-Kennzeichenschilder generell als personenbezogene Daten betrachten, soweit sich aus den Umständen der Verarbeitung nicht bereits die Möglichkeit zur Identifizierung des Inhabers der Zulassungsbescheinigung oder des Kennzeichenschilds ergibt.

Des Weiteren nahm die GK mit Besorgnis zur Kenntnis, dass die Kontrollen gemäß Artikel 102a in einigen Ländern bereits vor Beginn der Anwendung dieses Artikels durchgeführt wurden. Dies ließ nur den Schluss zu, dass diese Tätigkeiten nach dem einzelstaatlichen Recht dieser Länder als Zweckentfremdung zu bewerten seien. Dieser Schluss bestärkte die GK nur in ihrer strategischen Linie, unermüdlich für die Schaffung von Kontrollmechanismen, einschließlich regelmäßiger Kontrollen der Nutzung des Schengener Informationssystems, zu werben.
Abschließend stellte die GK fest, dass sie die Umsetzung von Artikel 102a mit Sorge betrachtete, auch wenn eingeräumt werden musste, dass diese Umsetzung und die Verarbeitung der Daten über Kfz-Zulassungsbescheinigungen und Kennzeichenschilder durch alle Mitgliedstaaten noch nicht abgeschlossen war. Diese Sorge bezog sich insbesondere auf den offensichtlichen Mangel an Kontrolle der Datennutzung. Die GK rief den Rat eindringlich auf, dafür Sorge zu tragen, dass die Mitgliedstaaten ihren Verpflichtungen nach Artikel 103 in Bezug auf Artikel 102a nachkommen.

Die GK ersuchte darum, dass diese Stellungnahme dem Bericht an das Europäische Parlament als Anlage beigefügt wird.

Am 7. Juli 2008 wurde die GK von der Gruppe "SIS/SIRENE" ersucht, eine Stellungnahme zur Anwendung des Artikels 102a im Jahr 2007 abzugeben.

Die GK stellte in ihrer Stellungnahme fest, dass nicht berücksichtigt worden war, dass das SDÜ in neun der neuen Mitgliedstaaten am 1. September 2007 in Kraft getreten ist.

Nach Anhang I des Beschlusses 2007/471/EG des Rates gelten die Bestimmungen des Artikels 64 SDÜ und der Artikel 92 bis 119 SDÜ sowie der Verordnung (EG) Nr. 1160/2005 seit 1. September 2007 für die neuen Schengen-Staaten. Obgleich diese neuen Staaten Artikel 102a gegebenenfalls

noch nicht tatsächlich angewandt haben, enthielt der Bericht diesbezüglich keinerlei Informationen.

Erneut hob die GK hervor, dass ordnungsgemäß protokolliert werden muss, wie Kfz-Zulassungsstellen bestimmte Daten nutzen, um festzustellen, ob ein Kraftfahrzeug gestohlen oder unterschlagen wurde oder sonst abhanden gekommen ist. Da der Bericht ein ähnliches Gesamtbild wie im Jahr 2006 zeichnete, zog die GK das gleiche Fazit wie im Berichtszeitraum 2006, nämlich "*dass die Kontrolle der Nutzung sachbezogener Daten, wie sie in Artikel 102a geregelt ist, nicht im Einklang mit Artikel 103 erfolgt*". Die GK erinnerte zudem erneut an den Standpunkt der nationalen Datenschutzbehörden in der Frage, ob nach Artikel 102a in das SIS eingegebene Daten als personenbezogene Daten betrachtet werden, sowie an die Verpflichtungen der Mitgliedstaaten hinsichtlich der ordnungsgemäßen Anwendung des Artikels 103 in Bezug auf Artikel 102a.

4.3. Stellungnahme zur Einrichtung eines der Weiterleitung von SIRENE-Nachrichten dienenden Mail-Servers als zentraler Verteiler bei der technischen Unterstützungseinheit C.SIS (SCHAC 2502/07)

Die Gemeinsame Kontrollinstanz erhielt ein Ersuchen des Vorsitzenden des Ausschusses "Artikels 36" um Stellungnahme zur Einrichtung eines zentralisierten Verbindungsnetzes in Stern-Topologie für den SIRENE-Nachrichtenverkehr und zu den vorgeschlagenen Grundsätzen für die Kommunikation zwischen den Staaten. In ihrer Stellungnahme befasste sich die GK vorrangig mit den im Ersuchen dargelegten Grundsätzen für die Kommunikation sowie mit einigen Grundsätzen betreffend die Verfügbarkeit des Netzes.
Diesbezüglich hob die GK hervor, dass die technische Unterstützungseinheit des Schengener Informationssystems (C.SIS) sowie die vorgeschlagene Nutzung eines Mail-Servers bei dieser Unterstützungseinheit den Datenschutzgrundsätzen des SDÜ sowie den Grundsätzen des Übereinkommens des Europarates vom 28. Januar 1981 und der Empfehlung R (87) 15 des Ministerkomitees des Europarates entsprechen sollte. In Anbetracht dessen sollten folgende Qualitätsanforderungen erfüllt werden:

i) Vertraulichkeit: Es ist dafür zu sorgen, dass nur Zugangsberechtigte auf die Informationen zugreifen können;

ii) Verfügbarkeit: Es muss sichergestellt werden, dass die zugangsberechtigten Nutzer bei Bedarf auf die benötigten Informationen und sonstigen Mittel zurückgreifen können.

