Vorblatt

Problem:

Mit der Schaffung eines EU-Polizeikooperationsgesetzes soll eine einheitliche Grundlage für die umfangreichen und teils auch sehr spezifischen Formen der polizeilichen Kooperation mit den Mitgliedstaaten der Europäischen Union geschaffen werden. Allerdings sind die vom Rat der Europäischen Union beschlossenen, unten angeführten Rechtsakte zwar für Österreich gemäß den Bestimmungen des Vertrags über die Europäische Union verbindlich, jedoch nicht unmittelbar wirksam (Art. 34 Abs. 2 lit. c EUV).

Ziel:

Mit dem vorliegenden Entwurf sollen die in den unten angeführten Rechtsakten enthaltenen unionsrechtlichen Vorgaben hinsichtlich der polizeilichen Kooperation in innerstaatliches Recht umgesetzt werden.

Inhalt /Problemlösung:

Ohne diese innerstaatliche Umsetzung sind die in den Rechtsakten enthaltenen, unionsrechtlichen Vorgaben nicht vollziehbar.

Alternativen:

Eine gesetzliche Bestimmung, die lediglich die innerstaatliche unmittelbare Anwendbarkeit der angeführten Beschlüsse anordnet, läuft Gefahr auch Bereiche mit einzubeziehen, die außerhalb des sachlichen und räumlichen Normenbereiches österreichischer Gesetze liegen; beispielsweise Regelungen technischer und haushaltsrechtlicher Natur im Beschluss über das Schengener Informationssystem der zweiten Generation oder die Einrichtung der Europolorgane einschließlich deren Aufgaben und haushaltsrechtliche Vorgaben an Europol, wie es der Europol-Beschluss vorsieht.

Andererseits würde eine Novellierung von Gesetzen wie insbesondere des Polizeikooperationsgesetzes und des Sicherheitspolizeigesetzes vor allem im Lichte der sehr unterschiedlichen Regelungsbereiche der Rechtsakte die Systematik und Übersichtlichkeit dieser Gesetze beeinträchtigen. Überdies ist es derzeit als sehr wahrscheinlich anzusehen, dass weitere Rechtsakte zu unterschiedlichsten Regelungsbereichen erlassen werden, was dieses Problem noch verschärfen würde.

Auswirkungen des Regelungsvorhabens:

– Finanzielle Auswirkungen:

Artikel 1 und 2: Einige der umzusetzenden Beschlüsse bedingen Mehrkosten, auf die im allgemeinen Teil der Erläuterungen näher eingegangen wird. Es ist aber auch darauf hinzuweisen, dass mit Ausnahme der Möglichkeit des Zugriffes auf das erst zu schaffende Visa-Informationssystem die in den Beschlüssen enthaltenen Regelungen bereits jetzt weitestgehend geltendes Recht darstellen, allerdings auf anderen Rechtsgrundlagen beruhend. So fallen insbesondere bereits jetzt Kosten auf Grund des Europol-Übereinkommens, des Schengener Durchführungsübereinkommens sowie des Prümer Vertrages an. Als finanzielle Auswirkungen zu berücksichtigen waren hier aber nur die zusätzlichen Kosten, die sich aus der Umsetzung der Beschlüsse ergeben.

Artikel 3: Durch die im § 58b Abs. 1 und 4 SPG geschaffene Möglichkeit der Anfertigung und Speicherung von Lichtbildern bei der Aufnahme bzw. der Verpflichtung der Löschung von Lichtbildern bei der Entlassung von Personen sowie durch die Aufgabenerweiterung des Rechtsschutzbeauftragten in § 91c Abs. 1 SPG ist mit Mehrausgaben zu rechnen.

Die Zusatzkosten finden im Rahmenbudget des Bundesministeriums für Inneres ihre Bedeckung. Näheres ist der Darstellung der finanziellen Auswirkungen im allgemeinen Teil zu entnehmen.

– Wirtschaftspolitische Auswirkungen:

– – Auswirkungen auf die Beschäftigung und den Wirtschaftsstandort Österreich:

keine

– – Auswirkungen auf die Verwaltungslasten für Unternehmen:

Es sind keine Informationsverpflichtungen für Unternehmen vorgesehen.

– Auswirkungen in umweltpolitischer, konsumentenschutzpolitischer sowie sozialer Hinsicht:

keine

– Geschlechtsspezifische Auswirkungen:

keine

Verhältnis zu Rechtsvorschriften der Europäischen Union:

Mit diesem Bundesgesetz werden umgesetzt:

- der Beschluss des Rates vom 6. April 2009 zur Errichtung des Europäischen Polizeiamts (Europol), Amtsblatt L121/2009, S. 37 - 66
- der Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, Amtsblatt Nr. L 210 vom 6.8.2008, S. 1 -11, sowie Beschluss 2008/616/JI des Rates vom 23. Juni 2008 zur Durchführung des Beschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, Amtsblatt Nr. L 210 vom 6.8.2008, S. 12 – 72
- der Beschluss 2008/617/JI des Rates vom 23. Juni 2008 über die Verbesserung der Zusammenarbeit zwischen den Spezialeinheiten der Mitgliedstaaten der Europäischen Union in Krisensituationen, Amtsblatt Nr. L 210 vom 6.8.2008, S. 73 - 75
- der Beschluss 2008/633/JI des Rates vom 23. Juni 2008 über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten, Amtsblatt Nr. L 218 vom 13.8.2008, S. 129 - 136
- der Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), Amtsblatt Nr. L 205 vom 7.8.2007, S. 63 – 84

Besonderheiten des Normerzeugungsverfahrens:

keine.

Erläuterungen

Allgemeiner Teil

Hauptgesichtspunkte des Entwurfes:

Mit dem vorliegenden Entwurf eines EU-Polizeikooperationsgesetzes (EU-PolKG) in Art. 1 und 2 soll ein Gesetz geschaffen werden, das die der sogenannten „dritten Säule“ zuzurechnende polizeiliche Zusammenarbeit mit den Mitgliedstaaten der Europäischen Union in einem Gesetzeswerk erfassen soll. Hintergrund dafür sind mehrere teilweise sehr detaillierte, von der Europäischen Union beschlossenen, eingangs angeführten Rechtsakte nach Art. 34 Abs. 2 lit. c EUV. Diese Rechtsakte berühren sehr unterschiedliche Bereiche, auf die nachfolgend im Einzelnen näher eingegangen wird.

Vorweg ist festzuhalten, dass mit Ausnahme der Möglichkeit des Zugriffes auf das erst zu schaffende Visa-Informationssystem die in den Beschlüssen enthaltenen Regelungen bereits jetzt weitestgehend geltendes Recht darstellen, allerdings auf anderen Rechtsgrundlagen beruhend. So finden sich die Regelungen über das Europäische Polizeiamt (Europol) derzeit im Europol-Übereinkommen (BGBl. III Nr. 123/1998), zum Schengener Informationssystem im Schengener Durchführungsübereinkommen (BGBl. III Nr. 90/1997) und die Regelungen im „Prüm-Beschluss“ neben anderen auch schon im Prümer Vertrag (BGBl. III Nr. 159/2006). Aufgrund der in den entsprechenden Beschlüssen enthaltenen Aufhebung bzw. Ersetzung dieser Übereinkommen bedarf es allerdings der Schaffung einer neuen innerstaatlichen Rechtsgrundlage, zumal die Beschlüsse zwar völkerrechtlich verbindlich, aber nicht unmittelbar wirksam sind.

Der Entwurf enthält nur insoweit Regelungen, als in den Rechtsakten enthaltene, Österreich bindende Vorgaben nicht bereits jetzt auf geltendes Recht gestützt werden können oder Abweichungen von geltendem Recht vorzusehen waren.

Die vorgeschlagenen Änderungen des Sicherheitspolizeigesetzes im Artikel 3 betreffen einerseits die Verwendung von Lichtbildern für Zwecke der Vollzugsverwaltung und andererseits die Ausweitung des kommissarischen Rechtsschutzes.

Inhalt /Problemlösung:

Ausgehend von den Bestrebungen der Europäischen Union, der polizeilichen Zusammenarbeit zwischen den Mitgliedstaaten auch künftig breiten Raum zu widmen und diese Zusammenarbeit im Interesse der Schaffung eines gemeinsamen Raums der Freiheit, der Sicherheit und des Rechts wohl noch intensiviert werden dürfte, wird vorgeschlagen, die angeführten Rechtsakte in einem neu zu schaffenden Gesetz in innerstaatliches Recht umzusetzen. Es kann daher derzeit davon ausgegangen werden, dass weitere unionsrechtliche Regelungen über die polizeiliche Zusammenarbeit folgen werden; diese könnten dann ebenfalls im vorgeschlagenen Gesetz implementiert werden, was insbesondere auch der Überschaubarkeit und Rechtssicherheit der auf Unionsrecht zurückzuführenden Vorgaben dient.