Die GK beschrieb die Umsetzung des Vertraulichkeitsgrundsatzes bei der Nutzung des Mail-Servers im C.SIS und bei den im Ersuchen dargelegten Verfahren und stellte diesbezüglich fest, dass Folgendes sichergestellt werden sollte:

1. Im Aufbewahrungszeitraum sollten Nachrichten stets in verschlüsselter Form gespeichert werden.
2. Nachrichten, die vom C.SIS an den Empfänger übermittelt wurden, sind nach Eingang der Empfangsbestätigung unverzüglich zu löschen.
3. Nachrichten, deren Übermittlung an den Empfänger gescheitert ist, sollten (nach einer bestimmten Anzahl fehlgeschlagener Versuche) grundsätzlich an den Absender zurückgeschickt werden, nebst dem betreffenden Statusbericht zur gescheiterten Mailzustellung.
4. Das Ersuchen enthielt keine Angaben über den kryptographischen Schlüssel, der von den SIRENE-Büros bei der Übermittlung von Nachrichten zu verwenden ist, falls der Backup-Server in Österreich (aufgrund eines Ausfalls des C.SIS-Servers) in Betrieb genommen wird.

    a) Entweder wird der Private Key der C.SIS-Unterstützungseinheit auch in ihrer Backup-Anlage (Österreich) verwendet und wäre somit aufgrund der Missachtung des bewährten Grundsatzes, wonach ein Private Key ausschließlich seinem Inhaber bekannt sein sollte, äußerst gefährdet, oder aber
    b) in Österreich wird ein anderer Schlüssel verwendet. Dann allerdings sollte es ein förmliches Verfahren geben, das die Vorgehensweise bei der Behebung von Unstimmigkeiten beschreibt, die sich aus der Verwendung unterschiedlicher Public Keys bei der Übermittlung von Nachrichten von den nationalen Büros zum Server ergeben. Darüber hinaus bedarf es einer Verfahrensbeschreibung hinsichtlich der Transition der mit dem Public Key des Backup-Servers verschlüsselt Nachrichten an den C.SIS-Server (und umgekehrt). Schließlich sollte ein Verfahren für die Rückwärtsauflösung in Bezug auf Nachrichten vorgegeben werden, die mit nicht länger gültigen Schlüsseln verschlüsselt wurden.

5. Zudem sollte ein Schlüsselverwaltungsverfahren festgelegt werden.
6. Es sollte dargelegt werden, wie mit Nachrichten zu verfahren ist, die (aus welchem Grund auch immer) als "Non-use" gekennzeichnet wurden.

Zur Gewährleistung des Verfügbarkeitsgrundsatzes bei der Nutzung des Mail-Servers beim C.SIS sollten folgende Maßnahmen ergriffen werden:

1. Um die Verfügbarkeit des die Mail-Zustellung abwickelnden Subsystems zu erhöhen, sollten für Mail-Server-Nachrichten eine andere Verbindung als für die Kommunikation zwischen N.SIS und C.SIS genutzt werden.
2. Der Mail-Server im C.SIS sollte zudem über eine alternative Verbindung für das Routing von Nachrichten für den Fall verfügen, dass die hierfür vorgesehene Hauptverbindung nicht zur Verfügung steht.

3. Es wurde empfohlen, eine kurze Risikoanalyse zu Fragen der Verfügbarkeit durchzuführen (Antwortzeiten, Reaktionszeit für den Backup, "Was-wenn"-Szenarien usw.). Für dieses spezifische Verfahren wird auch ein Notfallplan empfohlen.

4.4. Stellungnahme zu dem Entwurf von Durchführungsmaßnahmen einschließlich des SIRENE-Handbuchs für die zweite Generation des Schengener Informationssystems (SCHAC 2503/07)

Auf ein Ersuchen der Kommission hin um Stellungnahme zu dem Entwurf von Durchführungsmaßnahmen einschließlich des überarbeiteten SIRENE-Handbuchs für die zweite Generation des Schengener Informationssystems nahm die GK im Oktober 2007 eine Stellungnahme an.

In ihrer Stellungnahme befasste sich die GK besonders eingehend mit den Aufbewahrungsfristen für Protokolle, wobei sie sich fragte, warum anstelle des Zeitraums von einem Jahr, der sowohl in Artikel 18 Absatz 3 des Beschlusses 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)[1] als auch in Artikel 18 Absatz 3 der Verordnung des Europäischen Parlaments und des Rates[2] zum gleichen Gegenstand genannt wird, die längste Speicherdauer gewählt worden war.

Ein weiterer Punkt, der der GK Sorge bereitete, war die Löschung nicht mehr gültiger Europäischer Haftbefehle (EuHB). Die GK stellte fest, dass die Löschung abgelaufener EuHB nicht automatisch erfolgt, sondern von dem betreffenden Mitgliedstaat vorzunehmen ist.

Dieser prüft hierbei zudem, ob er gegen den Betroffenen weitere EuHB erlassen hat, die eine Verlängerung der Ausschreibung begründen könnten. Mit solchen Löschungsverfahren wurden nicht nur positive Erfahrungen gemacht, so dass eine automatische Löschung der betreffenden Aufzeichnungen empfohlen wurde. Die GK schlug vor, eine technische Lösung anzuwenden, wonach im Falle mehrerer EuHB zu derselben Person nur der EuHB und nicht die Ausschreibung gelöscht wird.

Die GK befasste sich in ihrer Stellungnahme auch eingehend mit dem Format und der Qualität der biometrischen Daten. Sie lenkte die Aufmerksamkeit auf die durch den Ratsbeschluss ermöglichte

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

umfassendere Nutzung von Fingerabdrücken und Lichtbildern. Solche biometrischen Daten sollten nur herangezogen werden, um die Identität einer Person zu bestätigen, die durch eine alphanumerische Abfrage im SIS II aufgefunden wurde.
In ihrer Analyse der möglichen Auswirkungen der Verknüpfung von Ausschreibungen auf die Grundsätze des Datenschutzes schlug die GK vor, dafür zu sorgen, dass in dem Text die Bestimmungen dahingehend geändert werden, dass die entscheidende Bedeutung der Zugangsrechte für die Gewährung des Zugangs zu verknüpften Ausschreibungen betont wird.