Geprüft wurden aber auch Alternativen zur Schaffung eines eigenen Gesetzes:

So etwa würde einerseits eine gesetzliche Bestimmung, die lediglich die innerstaatliche unmittelbare Anwendbarkeit der angeführten Beschlüsse anordnet, Gefahr laufen, auch Bereiche einzubeziehen, die außerhalb des sachlichen und räumlichen Normenbereiches österreichischer Gesetze liegen; beispielsweise Regelungen technischer (CS.SIS) und EU-haushaltsrechtlicher Natur hinsichtlich des Beschlusses über das Schengener Informationssystem der zweiten Generation, weiters die Einrichtung der Europolorgane, deren Aufgaben sowie haushaltsrechtliche Vorgaben für Europol, wie es der Europol-Beschluss vorsieht.

Eine Novellierung bestehender Gesetze, wie insbesondere des Polizeikooperationsgesetzes und des Sicherheitspolizeigesetzes, würde andererseits vor allem im Lichte der sehr unterschiedlichen Regelungsbereiche der Rechtsakte die Systematik dieser Gesetze beeinträchtigen. Dazu kommt, dass die zahlreichen, sehr detaillierten Regelungen in den Rechtsakten zu unterschiedlichsten Bereichen polizeilicher Zusammenarbeit deutlich über den Zweck des geltenden PolKG hinausgehen würden. Die polizeiliche Zusammenarbeit im und außerhalb des Rahmens der Europäischen Union sollte aus Gründen der besseren Verständlichkeit und Anwendbarkeit in zwei verschiedenen Bundesgesetzen geregelt werden: Die seit Inkrafttreten des Vertrags von Maastricht am 1.11.1993 zusehends intensivere polizeiliche Zusammenarbeit der Mitgliedstaaten der Europäischen Union soll daher in einem eigenen Gesetz (EU-PolKG) ihren Niederschlag finden, wogegen für die schon wesentlich länger bestehende bi- und multilaterale Zusammenarbeit außerhalb des rechtlichen Rahmens der Europäischen Union das PolKG weiterhin allgemeine Geltung behalten soll.

Der Entwurf sieht einen allgemeinen Teil vor, der jene Bestimmungen zusammenfasst, wie sie für alle umzusetzenden Rechtsakte gelten. Daran anschließend finden sich die aus der Umsetzung der Rechtsakte notwendigen innerstaatlichen Bestimmungen jeweils in einem eigenen Teil. Der Schlussteil enthält die Inkrafttretensbestimmung, die Gender-Bestimmung sowie eine Verweisungsreglung. Dies scheint dem Aufbau und der Systematik durchaus förderlich zu sein, da die Rechtsakte zum Teil sehr unterschiedliche Bereiche regeln und eine nicht konsequente Trennung verwirrend sein könnte.

Schließlich ist noch auf den Rahmenbeschluss 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union, Amtsblatt Nr. L 386 vom 29.12.2006, S. 89 - 100 und Amtsblatt Nr. L 75 vom 15.3.2007, S. 26 (Berichtigung) einzugehen: Dieser Rahmenbeschluss wurde im Zuge der Umsetzungsarbeiten der eingangs angeführten EU-Rechtsakte ebenfalls auf die Notwendigkeit einer innerstaatlichen legistischen Umsetzung geprüft. Als Ergebnis ist festzuhalten, dass die Vorgaben aus dem Rahmenbeschluss bereits jetzt auf das PolKG gestützt werden können oder – mangels Außenwirkung – einer Regelung im Erlassweg zugängig sind. So ist etwa in der vorgesehenen Verwendung bestimmter Formulare eine rein administrative Regelung zu sehen. Gleiches gilt auch für die Einhaltung bestimmter Fristen, binnen derer eine Anfrage zu beantworten sein wird.

1. Zum Beschluss des Rates vom 6. April 2009 zur Errichtung des Europäischen Polizeiamts (Europol), Amtsblatt L121/2009, S. 37 - 66

Die Errichtung eines Europäischen Polizeiamtes (Europol) mit Sitz in Den Haag (Niederlande) wurde im Vertrag über die Europäische Union vom 7. Februar 1992 vereinbart und durch das Europol–Übereinkommen auf der Grundlage des Artikels K.3 des Vertrages über die Europäische Union bezüglich der Errichtung von Europol (Vertrag von Maastricht) geregelt. In der Folge wurde am Europol-Übereinkommen eine Reihe von Anpassungen vorgenommen, die nach einem langwierigen Ratifizierungsprozess in allen Mitgliedstaaten der Union in Kraft getreten sind. Auch Österreich hat das Übereinkommen (BGBl. III Nr. 123/1998) und die nachfolgenden Änderungsprotokolle ratifiziert (BGBl. III Nr. 193/1998, BGBl. III Nr. 81/1999, BGBl. III Nr. 120/2007, BGBl. III Nr. 121/2007 und BGBl. III Nr. 122/2007).

Durch die Ersetzung des Europol–Übereinkommens durch einen Beschluss des Rates sollen künftige Änderungen im Sinne einer schnelleren Anpassung Europols an die Bedürfnisse moderner Kriminalitätsbekämpfung erleichtert und Europol ein flexibleres Reagieren auf neue Herausforderungen ermöglicht werden.

Die Etablierung Europols als eine aus dem Gesamthaushaltsplan der Europäischen Union finanzierte Sicherheitsagentur trägt zur Vereinfachung und Verbesserung des Europol–Rechtsrahmens bei, da in der Folge im Wesentlichen die allgemeinen gemeinschafts- bzw. unionsrechtlichen Vorschriften und Verfahren der anderen vom Gemeinschaftshaushalt finanzierten Agenturen Anwendung finden. In Bereichen, die unter Titel VI des Vertrages über die Europäische Union fallen, wurden bereits vergleichbare Einrichtungen der Union geschaffen, wie beispielsweise Eurojust – eingerichtet mittels Beschluss des Rates 2002/187/JI vom 28. Februar 2002 zur Errichtung von Eurojust zur Verstärkung der Bekämpfung der schweren Kriminalität – und CEPOL – eingerichtet durch den Beschluss 2005/681/JI des Rates vom 20. September 2005 über die Errichtung der Europäischen Polizeiakademie. Die Rechtsaktsform des Beschlusses des Rates ermöglicht eine flexiblere Anpassung der genannten Organisationen an neue Situationen und politische Prioritäten, wie insbesondere das Stockholmer Programm, das dem Haager Programm nachfolgt.

Das Ziel von Europol liegt darin, die Leistungsfähigkeit der zuständigen Behörden der Mitgliedstaaten und ihre Zusammenarbeit im Hinblick auf die Verhütung und Bekämpfung des Terrorismus, des illegalen Drogenhandels und sonstiger schwerwiegender Formen der internationalen Kriminalität zu verbessern, sofern tatsächliche Anhaltspunkte für eine kriminelle Organisationsstruktur vorliegen und von den genannten Kriminalitätsformen zwei oder mehr Mitgliedstaaten in einer Weise betroffen sind, die aufgrund des Umfangs, der Bedeutung und der Folgen der strafbaren Handlungen ein gemeinsames Vorgehen der Mitgliedstaaten erfordert.

Zu den wichtigsten Neuerungen:

Eine der wichtigen Verbesserungen Europols in der Unterstützung der Mitgliedstaaten stellt die Mandatserweiterung dar: Europol wird nun zuständig für die Prävention und Bekämpfung von Schwerkriminalität einschließlich organisierter Kriminalität und Terrorismus sowie anderer Kriminalitätsformen, die im Annex des Beschlusses - und als Anlage zu diesem Gesetz - angeführt sind, wenn zwei oder mehrere Mitgliedstaaten in einer Weise betroffen sind, die gemeinsames Handeln

erfordert. Damit entfällt der Nachweis, dass tatsächliche Anhaltspunkte für eine kriminelle Organisationsstruktur vorliegen müssen.

Der Beschluss enthält auch die Möglichkeit für Europol, leichter neue Datenverarbeitungssysteme zu schaffen, um flexibler auf neue Formen von Kriminalität reagieren zu können. Darüber entscheidet der Verwaltungsrat, basierend auf einem Vorschlag des Europol-Direktors, nach Konsultation der Gemeinsamen Kontrollinstanz. Diese Entscheidung wird dem Rat zur Verabschiedung vorgelegt. Dabei werden die Rechtsgrundsätze, die im Übereinkommen des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten verankert sind und im Einklang mit der Empfehlung Nr. R (87) 15 des Ministerkomitees des Europarates vom 17. September 1987 stehen.