Hinsichtlich der Abfragemodalitäten für das SIS II betonte die GK, dass in Anbetracht des Zwecks dieses Informationssystems vorgeschrieben werden sollte, zuerst die Standardabfrage einzugeben, gegebenenfalls gefolgt von weiteren Abfragen entsprechend den Erfordernissen sowie den Ergebnissen der zuerst durchgeführten Standardabfrage. Die GK sprach sich nachdrücklich dafür aus, durch eine Textänderung zu verdeutlichen, dass im SIS II als erster Suchvorgang stets die Standardabfrage vorgeschrieben ist, erforderlichenfalls gefolgt von weiteren Abrufen.

Ein weiterer zu beachtender Aspekt war die Definition der "erweiterten Abfrage" (extended query) als Funktionalität zur Durchführung komplexer Abfragen, die nicht anhand anderer Arten von Abrufen vorgenommen werden können und die von den Nutzern unter Anwendung einer speziellen Abfragesprache festgelegt werden können. Die GK empfahl nachdrücklich, diese "erweiterte Abfrage" erneut zu prüfen und diejenigen Suchkriterien festzulegen, deren Anwendung im Rahmen des Ratsbeschlusses und der Verordnung zulässig ist.

Die GK ging zudem auf das überarbeitete SIRENE-Handbuch ein. Die GK prüfte eingehend die Nutzung des SIS II zu anderen Zwecken und fragte sich, wie das SIRENE-Büro des die Daten eingebenden Mitgliedstaats seiner Verpflichtung nach Artikel 7 Absatz 2 des Ratsbeschlusses und der Verordnung nachkommen kann, die Überprüfung der Qualität der in das SIS II eingegebenen Daten zu koordinieren.

Die GK befasste sich zudem mit den verschiedenen Verantwortlichkeiten für die Qualität der Daten sowie mit der Notwendigkeit spezifischer Regeln für die praktische Umsetzung und Überprüfung dieser Verantwortlichkeiten.

Weitere Aspekte, zu denen die GK Bedenken äußerte, waren die Eingabemaske mit 15 Angabenkategorien zu Fingerabdrücken und die Zweckmäßigkeit zusätzlicher Informationen, sowie die Übereinstimmung einer solchen Datenverarbeitung mit den Bestimmungen des Ratsbeschlusses und der Verordnung.

Als weiterer wichtiger Punkt wurde in dieser Stellungnahme die Beziehung zwischen SIRENE und Europol angesprochen. Die GK befürwortete nachdrücklich eine solche Zusammenarbeit, insoweit diese zur Qualität der im SIS II verarbeiteten Daten sowie dazu beiträgt, die Einhaltung bestimmter Artikel des Ratsbeschlusses betreffend den Zugang von Europol zum SIS II zu gewährleisten. Nach Artikel 41 Absatz 2 des Ratsbeschlusses hat Europol, wenn sich bei einer Abfrage durch Europol herausstellt, dass eine Ausschreibung im SIS II gespeichert ist, den ausschreibenden Mitgliedstaat davon in Kenntnis zu setzen. Kapitel 2.14 des Handbuchs verweist auf die nationale Europol-Stelle als Kontaktstelle der Mitgliedstaaten. Es wird allerdings darauf hingewiesen, dass seit der jüngsten Änderung des Europol-Übereinkommens[1] es der nationalen Europol-Stelle nicht länger möglich ist, als einziges Verbindungsbüro zwischen Europol und einem Mitgliedstaat zu fungieren (siehe Artikel 4 Artikel 2 des Europol-Übereinkommens). Zudem können – auch in Anbetracht der Aufgabenstellung Europols – die Gründe für die Unterrichtung eines Mitgliedstaats über die nationale Europol-Stelle mannigfaltig sein und mit dem Geheimhaltungsgrad der Informationen im Zusammenhang stehen. Eine Verpflichtung zur Unterrichtung der SIRENE über jeden Austausch, wie dies im Handbuch vorgeschlagen wird, verstößt gegebenenfalls gegen bestimmte Bedingungen, die für den Informationsaustausch zwischen Europol und seinen Kontaktstellen in den Mitgliedstaaten gelten. Die GK schlug daher vor, Kapitel 2.14 umzuformulieren und hinsichtlich der Verantwortlichkeit der Mitgliedstaaten für die Qualität der Daten eine Verpflichtung einzufügen, wonach dem SIRENE-Büro jede Information mitzuteilen ist, die sich aus Kontakten zwischen Europol und den Mitgliedstaaten ergibt und die zu einer Änderung oder Löschung einer SIS-II-Ausschreibung führen könnte.

4.5. Stellungnahme zu den Grundsätzen für die Zusammenarbeit zwischen den nationalen Kontrollinstanzen auf der Grundlage des SDÜ

Im November 1996 beschloss die GK, Grundsätze für die Zusammenarbeit zwischen den nationalen Kontrollinstanzen festzulegen. Aufgrund der Erfahrungen mit dieser Zusammenarbeit und einem Audit der GK zur Anwendung des Artikels 111 wurde eine Aktualisierung der Grundsätze aus dem Jahr 1996 beschlossen. Folglich nahm die GK im Juni 2008 eine neue Stellungnahme zu den Grundsätzen für die Zusammenarbeit zwischen den nationalen Kontrollinstanzen an.

Der verstärkte EU-weite Austausch strafverfolgungsrelevanter Informationen hat dazu geführt, dass Daten zu einer Person in verschiedenen Mitgliedstaaten und/oder EU-Einrichtungen verarbeitet werden können, wodurch es für die Betroffenen schwieriger wurde, ihre Rechte geltend zu machen. Weitere Hürden stellen sich dem Betroffenen aufgrund der unterschiedlichen nationalen Rechts-

[1] ABl. C 2 vom 6.1.2004, S. 3.

vorschriften und Verfahren sowie der bestehenden Sprachbarrieren.