Auch die Kontrolle durch das Europäische Parlament wird verbessert: der Ratsvorsitzende, der Vorsitzende des Verwaltungsrates und der Direktor von Europol müssen auf Anforderung vor dem Parlament erscheinen. Somit ist eine gewisse Transparenz und Rechenschaftspflicht gewährleistet, wobei operative Informationen vertraulich behandelt werden.

Der bereits bestehende hohe Datenschutzstandard bei Europol erfährt insbesondere durch die Einführung eines Datenschutzbeauftragten, der auf Vorschlag des Europol-Direktors vom Verwaltungsrat ernannt wird, eine Verbesserung. Dieser hat die Aufgabe, auf unabhängige Weise zu gewährleisten, dass personenbezogene Daten einschließlich der gemäß Artikel 24 der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr geschützten Daten des Europol – Personals rechtmäßig und im Einklang mit diesem Beschluss verarbeitet werden.

2. Zum Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, Amtsblatt Nr. L 210 vom 6.8.2008, S. 1 -11, und Beschluss 2008/616/JI des Rates vom 23. Juni 2008 zur Durchführung des Beschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, Amtsblatt Nr. L 210 vom 6.8.2008, S. 12 – 72, sowie zum Beschluss 2008/617/JI des Rates vom 23. Juni 2008 über die Verbesserung der Zusammenarbeit zwischen den Spezialeinheiten der Mitgliedstaaten der Europäischen Union in Krisensituationen, Amtsblatt Nr. L 210 vom 6.8.2008, S. 73 – 75.

Am 27. Mai 2005 wurde in Prüm/Deutschland der Vertrag über die Vertiefung der grenzüberschreitenden Zusammenarbeit insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration (Prümer Vertrag) zwischen Belgien, Deutschland, Spanien, Frankreich, Luxemburg, den Niederlanden und Österreich unterzeichnet. Der ratifikationspflichtige Staatsvertrag steht allen Mitgliedstaaten der Europäischen Union zum Beitritt offen. Alle sieben Unterzeichnerstaaten haben die Ratifikation abgeschlossen. Finnland, Slowenien, Ungarn, Estland, Rumänien, Slowakei und Bulgarien sind dem Vertrag beigetreten und Portugal, Italien und Schweden haben ihr Interesse an einem Beitritt bekannt gegeben.

Nach einem Beobachtungszeitraum war die Überführung des Prümer Vertrages in ein EU Rechtsinstrument vorgesehen, sofern sich dieses Instrument als geeignet erweisen sollte (siehe Ausführungen der Präambel sowohl des Vertrags als auch des Beschlusses). Der Vertrag war als „Pilotprojekt“ einiger EU-Staaten gedacht. Nach den sofortigen enormen Erfolgen des Onlinedatenaustausches im DNA-Bereich setzte aber bereits unmittelbar nach Bekanntwerden dieser Ergebnisse nach der Aufnahme des Echtbetriebes im Dezember 2006 zwischen Österreich und Deutschland ein großer Antrag von Beitrittsgesuchen weiterer EU-Staaten ein, der dazu führte, dass diese Frist nicht mehr länger abgewartet wurde.

Die Bundesrepublik Deutschland startete Anfang 2007 im Zuge ihrer EU-Präsidentschaft eine Initiative zur Überführung des Prümer Vertrags in das EU-Recht und legte gemeinsam mit den Prüm-Partnern den Entwurf eines Beschlusses zur Überführung eines Teils der Bestimmungen des Prümer Vertrags vor: Datenaustausch in den Bereichen DNA-Profile, daktyloskopische Daten, Kfz-Register, Großereignisse und Terrorismusprävention; gemeinsame Einsatzformen und Hilfeleistung bei Großereignissen, Katastrophen und schweren Unglücksfällen.

Die Arbeiten am Beschluss verliefen sehr erfolgreich. Daher konnte bereits beim JI-Rat am 12. Juni 2007 die politische Einigung erzielt werden. Der JI-Rat bestätigte am 5. Juni 2008 diese politische Einigung. Am 8. November 2007 konnte im JI-Rat auch die politische Einigung zum Durchführungsbeschluss erzielt werden. Die formelle Annahme des Prüm-Beschlusses und des Prüm-Durchführungsbeschlusses

erfolgte am 23. Juni 2008 im Rat. Mit der am 6. August 2008 erfolgten Veröffentlichung im Amtsblatt wurden beide Rechtsakte wirksam. Der Beschluss ist nach Artikel 36 binnen einem Jahr von allen EU Staaten umzusetzen. Davon ausgenommen ist das Kapitel 2, welches zur Verbesserung des Informationsaustauschs die automatisierten Zugriffsrechte auf DNA-Analyse-Dateien, ihre automatisierten daktyloskopischen Identifizierungssysteme sowie die Fahrzeugzulassungsregister beinhaltet. Hier ist der Echtbetrieb binnen drei Jahren umzusetzen.

Im Verhältnis zum Prüm-Beschluss 2008/615/JI enthält der (Durchführungs-)Beschluss 2008/616/JI die notwendigen Maßnahmen zur technischen Umsetzung des Prüm-Beschlusses. Der Durchführungsbeschluss entspricht in seiner Substanz dem Durchführungsbeschluss des Prümer Vertrages. Aus redaktionellen Gründen sowie auf Grund unionsrechtlicher Vorgaben gibt es zwar Abweichungen; diese führen jedoch weder zu einer Änderung der bestehenden Prüm-Anwendung noch zu einer Erweiterung der Befugnisse der Strafverfolgungsbehörden oder Einschränkung von Rechten Betroffener.

Bei Daten aus den nationalen DNA-Analyse-Dateien und den nationalen automatisierten daktyloskopischen Identifizierungssystemen sollte ein Treffer/Kein-Treffer-System dem abfragenden Mitgliedstaat die Möglichkeit geben, in einem zweiten Schritt um spezifische dazugehörige personenbezogene Daten und gegebenenfalls um weitere Informationen im Verfahren der gegenseitigen Unterstützung zu ersuchen.

Das Treffer/Kein-Treffer-System bietet eine Struktur für den Abgleich anonymer Profile, bei der zusätzliche personenbezogene Daten nur nach einem Treffer ausgetauscht werden und Übermittlung wie Empfang dieser Daten dem einzelstaatlichen Recht, einschließlich der Bestimmungen über die Amts- und Rechtshilfe, unterliegen. Damit wird ein angemessenes Datenschutzsystem gewährleistet, wobei davon ausgegangen wird, dass die Übermittlung personenbezogener Daten an einen anderen Mitgliedstaat ein angemessenes Datenschutzniveau seitens der empfangenden Mitgliedstaaten voraussetzt.

Im Gegensatz zu anderen Beschlüssen war die Schaffung eigener Datenschutzregelungen im Zuge der Umsetzung des Prüm-Beschlusses nicht notwendig; die erforderlichen gesetzlichen Grundlagen finden sich bereits im DSG 2000, das nicht nur die gemeinschaftsrechtlichen Vorgaben der 1. Säule abdeckt, sondern auch für die sicherheits- und kriminalpolizeiliche Zusammenarbeit im Rahmen der 3. Säule anzuwenden ist.

- Weiters werden mit dem Prüm-Beschluss die unionsrechtlichen Voraussetzungen für einen europaweiten Einsatz von Organen von Sicherheitsbehörden geschaffen. Da Straftäter strafbare Handlungen oftmals nicht nur in ihren Herkunftsstaaten setzen, ist es für die europäischen Polizeibehörden notwendig, Polizeibeamte anderer Mitgliedstaaten zur Unterstützung der eigenen Polizei einzusetzen. Bislang war es österreichischen Polizisten in den EU-Mitgliedstaaten oder europäischen Polizisten in Österreich nur aufgrund bilateraler Regelungen möglich, mit polizeilichen Befugnissen ausgestattet zu werden.

Für eine effektive polizeiliche Zusammenarbeit auf europäischer Ebene ist es notwendig, Polizeibeamte anderer EU-Mitgliedstaaten mit den gleichen hoheitlichen Befugnissen auszustatten, wie sie auch Beamten des Staates, in dem die Unterstützung erfolgt, verfügen. Ihre Tätigkeiten sollten sich nicht auf die bloße Anwesenheit beschränken. Dies ist insbesondere bei bi- und multilateralen Streifen in Grenzgebieten, bei großangelegten Schwerpunktaktionen sowie Großveranstaltungen notwendig. Ohne diese Regelung könnten sich Beamte des Entsendestaates lediglich auf Basis von Hospitationen an derartigen Einsatzformen beteiligen, wodurch tatsächliche Unterstützung nicht geleistet werden kann. Die Notwendigkeit, Polizeibeamte anderer EU-Mitgliedstaaten mit den gleichen hoheitlichen Befugnissen auszustatten, hat sich insbesondere auch beim letzten Großereignis, nämlich der EURO 2008, gezeigt; soweit nicht in Staatsverträgen über die polizeiliche Zusammenarbeit derartige Regelungen enthalten waren, musste sich die Unterstützungsfunktion weitgehend auf Hospitationen beschränken.