Das SDÜ enthält Beispiele für die spezielle Zusammenarbeit zwischen nationalen Datenschutzbehörden bezüglich der Rechte der Betroffenen. Ein Betroffener darf in jedem der Schengen-Staaten ein Auskunftsersuchen stellen, auch wenn dieser Staat die ihn betreffenden Daten nicht in das Schengener Informationssystem eingegeben hat. Es gelten spezifische Regelungen für das anzuwendende Recht und die Zusammenarbeit zwischen nationalen Datenschutzbehörden. Obgleich der Begriff "in enger Abstimmung" im SDÜ nicht näher bestimmt wird, sind die Datenschutzbehörden gehalten, auf solche Weise zusammenzuarbeiten, dass sie sich untereinander sowie den sein Recht ausübenden Betroffenen umfassend unterstützen.

Was bedeutet dies konkret? Gemeint ist, dass die Ausübung der Rechte der Betroffenen gewährleisten sollte, dass diese Personen Zugang zur Justiz als grundlegendes Element eines wirksamen Rechtsschutzes erhalten.

Wichtig ist das SDÜ, weil darin anerkannt wird, dass es einem Betroffenen aufgrund der Reisekosten oder der Sprachenbarriere nicht immer möglich ist, sich zur Wahrnehmung seiner Rechte in einen anderen Staat zu begeben oder sich dort an eine Behörde zu wenden. Diesbezüglich liefern uns die Erfahrungen mit dem SIS und den Rechten von Betroffenen Erkenntnisse darüber, wie die Zusammenarbeit zwischen den nationalen Datenschutzbehörden weiter ausgebaut werden könnte.

Die betreffenden Grundsätze stützen sich auf folgende Artikel[1] des SDÜ:
Artikel 106 Absatz 3 bestimmt das Verfahren für den Fall, dass Schengen-Staaten sich nicht darüber einigen können, ob Daten unrichtig sind oder unrechtmäßig gespeichert worden sind.
Artikel 109 regelt das Auskunftsrecht und das anzuwendende Verfahren.
Artikel 110 beschreibt das Recht eines jeden, auf seine Person bezogene unrichtige Daten berichtigen oder unrechtmäßig gespeicherte Daten löschen zu lassen.
Artikel 111 bezieht sich auf das Recht, vor einem Gericht Klage zu erheben, sowie auf die von den Schengen-Staaten eingegangene Verpflichtung, unanfechtbare Entscheidungen der Gerichte zu vollziehen.
Artikel 114 regelt das Recht, die Kontrollinstanzen zu ersuchen, Daten zur eigenen Person zu überprüfen, sowie das für den Fall anzuwendende Verfahren, dass diese Daten von einem anderen Schengen-Staat eingegeben wurden.

In ihrer Stellungnahme prüfte die GK mehrere praktische Aspekte.

[1] Die neue Rechtsgrundlage für das SIS II enthält ähnliche Bestimmungen (ausgenommen Artikel 114).

Sprachen: Die Prüfung der Zusammenarbeit in der Praxis zeigte, dass Ersuchen oder die betreffenden Antworten gelegentlich in der Sprache der ersuchenden und der antwortenden Behörde formuliert wurden. Da die von den nationalen Kontrollinstanzen ausgearbeiteten Dokumente gegebenenfalls auch dem Betroffenen vorzulegen sind, könnte der Fall eintreten, dass dieser Informationen in einer ihm verständlichen Sprache erhält.
Zwei Szenarien wären möglich:

– Der gesamte Schriftwechsel erfolgt in einer einzigen Sprache; in diesem Fall wird die englische Sprache empfohlen.
– Der gesamte Schriftwechsel erfolgt in den Sprachen der Beteiligten, wobei jeder von ihnen dafür sorgt, dass eine amtliche Übersetzung in eine für die andere nationale Kontrollinstanz und den Betroffenen verständliche Sprache erstellt wird.

Fristen: Da grundlegende Interessen des Betroffenen berührt werden, erfolgt die Bearbeitung von Kooperationsersuchen ohne ungebührliche Verzögerung.

Kontaktpersonen: Zur weiteren Vereinfachung der Zusammenarbeit wird jede nationale Kontrollinstanz über eine Liste der Kontaktpersonen verfügen. In Anbetracht der Schwierigkeit, eine solche Liste ständig auf dem neuesten Stand zu halten, werden die Mitglieder der GK als Kontaktpersonen fungieren.

4.6. Stellungnahme zum Schengener Informationssystem (SIS) und zu gewalttätigen Störern 08/10

Im Sommer 2008 nahm die GK Kenntnis von den Beratungen der Gruppe "SIS/SIRENE" über den Rückgriff auf Artikel 99 SDÜ zur Ausschreibung gewalttätiger Störer ("violent troublemakers") im SIS. Im Mittelpunkt dieser Beratungen stand die Aufnahme neuer Kategorien von Daten in das SIS: Daten zu gewalttätigen Störern, denen der Zugang zu bestimmten Veranstaltungen, z.B. EU-Gipfeln oder ähnlichen Zusammenkünften, internationalen Sport- oder Kulturveranstaltungen oder anderen Großveranstaltungen unter Nutzung von SIS-Ausschreibungen nach Artikel 99 SDÜ zu verwehren ist.

Dieser Vorschlag warf aus der Sicht des Datenschutzes einige Fragen auf. Die GK brachte in einem Schreiben an den Vorsitzenden der Gruppe "SIS/SIRENE" Gemischter Ausschuss ihre Besorgnis und ihre Zweifel hinsichtlich dieser Initiative zum Ausdruck. Zudem bedauerte die GK, dass ihr Standpunkt in dieser Angelegenheit nicht schon früher eingeholt wurde.
Zuallererst merkte die GK an, dass Ausschreibungen nach Artikel 99 speziell auf die Verfolgung bereits initiierter Straftaten oder die Abwehr von Gefahren für die öffentliche Sicherheit abzielen.