Die Unterstützung muss sich aber nicht immer nur auf größere Einheiten beziehen, sondern kann auch einzelne Experten bzw. Expertenteams umfassen.

Die Ausübung von polizeilichen Befugnissen erfolgt grundsätzlich unter der Leitung von Beamten des Staates, in dem der Einsatz erfolgt. Damit wird sichergestellt, dass die Leitungsfunktion bei gemeinsamen Einsätzen, insbesondere bei größeren Einsatzformen, von einem sach- und ortskundigen Beamten erfolgt.

- Eine Sonderform der operativen Zusammenarbeit von Polizeieinheiten sieht der Beschluss 2008/617/JI des Rates vom 23. Juni 2008 über die Verbesserung der Zusammenarbeit zwischen den Spezialeinheiten der Mitgliedstaaten der Europäischen Union in Krisensituationen, Amtsblatt Nr. L 210 vom 6.8.2008, S. 73 – 75, vor.

Mit der Umsetzung dieses Beschlusses werden die rechtlichen Voraussetzungen für die Zusammenarbeit der Spezialeinheiten zur operativen Bekämpfung von Terrorlagen geschaffen. Nur wenige EU-Mitgliedstaaten können gewährleisten, dass sie genügend spezialisiertes Personal, die aktuellsten technischen Einsatzmittel oder die notwendige Ausrüstung zur Bewältigung von Krisensituationen insbesondere spezifischer terroristischer Gefahrensituationen, wie Massengeiselllagen in Gebäude und Transportmitteln, zur Verfügung haben.

Seit 2003 arbeiten die operativen Spezialeinheiten der EU-Mitgliedstaaten in der Kooperation „ATLAS“ unter der Leitung der „Task Force Chiefs of Police“ an Konzepten für die Bewältigung solcher außergewöhnlicher terroristischer Lagen. In der Arbeitsgruppe werden mit finanzieller Unterstützung der Europäischen Union Erfahrungen ausgetauscht, technische Einsatzmöglichkeiten weiterentwickelt, nach neuen Lösungsmöglichkeiten geforscht und die gemeinsame Bewältigung von solchen Einsatzlagen trainiert. Weiters wurde mit Unterstützung von Europol ein sicheres EDV-Kommunikationsnetzwerk mit einer integrierten Datenbank errichtet. Österreich ist in dieser europäischen Kooperation durch die Sondereinheit „Einsatzkommando Cobra“ vertreten. Für eine tatsächliche operative Unterstützung in einem anderen EU-Mitgliedstaat haben bisher aber die rechtlichen Grundlagen gefehlt.

Mit den vorgeschlagenen gesetzlichen Bestimmungen werden die rechtlichen Rahmenbedingungen für eine Unterstützungstätigkeit in einem anderen EU-Mitgliedstaat auf dessen Ersuchen (beispielsweise durch die Sondereinheit „Einsatzkommando Cobra“) und die Unterstützungsleistung von Spezialisten eines anderen EU-Mitgliedstaates in Österreich für die Anforderung, Unterstellung, die Befugnisse im Einsatzfall sowie die zivil- und strafrechtliche Haftung festgelegt. Der Schwerpunkt einer operativen Zusammenarbeit wird sich naturgemäß mit den Nachbarstaaten Österreichs ergeben, aber auch die Unterstützung durch Spezialisten aus anderen EU-Mitgliedstaaten ist dadurch ermöglicht.

Da die operativen Teile des Prüm-Beschlusses und der Beschluss über den Einsatz von Sondereinheiten jeweils bestimmte polizeilichen Einsatzformen zum Regelungsgegenstand haben, wird vorgeschlagen, die innerstaatlichen Umsetzungsbestimmungen gemeinsam in einem Teil zu regeln.

Schließlich enthält der Beschluss auch Regelungen über die Übermittlung von Informationen im Zuge von Großveranstaltungen und zur Verhinderung terroristischer Straftaten. Diese Informationsübermittlung kann bereits jetzt auf das PolKG gestützt werden, es bedarf daher keiner weiteren Normierung in diesem Gesetz.

3. Zum Beschluss 2008/633/JI des Rates vom 23. Juni 2008 über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten, Amtsblatt Nr. L 218 vom 13.8.2008, S. 129 - 136

Mit der Entscheidung 2004/512/EG des Rates vom 8. Juni 2004 zur Errichtung des Visa-Informationssystems (VIS) wurde das VIS als System für den Austausch von Visa-Daten zwischen Mitgliedstaaten geschaffen. Die Einrichtung des VIS stellt eine der wichtigsten Initiativen im Rahmen der Strategie der Europäischen Union zur Schaffung eines Raums der Freiheit, der Sicherheit und des Rechts dar. Ziel des VIS ist eine verbesserte Durchführung der gemeinsamen Visumpolitik. Das VIS soll ferner zur Steigerung der inneren Sicherheit und zur Bekämpfung des Terrorismus unter genau bestimmten und kontrollierten Umständen beitragen. Auf der Tagung vom 7. März 2005 nahm der Rat Schlussfolgerungen an, denen zufolge das „Ziel der Verbesserung der inneren Sicherheit und der Terrorismusbekämpfung nur dann uneingeschränkt erreicht werden kann, wenn sichergestellt wird, dass die für die innere Sicherheit zuständigen Behörden der Mitgliedstaaten bei der Ausübung ihrer Befugnisse im Bereich der Prävention von Straftaten sowie ihrer Aufdeckung und Ermittlung, einschließlich im Hinblick auf terroristische Handlungen und Bedrohungen, Zugang zur Abfrage des VIS haben“; dieser Zugang darf nur unter strikter Einhaltung der Vorschriften für den Schutz personenbezogener Daten erfolgen.

Durch den Beschluss 2008/633/JI des Rates vom 23. Juni 2008 wurde die Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung) insofern ergänzt, als er eine Rechtsgrundlage im Rahmen von Titel VI des Vertrages über die Europäische Union schafft, die den benannten Behörden und Europol den Zugang zum VIS gestattet.

Abfragen im VIS sind nur im Einzelfall und nur dann zulässig, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass diese Abfrage zu Informationen führt, die zur Verhütung schwerwiegender Straftaten sowie zu deren Aufdeckung und Ermittlung beitragen. Solch ein Einzelfall ist insbesondere dann gegeben, wenn die Abfrage mit einem besonderen Vorkommnis oder mit einer durch eine schwerwiegende Straftat hervorgerufenen Gefahr oder mit einer bestimmten Person oder mehreren bestimmten Personen in Verbindung steht, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass

sie terroristische Straftaten oder andere schwerwiegende Straftaten verübt hat bzw. haben oder verüben wird bzw. werden oder in entsprechender Verbindung zu einer solchen Person oder zu solchen Personen steht bzw. stehen.

4. Zum Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), Amtsblatt Nr. L 205 vom 7.8.2007, S. 63 - 84

Das Schengener Informationssystem (SIS), das gemäß den Bestimmungen von Titel IV des Übereinkommens vom 19. Juni 1990 zur Durchführung des Übereinkommens von Schengen vom 14. Juni 1985 (SDÜ) zwischen den Regierungen der Staaten der Benelux-Wirtschaftsunion, der Bundesrepublik Deutschland und der Französischen Republik betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen errichtet wurde, und seine Weiterentwicklung, das SIS 1+, stellen ein wichtiges Instrument für die Anwendung der Bestimmungen des in den Rahmen der Europäischen Union einbezogenen Schengen-Besitzstands dar. Im Jahr 2001 musste allerdings festgestellt werden, dass die Systemarchitektur des SIS nicht (mehr) in der Lage ist, notwendige weitere Funktionalitäten aufzunehmen und zusätzliche Mitgliedstaaten mit einzubeziehen. Aus diesem Grund wurde die Kommission mit der Entwicklung des SIS II (Schengener Informationssystems der zweiten Generation) betraut.

Dieses um neue Leistungsmerkmale ergänzte Schengener Informationssystem der zweiten Generation (SIS II) wird das mit dem SDÜ geschaffene SIS ersetzen. Zu den wichtigsten neuen Funktionalitäten zählen:

- die Erweiterung der Liste der Kategorien abhanden gekommener Sachen, die Gegenstand einer SIS-Ausschreibung sein können: Hinzugefügt werden Wasserfahrzeuge, Luftfahrzeuge, industrielle Ausrüstungen, Außenbordmotoren, Container, Wertpapiere und Zahlungsmittel wie Schecks, Kreditkarten, Obligationen, Aktien und Anteilspapiere;

- die Speicherung biometrischer Daten wie Fingerabdrücke und Fotografien im SIS zwecks rascherer Identifizierung gesuchter Personen;

- die Speicherung des Europäischen Haftbefehls im SIS sowie

- das Verknüpfen von Personen- und Sachenfahndungen (um beispielsweise einen Bezug zwischen einem flüchtigen Straftäter und dem von ihm verwendeten Fahrzeug herzustellen).