Dies gilt als Voraussetzung für Ausschreibungen nach Artikel 99. Angesichts des vorgeschlagenen Zwecks in Bezug auf den Rückgriff auf Artikel 99 SDÜ könnte angenommen werden, die Abwehr von Gefahren für die öffentliche Ordnung sei das alleinige Ziel der (vorgeschlagenen) Ausschreibung. Zudem darf nach Artikel 99 nur eine SIS-Ausschreibung zu einer Person eingegeben werden, die in erheblichem Umfang **außergewöhnlich schwere Straftaten** plant oder begeht, oder wenn die Gesamtbeurteilung des Betroffenen, insbesondere aufgrund von Informationen über bisher von ihm begangenen Straftaten, erwarten lässt, dass er auch künftig **außergewöhnlich schwere Straftaten** begehen wird. Der Begriff **"außergewöhnlich schwere Straftat"** ist nicht im SDÜ definiert; zudem kann das Strafrecht in den verschiedenen Schengen-Staaten unterschiedlich ausgestaltet sein. In Anbetracht der Bezeichnung dieser Personenkategorie als "gewalttätige Störer" und des allgemeinen Kontextes, d.h. Großveranstaltungen wie internationale Sport- und Kulturveranstaltungen sowie EU-Gipfel und vergleichbare Zusammenkünfte (G8), zog die GK in Zweifel, ob die im Vorschlag beschriebenen Handlungen als "**außergewöhnlich schwere Straftaten**" eingestuft werden und eine Ausschreibung nach Artikel 99 begründen können.

Die GK wies zudem darauf hin, dass weder das SDÜ noch ein anderes europäisches oder internationales Rechtsinstrument den Begriff "Störer" definiert. Mangels einer eindeutigen Definition und einer einheitlichen Auslegung dieses Begriffes bestehe ein großes Risiko, dass unschuldige Personen völlig grundlos im SIS ausgeschrieben werden. Besagte Personenausschreibungen sollten den Ausschluss der Betroffenen von der Teilnahme an Veranstaltungen bewirken. Hierdurch würde es den Betroffenen verwehrt werden, sich in die Nähe solcher Veranstaltungen zu begeben oder gar in das Land einzureisen, in der diese stattfinden. Diesbezüglich erklärte die GK, dass Artikel 99 SDÜ keine Zwangsmaßnahmen vorsieht (der Artikel bildet keine Grundlage für Festnahmen) und ausschließlich zum Zwecke der verdeckten Registrierung oder gezielter Kontrolle angewandt werden kann. Somit war der eigentliche Zweck des Vorschlags nicht eindeutig und würde zweifelsohne eine Abweichung von dem ursprünglichen Zweck der Ausschreibungen nach Artikel 99 bewirken.
Das SDÜ sowie die neue Rechtsgrundlage des SIS II[1] lassen keine Zweifel darüber, dass diese Ausschreibungen nur für bestimmte Kategorien von Personen und Straftaten zulässig sind. Die betreffenden Tatbestände werden im SDÜ als "außergewöhnlich schwere Straftaten" und im Ratsbeschluss als "schwere Straftaten" mit einem eindeutigen Hinweis auf die in Artikel 2 des Rahmenbeschlusses über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten aufgeführten Straftaten beschrieben. Die einzigen in diesem Rahmenbeschluss aufgeführten und mit Gewalt verbundenen Straftaten, die sich im Kontext von Veranstaltungen ereignen könnten, die für bestimmte Personen gesperrt werden sollten, wären "vorsätzliche Tötung"

[1] Beschluss des Rates über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II).

oder "schwere Körperverletzung".

Ein weiterer Aspekt, der hervorgehoben wurde, war der Zweck der Ausschreibung und das erwartete Vorgehen. Nach Artikel 99 SDÜ dient die Ausschreibung der verdeckten Registrierung oder gezielten Kontrolle und nach Artikel 36 des Ratsbeschlusses der verdeckten oder gezielten Kontrolle.

Zudem hat die Überprüfung, die von der GK zu Artikel 99 durchgeführt worden war, eindeutig gezeigt, dass das nationale Recht bestimmter Schengen-Staaten den zuständigen nationalen Behörden keine Möglichkeit zur Durchführung gezielter Kontrollen gibt und dass in anderen Staaten hierzu eine gerichtliche Anordnung erforderlich ist[1].

In Anbetracht der vorgeschlagenen Nutzung dieser Ausschreibungen für den Ausschluss gewalttätiger Störer von der Teilnahme an bestimmten Veranstaltungen, was gegebenenfalls die Festnahme oder Ingewahrsamnahme dieser Personen beinhalten würde, kam die GK zu dem Schluss, dass diese Nutzung des Artikels 99 SDÜ gegen den im SDÜ und im Ratsbeschluss festgelegten Zweck verstoßen würde. Diese Feststellung sowie die Erkenntnis, dass gewalttätige Störer wohl in keiner Weise den Täterkategorien im SDÜ und dem Ratsbeschluss zugeordnet werden können, führten zu dem Fazit, dass die vorgeschlagene Nutzung nicht der Rechtsgrundlage entspricht und somit unrechtmäßig ist.

[1] Bericht der Gemeinsamen Kontrollinstanz Schengen über ein Audit der Anwendung von Ausschreibungen nach Artikel 99 SDÜ im Rahmen des Schengener Informationssystems, Dokument SCHAC 2501/08 vom 18. Januar 2008.

5. RECHTE DER BETROFFENEN

Das SDÜ legt die Rechte der Betroffenen fest und schafft hierdurch ein Regelwerk, dass es den Betroffenen ermöglicht, ihre Rechte in jedem Schengen-Staat geltend zu machen.