Das SIS II gründet sich auf zwei EU-Rechtsakte: In Bezug auf Angelegenheiten, die in den Anwendungsbereich des Vertrags zur Gründung der Europäischen Gemeinschaft fallen, also Ausschreibungen zur Einreise- und Aufenthaltsverweigerung („Angelegenheiten der ersten Säule der Europäischen Union“), bildet die Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 die erforderliche SIS II-Rechtsgrundlage. In Bezug auf Angelegenheiten, die in den Anwendungsbereich des Vertrags über die Europäische Union fallen, also alle sonstigen nachstehend angeführten Ausschreibungen (Angelegenheiten der dritten Säule der Europäischen Union), bildet der Beschluss 2007/533/JI des Rates vom 12. Juni die erforderliche SIS II-Rechtsgrundlage. Während die Verordnung (EG) nach Art. 249 EGV aber unmittelbar in jedem Mitgliedstaat gilt, bedarf es wie eingangs schon angeführt hinsichtlich des SIS II-Beschlusses einer innerstaatlichen, legistischen Umsetzung (Art. 34 Abs. 2 lit. c EUV). Auch wenn – auf Grund der unions- und gemeinschaftsrechtlichen Vorgaben aus dem EUV und dem EGV – verschiedene Rechtsgrundlagen für das SIS II erlassen werden mussten, stellt das SIS II ein einziges Informationssystem dar, das auch als solches zu betreiben ist. Einige Bestimmungen dieser Rechtsinstrumente sind daher identisch.

Das SIS II soll neben den der ersten Säule zuzurechnenden Ausschreibungen zur Einreise- oder Aufenthaltsverweigerung weiters Ausschreibungen von Personen zum Zwecke der Übergabe- oder Auslieferungshaft, von Abgängigen zu deren Schutz oder zur Gefahrenabwehr, von Personen, die im Rahmen eines Gerichtsverfahrens gesucht werden, von Personen und Sachen zum Zwecke der verdeckten Kontrolle sowie Ausschreibungen von Sachen zur Sicherstellung oder Beweissicherung in Strafverfahren enthalten.

Auch die Verarbeitung biometrischer Daten (insbesondere von Fingerabdrücken und Lichtbildern) zur rascheren Identifizierung von Personen soll möglich werden. Ebenso soll das SIS II die Verarbeitung von Daten über Personen ermöglichen, deren Identität missbraucht wurde, um den Betroffenen Unannehmlichkeiten aufgrund einer falschen Identifizierung zu ersparen.

Das SIS II soll auch die Möglichkeit bieten, Ausschreibungen im SIS II miteinander zu verknüpfen und einer Ausschreibung einen Vermerk (Kennzeichnung genannt) hinzuzufügen, um dadurch deutlich zu

machen, dass die Maßnahmen, um die mit der Ausschreibung ersucht wird, in ihrem Hoheitsgebiet nicht ergriffen werden können.

Daten, die im SIS II verarbeitet werden, sollen einem Drittstaat oder einer internationalen Organisation nicht übermittelt oder zur Verfügung gestellt werden. Trotzdem soll die Zusammenarbeit zwischen der Europäischen Union und Interpol verstärkt werden, indem ein effizienter Austausch von Passdaten gefördert wird. Werden personenbezogene Daten aus dem SIS II an Interpol weitergeleitet, so sollen diese personenbezogenen Daten einem angemessenen Schutz unterliegen, der durch ein Abkommen gewährleistet wird, das strenge Schutzmaßnahmen und Bedingungen festlegt.

Die Ausschreibungen sollen nicht länger als für den verfolgten Zweck erforderlich im SIS II gespeichert werden. Generell sollen Ausschreibungen von Personen nach drei Jahren automatisch aus dem SIS II gelöscht werden. Sachfahndungsausschreibungen zum Zwecke der verdeckten Kontrolle sollen nach fünf Jahren automatisch aus dem SIS II gelöscht werden. Sachfahndungsausschreibungen zur Sicherstellung oder Beweissicherung in Strafverfahren sollen nach zehn Jahren automatisch aus dem SIS II gelöscht werden. Die Entscheidungen, Personenausschreibungen länger zu speichern, sollen auf der Grundlage einer umfassenden individuellen Bewertung ergehen. Die Mitgliedstaaten sollen Ausschreibungen von Personen innerhalb dieses Dreijahreszeitraums überprüfen. Nationale Kontrollinstanzen sollen die Rechtmäßigkeit der Verarbeitung personenbezogener Daten und der Europäische Datenschutzbeauftragte, der mit dem Beschluss 2004/55/EG des Europäischen Parlaments und des Rates vom 22. Dezember 2003 über die Nominierung für das Amt der unabhängigen Kontrollbehörde gemäß Artikel 286 des EG-Vertrags ernannt wurde, soll die Tätigkeiten der Organe und Einrichtungen der Gemeinschaft in Bezug auf die Verarbeitung personenbezogener Daten im Hinblick auf die eingeschränkten Aufgaben der Organe und Einrichtungen der Gemeinschaft in Bezug auf die Daten selbst kontrollieren.

In technischer Hinsicht besteht das SIS II aus einem zentralen System und einem nationalen, mit dem zentralen SIS II kommunizierenden System in jedem einzelnen Mitgliedstaat. Das zentrale System setzt sich aus einer technischen Unterstützungseinheit und einer einheitlichen nationalen Schnittstelle zusammen. Die technische Unterstützungseinheit des zentralen Systems ist in Straßburg (Frankreich) und eine Backup-Einheit in Sankt Johann im Pongau (Österreich) eingerichtet. Das Verfahren zur Migration der SIS 1+ Daten in das SIS II ist im Beschluss 2008/839/JI des Rates vom 24. Oktober 2008 geregelt.

Auf Grund zahlreicher technischer Probleme verzögerte sich die Inbetriebnahme bereits mehrfach. Seit dem Jahr 2008 befindet sich das SIS I+ (Renewal) in Betrieb, dessen Hardware laufend weiterentwickelt wird und das – nach derzeitigem Informationsstand – Mitte 2010 in der Lage sein soll, alle an das SIS II gestellten Anforderungen zu erfüllen.

Finanzielle Auswirkungen:

Zu Artikel 1 und 2:

1. Beschluss des Rates vom 6. April 2009 zur Errichtung des Europäischen Polizeiamts (Europol), Amtsblatt L121/2009, S. 37 - 66

Aus der Einrichtung weiterer Arbeitsdateien ist ein erhöhter administrativer Aufwand zu erwarten. Dafür bedarf es eines Arbeitsplatzes der Wertigkeit A3/v3, Funktionsgruppe 4. Unter Zugrundelegung einer Kalkulation eines v3-Arbeitsplatzes nach den Bestimmungen des § 14 Abs. 5 BHG entsprechend der VO des BMF ergibt sich somit ein jährlicher Mehrbedarf an Personal- und Querschnittsausgaben einschließlich der Ausgaben für Büroräumlichkeiten von rund € 49.300,--.

2. Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, Amtsblatt Nr. L 210 vom 6.8.2008, S. 1 -11, Beschluss 2008/616/JI des Rates vom 23. Juni 2008 zur Durchführung des Beschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, Amtsblatt Nr. L 210 vom 6.8.2008, S. 12 – 72, sowie Beschluss 2008/617/JI des Rates vom 23. Juni 2008 über die Verbesserung der Zusammenarbeit zwischen den Spezialeinheiten der Mitgliedstaaten der Europäischen Union in Krisensituationen, Amtsblatt Nr. L 210 vom 6.8.2008, S. 73 - 75

- Zum automatisierten Vergleich von DNA-Profilen, dem automatisierten Abruf von daktyloskopischen Daten aus der zentralen erkennungsdienstlichen Evidenz (§ 75 SPG) sowie dem automatisierten Abruf von Daten aus der zentralen Zulassungsevidenz :

Die technische Umsetzung wird in den kommenden Budgetjahren Ausgaben in der Höhe von rund € 4 Mio. verursachen. Daneben ist eine Unterstützungsleistung durch Österreich für andere Staaten (z. B. für internationale Softwareteile) geplant, was jährliche Ausgaben in der Höhe von € 1.780.000,--

verursachen wird. Der vorgenannte Betrag wird durch die EU mit € 1.250.000,-- gefördert; wodurch sich eine Belastung des Budgets für das Bundesministerium für Inneres in Höhe von € 530.000,-- ergibt.

In personeller Hinsicht ist mit einem Mehrbedarf von 5 VBÄ (1x E2a/6, 1x E2a/4, 3x E2a/3) für die Aufgabenerledigung auszugehen. Unter Zugrundelegung der aktuellen Kennzahlen und unter Anwendung der Bestimmungen der Verordnung des BMF betreffend die Ermittlung und Darstellung von finanziellen Auswirkungen neuer rechtsetzender Maßnahmen ergibt sich für diese Bediensteten ein jährlicher Mehrbedarf von ~ € 363.000,-- für das ho. Ressort.

- Zu den weiteren Formen polizeilicher Zusammenarbeit:

Derzeit werden nach Art. 24 des Prümer Vertrages nur wenige Schwerpunktaktionen oder gemischte Streifen durchgeführt. Durch die Umsetzung der aktuellen Vorgaben ist mit einer Vermehrung solch gemeinsamer Aktivitäten zu rechnen; dies insbesondere deshalb, weil nunmehr auch mit Mitgliedstaaten, mit denen bislang kein gemeinsames Abkommen bestanden hat, ein kooperatives Vorgehen ermöglicht wird. Eine Schätzung des dadurch zu erwartenden Mehraufwandes kann in Ermangelung unbekannter Häufigkeit und Dauer nicht durchgeführt werden.

Hinsichtlich des Einsatzes von Sondereinheiten wird es zu keinen budgetären Auswirkungen kommen, da bereits jetzt Schulungen und Veranstaltungen abgehalten werden, wie sie im Beschluss vorgesehen sind. Allenfalls durch andere Ereignisse hervorgerufene Kosten (z.B. anlassbezogene Personenschutzdienste), die Überstunden bedingen, können hier nicht eingerechnet bzw. berücksichtigt werden.

3. Beschluss 2008/633/JI des Rates vom 23. Juni 2008 über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten, Amtsblatt Nr. L 218 vom 13.8.2008, S. 129 - 136

Durch die Beschränkung der Zulässigkeit von Abfragen in besonders zu begründenden Fällen für kriminalpolizeiliche Zwecke ist nicht von Massenanfragen auszugehen. In den nächsten drei Jahren wird mit einer Maillösung das Auslangen gefunden (ein eigenständiger Workflow ist nicht beabsichtigt), die keine weiteren Personal- und Sachaufwendungen annehmen lässt.

4. Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), Amtsblatt Nr. L 205 vom 7.8.2007, S. 63 - 84

Für die Betriebsführung des Schengener Informationssystems der zweiten Generation wird mit jährlichen Mehrausgaben für Technik und Infrastruktur Kosten in der Höhe von ca. € 100.000.- zu rechnen sein. Daneben ist mit geringen Mehrausgaben für zusätzliche Personalleistungen zu rechnen. Diese sind allerdings wegen des unbekannten Bedarfes (VBÄ) und deren Wertigkeit weder kalkulier- noch schätzbar.

Zu Artikel 3:

Durch die im § 58b Abs. 1 und 4 SPG geschaffene Möglichkeit der Anfertigung und Speicherung von Lichtbildern bei der Aufnahme bzw. der Verpflichtung der Löschung von Lichtbildern bei der Entlassung von Personen sind infolge der bereits vorhandenen technischen Ausstattung der betroffenen Organisationseinheiten keine zusätzlichen Sachausgaben notwendig. Für den in diesem Zusammenhang notwendigen zusätzlichen Zeitbedarf sind jährliche Mehrausgaben für das Bundesministerium für Inneres in der Höhe von ~ € 14.000,-- (0,23 VBÄ E2b) zu erwarten.

Durch die Aufgabenerweiterung des Rechtsschutzbeauftragten in § 91c Abs. 1 SPG können derzeit nicht bezifferbare Mehrausgaben für die Entschädigung des Rechtsschutzbeauftragten entstehen. Auf Grund der erforderlichen zusätzlichen Meldungen an den Rechtsschutzbeauftragten wird im Bereich der Sicherheitsbehörden mit einem nicht unerheblichen Mehraufwand zu rechnen sein.

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Gesetzgebung stützt sich hinsichtlich der sicherheitspolizeilichen Aspekte der Gefahrenabwehr, des vorbeugenden Rechtsgutschutzes, der Fahndung und der ersten allgemeinen Hilfeleistung auf Artikel 10 Absatz 1 Ziffer 7 B-VG (Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit), hinsichtlich der Strafverfolgungsbereiche auf Artikel 10 Absatz 1 Ziffer 6 B-VG (Strafrechtswesen). Die Haftungsbestimmungen fallen unter den Kompetenztatbestand des Artikels 10 Absatz 1 Ziffer 6 B-VG (Zivilrechtswesen). Die Regelungen hinsichtlich des automatisierten Abrufs von Daten aus dem Fahrzeugregister sind Artikel 10 Absatz 1 Ziffer 9 B-VG (Kraftfahrwesen) zuzurechnen.

Besonderer Teil

Zu Art. 1

1. Teil Allgemeines

Zu § 1 (Anwendungsbereich)

Der vorliegende Entwurf regelt die unterschiedlichen Formen der Zusammenarbeit der Sicherheitsbehörden mit den Mitgliedstaaten der Europäischen Union sowie mit dem Europäischen Polizeiamt (Europol), wie sie in den entsprechenden angeführten Beschlüssen vorgesehen sind.

Soweit allerdings die Vorgaben aus den Beschlüssen schon jetzt auf geltendes Recht gestützt werden können, sollen weiterhin ausschließlich diese Normen gelten. Das soll mit der Aufzählung in Abs. 2 klar gestellt werden. Insbesondere wird auch klargestellt, dass die justizielle Zusammenarbeit nach dem Bundesgesetz über die justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union (EU-JZG), BGBl. I Nr. 36/2004, nach dem Auslieferungs- und Rechtshilfegesetz (ARHG), BGBl. Nr. 529/1979 oder nach zwischenstaatlichen Vereinbarungen unberührt bleibt.

Zu § 2 (Begriffsbestimmungen)

Mit Mitgliedstaaten sind jene Staaten gemeint, die Vertragspartei des Vertrages über die Europäische Union sind; soweit aber seitens der Europäischen Union nach dem Titel IV des Vertrages über die Europäische Union Übereinkünfte mit Drittstaaten oder mit internationalen Organisationen abgeschlossen werden, sind diese im Rahmen der jeweiligen Übereinkünfte den Mitgliedstaaten gleichzuhalten (Art. 24 und 38 EUV). Die Einbeziehung weiterer Staaten ist notwendig, da sich in einzelnen Bereichen auch europäische Staaten, die nicht Vertragspartei der Europäischen Union sind, an der polizeilichen Zusammenarbeit beteiligen, so insbesondere beim Schengener Informationssystem. Die teilnehmenden Drittstaaten sind allerdings den Mitgliedstaaten nur insoweit gleichzuhalten, als mit diesen Übereinkünfte (Art. 24 und 38 EUV) geschlossen wurden und nur im Rahmen dieser jeweiligen Übereinkünfte.

Zu § 3 (Haftung)

Die in den Beschlüssen enthaltenen Schadenersatzregelungen weichen teilweise voneinander ab. Dem entsprechend ist auch bei den Haftungsregelungen zu differenzieren:

Abs. 1 regelt die Haftung im Rahmen der Zusammenarbeit mit dem Europäischen Polizeiamt (Europol). Demnach haftet der Bund nach den Bestimmungen des Amtshaftungsgesetzes mit der Maßgabe, dass in jedem Fall das Landesgericht für Zivilrechtssachen Wien zuständig ist. Wien soll deshalb Gerichtsstand sein, da die Nationale Europol-Stelle, über die sämtliche Datenverarbeitung und Übermittlung zu Europol zu laufen hat, beim Bundeskriminalamt in Wien angesiedelt ist.

Außerdem soll klargestellt werden, dass der Bund seinerseits Regress zu nehmen hat, wenn durch Organe von Europol oder eines anderen Mitgliedstaates in Österreich ein Schaden verursacht wurde.

Die Regelung in Abs. 1 beschränkt sich auf die Haftung für Fälle unrichtiger oder unrechtmäßiger Datenverwendung. Soweit Organe des öffentlichen Sicherheitsdienstes etwa in gemeinsamen Ermittlungsgruppen mitwirken, kommen die Haftungsregelungen des PolKG oder gegebenenfalls des EU-JZG zum Tragen.

Abs. 2 regelt die Haftung bei operativen Polizeieinsätzen. Demnach hat der Bund einem Mitgliedstaat auf dessen Verlangen jenen Betrag zu erstatten, den dieser entsprechend seiner Rechtslage an die Geschädigten zu leisten hatte, wenn österreichische Organe des öffentlichen Sicherheitsdienstes in diesem Mitgliedstaat einen Schaden verursacht haben.