Nach Artikel 115 Absatz 3 des Schengener Durchführungsübereinkommens ist die gemeinsame Kontrollinstanz auch zuständig für die Prüfung der Anwendungs- oder Auslegungsfragen im Zusammenhang mit dem Funktionieren des Schengener Informationssystems, für die Prüfung von Fragen im Zusammenhang mit den von den nationalen Kontrollinstanzen der Vertragsparteien unabhängig vorgenommenen Kontrollen oder mit der Ausübung des Auskunftsrechts sowie für die Erarbeitung harmonisierter Vorschläge im Hinblick auf gemeinsame Lösungen für die bestehenden Fragen.

Es wird hervorgehoben, dass Titel IV Kapitel 3 SDÜ den Datenschutz und die Datensicherung im Schengener Informationssystem regelt. In diesem Kapitel werden die Verpflichtungen der am SIS teilnehmenden Staaten und die Rechte der Betroffenen dargelegt. Artikel 115 SDÜ regelt die Einrichtung der GK und beschreibt die Aufgaben und Zuständigkeiten dieser Kontrollinstanz. Dieser Artikel verleiht der GK keinerlei Zuständigkeiten oder Befugnisse für ein Eingreifen bei Konflikten zwischen Staaten in Einzelfällen.
Allerdings kann die GK dann Stellung nehmen, wenn sie Kenntnis über einen Fall erlangt, in dem das SDÜ Auslegungsfragen aufwirft, auf die näher eingegangen werden sollte oder die die Erarbeitung harmonisierter Vorschläge erfordern.

Am 17. August 2005 erhielt die GK ein Ersuchen des Rechtsbeistands des Drittstaatsangehörigen X. Die GK wurde unter Bezugnahme auf eine französische Ausschreibung nach Artikel 96 SDÜ und eine Entscheidung der österreichischen Datenschutzkommission zur Löschung dieser Ausschreibung ersucht, nach besten Kräften auf eine Lösung dieses Problemfalls hinzuarbeiten. Aufgrund einer von Frankreich eingegebenen Ausschreibung nach Artikel 96 SDÜ, die Herrn X die Einreise in den Schengen-Raum verwehrte, hatten die österreichischen Behörden Herrn X ein Visum verweigert. Dessen Rechtsbeistand stellte daraufhin ein Auskunftsersuchen zu den verarbeiteten Daten, woraufhin er vom österreichischen Bundesministerium für Inneres erfuhr, dass die französischen Behörden seinen Mandanten nach Artikel 96 im SIS ausgeschrieben hatten. Der Rechtsbeistand von Herrn X beantragte – über einen französischen Rechtsanwalt – bei der französischen Datenschutzbehörde CNIL die Löschung der Ausschreibung. Dieses Verfahren bewirkte jedoch nicht die Löschung der Daten. Der Rechtsbeistand von Herrn X legte anschließend

bei der österreichischen Datenschutzkommission Beschwerde gegen das französische Innenministerium ein. Die österreichische Datenschutzkommission entschied am 7. Juni 2005, der Beschwerde stattzugeben, und ordnete die Löschung der Ausschreibung innerhalb einer Frist von drei Wochen an. Diese hätte demnach bereits am 12. Juli 2005 gelöscht werden sollen. Die französischen Behörden löschten die Ausschreibung jedoch nicht. Daraufhin ersuchte der Rechtsbeistand von Herrn X die GK, sich mit diesem Fall zu befassen.

In diesem besonderen Fall stellte die GK das Zusammenfallen zweier unterschiedlicher Verfahren fest: ein Verfahren in Österreich, das zu einer Entscheidung der Datenschutzkommission geführt hatte, und ein Verfahren in Frankreich beim Conseil d'Etat (Staatsrat) infolge der Weigerung des französischen Innenministeriums, die von Herrn X beantragte Berichtigung oder Löschung der Ausschreibung vorzunehmen. In Anbetracht der Besonderheit dieses Falles legte die GK allen Beteiligten ihre Auslegung des Artikels 111 dar.

Bei Betrachtung des künftigen SIS-II-Rechtsrahmens betreffend die Rechte der Betroffenen ist festzustellen, dass dieser gegenüber dem SDÜ um einige neue positive Bestimmungen erweitert wurde. So haben nach Artikel 42 der Verordnung (EG) 1987/2006 Drittstaatsangehörige, die Gegenstand einer Ausschreibung nach dieser Verordnung sind, ein Recht auf Information. Der Beschluss 2007/533/JI des Rates und die Verordnung (EG) 1987/2006 legen den Schengen-Staaten eine größere Verantwortung auf, indem diese verpflichtet werden (Artikel 58 und 41), nach Eingang eines Antrags eines Betroffenen auf Auskunft bzw. auf Berichtigung oder Löschung von Daten den Antragsteller so schnell wie möglich zu informieren, spätestens jedoch 60 Tage nach Stellung des Antrags auf Auskunft oder früher, wenn die nationalen Rechtsvorschriften dies vorsehen.

Ein wichtiger Punkt ist, dass sowohl der Ratsbeschluss als auch die Verordnung die Staaten verpflichten, den Betroffenen so schnell wie möglich, spätestens jedoch drei Monate nach Stellung seines Antrags auf Berichtigung oder Löschung, oder früher, wenn die nationalen Rechtsvorschriften dies vorsehen, davon in Kenntnis zu setzen, welche Maßnahmen zur Wahrung seines Rechts auf Berichtigung oder Löschung getroffen wurden. Für den Betroffenen ist dieses Recht von allergrößter Bedeutung, da er zügig feststellen kann, welche ihn betreffenden personenbezogenen Daten im System verarbeitet werden.