Verursachen dagegen Organe von Sicherheitsbehörden anderer Mitgliedsstaaten in Österreich einen Schaden und hat der Bund Schadenersatz nach dem Amtshaftungsgesetz zu leisten, hat der Bund diesen Betrag von jenem Mitgliedstaat einzufordern, dessen Organe den Schaden verursacht haben; dies gilt nicht für vom Bund ersetzte Schäden, die das Organ bei seinem Einsatz bei Massenveranstaltungen, Katastrophen und schweren Unglücksfällen verursacht hat. Mit diesem Verzicht wird Art. 21 Abs. 6 des Beschlusses 2008/615/JI, ABl. L210/2009, entsprochen.

Wenn allerdings ein Schaden im Rahmen von Hilfeleistungen bei Massenveranstaltungen, Katastrophen und schweren Unglücksfällen verursacht wird, soll auf Regressnahmen verzichtet werden.

Abs. 3 regelt ähnlich wie Abs. 1 die Haftung des Bundes nach dem Amtshaftungsgesetz, wenn jemandem durch die (rechtswidrige und schuldhafte) Verwendung von Daten im Schengener Informationssystem ein Schaden entstanden ist. Da Eingaben und Abrufe im Schengener Informationssystem aber nicht alleine durch eine nationale Stelle erfolgen, sondern auch durch die Sicherheitsbehörden, bedarf es keiner

eigenen Regelung über den Gerichtsstand für Schadenersatzverfahren. Mit „dem Bund zuzurechnende Schadenzufügungen“ ist insbesondere gemeint, wenn der Schaden durch dem Bund zuzurechende Organe verursacht wurde. Aus der Haftung für Schäden nach den Bestimmungen des AHG ergibt sich, dass der Geschädigte das Organ nicht unmittelbar in Anspruch nehmen kann.

Zu § 4 (Verhältnis zu anderen Rechtsakten)

Die Abs. 1 regelt das Verhältnis zum Prümer Vertrag. Soweit sich Regelungen sowohl im Prümer Vertrag als auch im Prüm-Beschluss finden, soll künftig ausschließlich dieses Bundesgesetz maßgeblich sein. Gegenüber den Vertragsparteien des Prümer Vertrages sind dann also nur mehr die hier innerstaatlich umzusetzenden Bestimmungen des Prüm-Beschlusses anzuwenden.

Die Bestimmungen dieses Bundesgesetzes sind aber erst dann anstelle der entsprechenden Bestimmungen des Prümer Vertrag anzuwenden, wenn die einzelnen Vertragsstaaten ihren Verpflichtungen aus dem Prüm-Beschluss, insbesondere in technischer und rechtlicher Hinsicht, nachgekommen sind. Bis dahin ist gegenüber den Vertragsparteien weiterhin der Prümer Vertrag anzuwenden. Die Übergangsbestimmungen sollen hier Klarheit schaffen.

Die übrigen Bestimmungen des Prümer Vertrages, die davon nicht berührt werden, sind insbesondere die Regelungen über Flugsicherheitsbegleiter (Art. 18ff), Dokumentenberater (Art. 20ff) und Unterstützung bei Rückführungen (Art. 23) gemeint.

Der hier umzusetzende Europol-Beschluss ersetzt die bisherige Rechtsgrundlage für Europol, nämlich das Übereinkommen auf Grund von Art. K.3 des Vertrags über die Europäische Union über die Errichtung eines Europäischen Polizeiamts (Europol-Übereinkommen), BGBl. III Nr. 123/1998 (Abs. 2). Der Beschluss sieht auch vor, dass das Protokoll auf Grund von Artikel K.3 des Vertrages über die Europäische Union und von Artikel 41 Absatz 3 des Europol-Übereinkommens über die Vorrechte und Immunitäten für Europol, die Mitglieder der Organe, die stellvertretenden Direktoren und die Bediensteten von Europol, BGBl. III Nr. 131/1999, zuletzt geändert durch BGBl. III Nr. 120/2007, nicht mehr anzuwenden ist und stattdessen das Protokoll über die Vorrechte und Befreiungen der Europäischen Gemeinschaften, BGBl. III Nr. 24/2000, gelten soll. Art. 64 des Europol-Beschlusses sieht als Inkrafttretenszeitpunkt entweder den 1.1.2010 oder jenen Zeitpunkt vor, ab dem die gemäß Art. 51 Abs. 1 zu erlassende Verordnung gilt; je nachdem, welcher dieser Zeitpunkt später liegt. Diese Verordnung (EG) Nr. 371/2009 wurde mit ABl. L121 vom 15.5.2009, S. 1-2, kundgemacht und tritt mit 1.1.2010 in Kraft. Demnach war als Inkrafttreten der 1.1.2010 vorzusehen.

Auch die Bestimmungen zum Schengener Informationssystem im SDÜ werden durch die Regelungen dieses Bundesgesetzes ersetzt; allerdings erst mit dem Zeitpunkt, der vom Rat mit Zustimmung aller Mitglieder, die die Regierungen der am SIS 1+ teilnehmenden Staaten vertreten, festgelegt wird. Erst mit diesem Zeitpunkt werden die Artikel 64 und 92 bis 119 des Schengener Übereinkommens mit Ausnahme der Artikel 92a und 102a dieses Übereinkommens durch die Bestimmungen dieses Bundesgesetzes ersetzt. Aus Gründen der Rechtssicherheit wird vorgeschlagen, dass der Bundesminister für Inneres diesen Zeitpunkt im Bundesgesetzblatt kundzumachen hat (Abs. 3).

2. Teil Europol

Zu § 5 (Zusammenarbeit mit Europol)

Eine Zusammenarbeit der nationalen Europol-Stellen in den Mitgliedstaaten mit dem Europäischen Polizeiamt (Europol) bezieht sich auf die Vorbeugung und Bekämpfung von Straftaten im Bereich organisierter Kriminalität, Terrorismus sowie anderer Formen schwerer Kriminalität gemäß dem Anhang zum PolKG, sofern zwei oder mehr Mitgliedstaaten betroffen sind. Derzeit regeln die Art. 2 und 3 des Europol-Übereinkommens die Ziele und Aufgaben von Europol in ähnlicher Weise. Ein solcher Fall liegt beispielsweise vor, wenn EURO-Scheine gefälscht werden.

Europol wird für die Prävention und Bekämpfung von Schwerkriminalität einschließlich organisierter Kriminalität und Terrorismus sowie anderer Kriminalitätsformen, die im Annex des Beschlusses und als Anlage zu diesem Gesetz angeführt sind, zuständig, wenn zwei oder mehrere Mitgliedstaaten in einer Weise betroffen sind, die gemeinsames Handeln erfordert. Damit entfällt der Nachweis, dass tatsächliche Anhaltspunkte für eine kriminelle Organisationsstruktur vorliegen müssen.

Abs. 2 erweitert den Zuständigkeitsbereich von Europol noch dahingehend, als sich die Kooperation mit Europol auch auf Straftaten erstreckt, die mit den in Abs. 1 genannten in Zusammenhang stehen und begangen werden, um die Mittel zur Begehung von in den Zuständigkeitsbereich von Europol fallenden Handlungen zu beschaffen, weiters um Handlungen zu erleichtern oder durchzuführen, die in den Zuständigkeitsbereich von Europol fallen, oder um sicherzustellen, dass in den Zuständigkeitsbereich von Europol fallende Handlungen straflos bleiben.

Zu § 6 (Nationale Europol-Stelle)

Nach Art. 8 des Europol-Beschlusses hat jeder Mitgliedstaat eine nationale Stelle zu benennen. Diese ist die Verbindungsstelle der Mitgliedstaaten zu Europol, über sie hat die Zusammenarbeit mit Europol zu laufen. Ähnlich regelt derzeit Art. 4 des Europol-Übereinkommens die Funktion der Nationalen Europol-Stelle.

Gemäß § 4 Abs. 1 Bundeskriminalamt-Gesetz (BKA-G) nimmt das Bundeskriminalamt die damit in Zusammenhang stehenden Aufgaben für den Bundesminister für Inneres wahr.

Im Zuständigkeitsbereich des Bundesamtes zur Korruptionsprävention und Korruptionsbekämpfung fungiert dieses gemäß § 4 Abs. 2 des Bundesgesetzes über die Einrichtung und Organisation des Bundesamts zur Korruptionsprävention und Korruptionsbekämpfung als zentrale Ansprechstelle.