6. ZUKUNFT DER GEMEINSAMEN ÜBERWACHUNG

Die Anwendung des Beschlusses 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) (nachstehend "Ratsbeschluss" genannt) und der 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) (nachstehend "Verordnung" genannt) wird mit einigen Neuerungen für den künftigen gemeinsamen Regelungsrahmen für die Überwachung des SIS II einhergehen. Wichtig ist zudem die Tatsache, dass die neue koordinierte Überwachung nicht weniger strikt sein wird als die im SDÜ festgelegte Kontrolle. Nach Artikel 61 der Ratsbeschlusses überwacht der Europäische Datenschutzbeauftragte, dass die Tätigkeiten der Verwaltungsbehörde zur Verarbeitung personenbezogener Daten im Einklang mit diesem Beschluss durchgeführt werden. Die Bestimmungen in Bezug auf die Aufgaben und Befugnisse nach den Artikeln 46 und 47 der Verordnung (EG) Nr. 45/2001 finden entsprechend Anwendung. Artikel 62 des Ratsbeschlusses schafft einen neuen Rechtsrahmen für das koordinierte Vorgehen der nationalen Kontrollinstanzen und des Europäischen Datenschutzbeauftragten; diese sollten im Rahmen ihrer jeweiligen Zuständigkeiten aktiv zusammenarbeiten und eine koordinierte Überwachung des SIS II gewährleisten. Die Verordnung enthält vergleichbare Bestimmungen. Die künftige Zusammenarbeit wird sich wie folgt gestalten: Im Rahmen ihrer jeweiligen Zuständigkeiten tauschen die nationalen Kontrollinstanzen und der Europäische Datenschutzbeauftragte einschlägige Informationen aus, unterstützen sich gegenseitig bei Überprüfungen und Inspektionen, prüfen Schwierigkeiten bei der Auslegung oder Anwendung des Ratsbeschlusses (bzw. der Verordnung), gehen Problemen bei der Wahrnehmung der unabhängigen Überwachung oder der Ausübung der Rechte betroffener Personen nach, arbeiten harmonisierte Vorschläge im Hinblick auf gemeinsame Lösungen für etwaige Probleme aus und fördern erforderlichenfalls die Sensibilisierung für die Datenschutzrechte.

Die nationalen Kontrollinstanzen und der Europäische Datenschutzbeauftragte treffen zu diesem Zweck mindestens zweimal jährlich zusammen. In der ersten Sitzung wird eine Geschäftsordnung angenommen. Weitere Arbeitsverfahren werden je nach Bedarf gemeinsam festgelegt. Ein gemeinsamer Tätigkeitsbericht ist dem Europäischen Parlament, dem Rat, der Kommission und der Verwaltungsbehörde alle zwei Jahre zu übermitteln. Somit werden der auf Artikel 115 SDÜ gestützte Mechanismus der gemeinsamen Überwachung und seine Infrastruktur in den neuen Kooperationsrahmen umgewandelt. Es sollte hervorgehoben werden, dass nach Artikel 44 der Verordnung die

von jedem Mitgliedstaat bezeichnete(n) Behörde(n), die mit den Befugnissen nach Artikel 28 der Richtlinie 95/46/EG ausgestattet ist/sind, die Rechtmäßigkeit der Verarbeitung personenbezogener SIS-II-Daten in ihrem Hoheitsgebiet und deren Übermittlung aus ihrem Hoheitsgebiet und den Austausch und die Weiterverarbeitung von Zusatzinformationen unabhängig überwacht/überwachen. Demnach erhalten die nationalen Kontrollinstanzen weiterreichende Befugnisse als nach Artikel 114 SDÜ.

Für den Datenschutz im Übergangszeitraum sieht Artikel 63 des Ratsbeschlusses Folgendes vor: "Überträgt die Kommission ihre Zuständigkeiten während der Übergangszeit gemäß Artikel 15 Absatz 4 einer oder mehreren anderen Stellen, so sorgt sie dafür, dass der Europäische Datenschutzbeauftragte das Recht und die Möglichkeit hat, seinen Aufgaben uneingeschränkt nachzukommen, einschließlich Überprüfungen vor Ort vorzunehmen und von sonstigen Befugnissen Gebrauch zu machen, die ihm aufgrund von Artikel 47 der Verordnung (EG) Nr. 45/2001 übertragen wurden." Allerdings sind noch die Datenschutzgarantien zu klären, die im Hinblick auf die gemeinsame Überwachung für die Phase der Migration vom SIS I+ zum SIS II vorgesehen sind. Welche neuesten Herausforderungen stellen sich der gemeinsamen Überwachung? Die reibungslose Datenmigration vom SIS 1+ zum SIS II und ein reibungsloser Übergang von der Gemeinsamen Kontrollinstanz zur koordinierten Überwachung? Am 30. Juni 2008 organisierte der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments ein Rundtisch-Gespräch zum Thema "Freiheit und Sicherheit beim integrierten Management der Grenzen der EU", wobei auch das Thema "Auswirkungen der Migration vom SIS I+ zum SIS II auf den Datenschutz" erörtert wurde. Der Vorsitz der GK und der Europäische Datenschutzbeauftragte wurden gebeten, einen Diskussionsbeitrag zu leisten und ihre Standpunkte zu dieser Frage darzulegen. Beide vertraten einheitlich die Position, dass es zu keiner Überschneidung der Zuständigkeiten der beiden Überwachungsgremien kommen wird. Der Europäische Datenschutzbeauftragte gab seiner Zuversicht Ausdruck, dass ein reibungsloser Übergang bei der Überwachung des Systems erzielt werden könne; die Migrationsphase würde die Gelegenheit bieten, diese "Partnerschaft" in die Wege zu leiten.

Beide Sprecher bekräftigten ihr Vertrauen in eine erfolgreiche koordinierte Überwachung des Systems in der Übergangszeit, als Vorbereitung der konkreten gemeinsamen Überwachung. Bei Betrachtung des künftigen Rahmens für die koordinierte Überwachung müssen die Bedeutung und der Einfluss der Arbeiten der Gemeinsamen Kontrollinstanz gewürdigt und anerkannt werden. Über Jahre hinweg hat sie entschlossen und hart gearbeitet, Erfahrung gesammelt, Kenntnisse erworben und Vertrauen in ihre Kompetenz aufgebaut, was von unschätzbarem Wert für die künftigen Arbeiten sein wird, die die nationalen Kontrollinstanzen gemeinsam mit dem Euro-

päischen Datenschutzbeauftragten aufnehmen werden. Selbstverständlich wird die Überwachung einer derart komplexen Datenbank wie das SIS II zusätzliche Zeit und Anstrengungen erfordern, um die Wirksamkeit einer solchen koordinierten Überwachung unter Beweis zu stellen. Es besteht kein Zweifel daran, dass die Überwachung auch weiterhin gut funktionieren wird und von der Erfahrung und dem Wissen der GK profitieren wird.

7. MITGLIEDER DER GEMEINSAMEN KONTROLLINSTANZ SCHENGEN

Vorsitzender: **Herr Georges de La LOYÈRE**

Stellvertretende Vorsitzende: **Frau Angelika SCHRIEVER-STEINBERG**

ÖSTERREICH MITGLIEDER Frau Waltraut KOTSCHY Frau Eva SOUHRADA-KIRCHMAYER STELLVERTRETENDE MITGLIEDER Herr Gregor KÖNIG	BELGIEN MITGLIEDER Herr Willem DEBEUCKELAERÉ Herr Bart DE SCHUTTER STELLVERTRETENDE MITGLIEDER Frau Priscilla de LOCHT
TSCHECHISCHE REPUBLIK MITGLIEDER Frau Ludmila NOVAKOVA STELLVERTRETENDE MITGLIEDER Frau Miroslava MATOUŠOVÁ	DÄNEMARK MITGLIEDER Frau Lena ANDERSEN Herr Sten HANSEN STELLVERTRETENDE MITGLIEDER Herr Jens Harkov HANSEN Herr Ole TERKELSEN
ESTLAND MITGLIEDER Herr Taago PÄHKEL STELLVERTRETENDE MITGLIEDER Frau Kaja PUUSEPP	FINNLAND MITGLIEDER Herr Reijo AARNIO Frau Elisa KUMPULA STELLVERTRETENDE MITGLIEDER Herr Heikki HUHTINIEMI
FRANKREICH MITGLIEDER Herr Georges de La LOYÈRE STELLVERTRETENDE MITGLIEDER Herr Michel MAZARS	DEUTSCHLAND MITGLIEDER Herr Peter SCHAAR Frau Angelika SCHRIEVER-STEINBERG STELLVERTRETENDE MITGLIEDER Herr Wolfgang Von POMMER ESCHE Herr Michael RONELLENFITSCH
GRIECHENLAND MITGLIEDER Herr Leonidas KOTSALIS STELLVERTRETENDE MITGLIEDER Frau Maria ALIKAKOU	UNGARN STELLVERTRETENDE MITGLIEDER Frau Agnes PAJÓ
ISLAND MITGLIEDER Herr Bjorn GEIRSSON Frau Sigrun JOHANNESDOTTIR Frau Thórdur SVEINSSON	ITALIEN MITGLIEDER Herr Giovanni BUTARELLI Frau Vanna PALUMBO

LETTLAND MITGLIEDER Frau Signe PLUMINA Frau Aiga BALODE	LITAUEN MITGLIEDER Frau Rita VAITKEVIČIENĖ Frau Neringa KAKTAVIČIŪTĖ-MICKIENĖ
LUXEMBURG MITGLIEDER Herr Georges WIVENES Herr Pierre WEIMERSKIRCH STELLVERTRETENDE MITGLIEDER Herr Thierry LALLEMANG	MALTA STELLVERTRETENDE MITGLIEDER Herr David CAUCHI
NIEDERLANDE MITGLIEDER Herr Jacob KOHNSTAMM Frau Jannette BEUVING STELLVERTRETENDE MITGLIEDER Frau Laetitia KRÖNER	NORWEGEN MITGLIEDER Herr George APENES Frau Guro SLETTEMARK STELLVERTRETENDE MITGLIEDER Frau Astrid FLESLAND
POLEN MITGLIEDER Herr Michał SERZYCKI STELLVERTRETENDE MITGLIEDER Herr Piotr DROBEK	PORTUGAL MITGLIEDER Herr Luis BARROSO Frau Isabel CERQUEIRA DA CRUZ STELLVERTRETENDE MITGLIEDER Frau Clara VIEIRA CARDOSO GUERRA
SLOWAKISCHE REPUBLIK MITGLIEDER Herr Peter LIESKOVSKÝ STELLVERTRETENDE MITGLIEDER Herr Tomaš MIČO	SLOWENIEN MITGLIEDER Frau Alenka JERŠE Frau Natasa PIRC MUSAR STELLVERTRETENDE MITGLIEDER Herr Marijan ÈONÈ
SPANIEN MITGLIEDER Herr Rafael GARCÍA GOZALO STELLVERTRETENDE MITGLIEDER Frau Marta AGUIRRE CALZADA	SCHWEDEN MITGLIEDER Frau Elizabeth WALLIN STELLVERTRETENDE MITGLIEDER Frau Birgitta ABJÖRNSSON
SCHWEIZ MITGLIEDER Herr Bruno BAERISWYL Herr Jean-Philippe WALTER	

8. BEOBACHTER DER GEMEINSAMEN KONTROLLINSTANZ SCHENGEN

BULGARIEN Herr Veselin TSELKOV Herr Valentin ENEV	Zypern Frau Goulla FRANGOU Frau Louiza MARKIDOU
IRLAND Herr Billy HAWKES Frau A. GARDNER Frau A. McCABE	LIECHTENSTEIN Herr Philipp MITTELBERGER
RUMÄNIEN Frau Georgeta BASARABESCU Herr George GRIGORE	VEREINIGTES KÖNIGREICH Herr David Smith Frau Jane DAWSON