Abs. 2 nennt in einer demonstrativen Aufzählung die wichtigsten Aufgaben der Nationalen Europol-Stelle. So obliegt ihr insbesondere, Europol aus eigener Initiative Informationen und Erkenntnisse, die Europol für die Durchführung seiner Aufgaben benötigt, zu übermitteln, Informations-, Erkenntnis- und Beratungsanfragen von Europol zu beantworten, Informationen und Erkenntnisse auf dem aktuellen Stand zu halten, Informationen und Erkenntnisse für die Sicherheitsbehörden auszuwerten und an diese weiterzuleiten, Beratungs-, Informations-, Erkenntnis- und Analyseanfragen an Europol zu richten sowie Informationen für die Speicherung in seinen Datenbanken an Europol zu übermitteln und die Rechtmäßigkeit des Informationsaustauschs mit Europol zu gewährleisten.

Wenn andere Sicherheitsbehörden als die Nationale Europol-Stelle Abfragen aus dem Europol-Informationssystem durchführen, darf aus dem Abfrageergebnis nur ersichtlich sein, ob ein angefragter Datensatz im Europol-Informationssystem verfügbar ist oder nicht. Weitere Informationen sind ausschließlich über die Nationale Europol-Stelle einzuholen. Eingaben in das Europol-Informationssystem haben dagegen ausnahmslos durch die Nationale Europol-Stelle zu erfolgen (Abs. 3).

Nach Abs. 4 bedarf die Weitergabe von Daten an Einrichtungen der Europäischen Union, Drittstaaten und Drittorganisationen (z.B. INTERPOL) der Zustimmung der Nationalen Europol-Stelle (Art. 24 des Beschlusses, Art. 18 des Übereinkommens). Auf Grund der schon derzeit laufenden, intensiven Zusammenarbeit mit Europol erscheint es vertretbar, dass diese Zustimmung nicht in jedem Einzelfall, sondern allgemein oder beschränkt auf bestimmte Fachbereiche oder Organisationen oder Mitgliedstaaten erteilt werden kann. Die Zustimmung kann jederzeit widerrufen werden. Die Verwendung kann auch an die Einhaltung bestimmter Auflagen (§ 8 Abs. 1 PolKG) gebunden werden. Bei Vorliegen der in § 8 Abs. 2 PolKG vorliegenden Gründe ist die Zustimmung zu verweigern.

Zu § 7 (Entsendung von Verbindungsbeamten zu Europol)

Nach Art. 9 des Europol-Beschlusses (Art. 5 des Europol-Übereinkommens) hat jeder Mitgliedstaat mindestens einen Verbindungsbeamten zu Europol zu entsenden. Diese haben im Rahmen ihrer Aufgabenstellung die Interessen Österreichs bei Europol zu vertreten und unterliegen als weisungsgebundene Organe den Aufträgen der Nationalen Europol-Stelle.

Die nach den dienstrechtlichen Vorschriften (§ 39 BDG, § 6b VBG) entsandten Verbindungsbeamten sollen den Informationsfluss zwischen der Nationalen Europol-Stelle und Europol gewährleisten und mit den Bediensteten von Europol entsprechend zusammenarbeiten. Die Verbindungsbeamten haben, soweit dies zur Aufgabenerfüllung erforderlich ist, Zugriff auf Informationen aus den verschiedenen Dateien bei Europol.

Zu § 8 (Ersuchen von Europol um Einleitung strafrechtlicher Ermittlungen)

Nach Art. 7 des Beschlusses (Art. 3b des Europol-Übereinkommens) hat die Nationale Europol-Stelle Ersuchen von Europol um Einleitung, Durchführung oder Koordinierung von Ermittlungen entgegen zu nehmen, zu prüfen, erforderlichenfalls an die zuständigen Stellen weiterzuleiten und Europol darüber zu informieren, ob die Ermittlungen, die Gegenstand des Ersuchens sind, eingeleitet werden. Langen Ersuchen von Europol bei nachgeordneten Sicherheitsbehörden ein, haben diese die Anfrage unverzüglich der Nationalen Europol-Stelle vorzulegen.

Kann einem Ersuchen von Europol nicht entsprochen werden, so ist Europol von dieser Entscheidung unter Darlegung der maßgeblichen Gründe in Kenntnis zu setzen. Die Begründung kann entfallen, wenn wesentliche nationale Sicherheitsinteressen oder der Erfolg laufender Ermittlungen oder die Sicherheit von Personen dadurch gefährdet würden. Die entsprechenden Antworten werden gemäß den einschlägigen innerstaatlichen Rechtsvorschriften durch die Nationale Europol-Stelle (Bundesministerium für Inneres – Bundeskriminalamt) übermittelt.

Zu § 9 (Europol-Informationssystem)

Europol betreibt schon derzeit gemäß Art. 7 bis 9 des Europol-Übereinkommens (nunmehr Art. 11 bis 13 des Europol Beschlusses) ein Informationssystem, in das die Nationalen Stellen, die Verbindungsbeamten und - bei Daten von Drittstaaten und Analysedaten - Europol selbst Daten eingeben.

In das Europol-Informationssystem dürfen ausschließlich die in Abs. 1 und 2 angeführt Datenkategorien und nur zur Vorbeugung und Bekämpfung von Straftaten im Bereich organisierter Kriminalität, Terrorismus sowie anderen Formen schwerer Kriminalität gemäß **Anhang 1** eingegeben werden, für die Europol zuständig ist.

Auf die in diesem System gespeicherten Daten haben grundsätzlich nur die Nationalen Stellen, die Verbindungsbeamten, der Direktor und die stellvertretenden Direktoren sowie die dazu ermächtigten Europol-Bediensteten unmittelbaren Zugriff. Die Verantwortung für die Einhaltung der Bestimmungen über die Zusammenarbeit und für die Führung des Informationssystems liegt ebenso wie für die technische und betriebliche Sicherheit des Systems bei Europol. Weiters trifft Europol die für die Beachtung der Speicherungs- und Löschungsfristen sowie für die Datensicherheit erforderlichen Maßnahmen.

Der Abruf von Daten ist aus der Sicht einer österreichischen Sicherheitsbehörde eine Datenermittlung, deren Zulässigkeit nach nationalen Vorschriften, insbesondere nach § 53 Abs. 1 SPG, zu beurteilen ist. Schon aus dem Verhältnismäßigkeitsprinzip folgt, dass eine solche Ermittlung nur dann zulässig ist, wenn sie im Einzelfall zur Aufgabenerfüllung erforderlich ist.

Verdächtig ist jemand, sobald Kriminalpolizei oder Staatsanwaltschaft gegen eine bekannte Person ermitteln oder Zwang ausüben (§ 1 Abs. 2 StPO).

Tatmittel (Abs. 2) sind beispielsweise Tatwerkzeuge, der Begriff Eingabestelle bezeichnet jene Stelle, die das Formular ausfüllt, auf deren Basis die Eingabe durch die Nationale Europol-Stelle erfolgt. Solche Daten dürfen auch dann eingegeben werden, wenn noch kein Bezug zu bestimmten Personen gegeben ist.

Nach Abs. 3 haben die Nationale Europol-Stelle sowie die Verbindungsbeamten Änderungen, Richtigstellungen und Löschungen von Daten ausschließlich hinsichtlich jener Daten durchzuführen, die von ihnen eingegeben worden sind. Dem Beschluss entsprechend sind Richtigstellungen und Löschungen im Europol-Informationssystem generell nur durch jene Stelle durchzuführen, die die Daten eingegeben hat.

Bei Vorliegen von Hinweisen, wonach von anderen nationalen Kontaktstellen eingegebene Daten unrichtig, unvollständig oder unrechtmäßig verarbeitet wurden, haben die Nationale Europol-Stelle und die Verbindungsbeamten unverzüglich jene Stelle darüber zu informieren, die die Daten eingegeben hat (Abs. 4). Keinesfalls hat sie die Richtigstellungen oder Löschungen selbst durchzuführen.

Die Regelungen der Abs. 3 und 4 folgen dem Grundprinzip, dass die Verantwortung hinsichtlich der Veränderung, Richtigstellung oder Löschung von Daten denjenigen trifft, der die Daten eingegeben hat. Dahinter steht die Erwägung, dass regelmäßig nur diese Stelle die Richtigkeit und Rechtmäßigkeit der ursprünglichen Dateneingabe beurteilen kann. Allerdings haben andere Stellen, die zur Auffassung gelangen, dass eingegebene Daten unrichtig sind, die Pflicht, dies der für die eingegebenen Daten verantwortlichen Stelle mitzuteilen. Damit soll eine bestmögliche Datenrichtigkeit gewährleistet werden.

Was die Ergänzung von Datensätzen nach Abs. 5 anlangt, so ist das vorgesehene Verfahren davon abhängig, ob es sich um Daten nach Abs. 1 oder Abs. 2 handelt. Die erstgenannte Datenkategorie kann ausschließlich von jener Stelle ergänzt werden, die die ursprünglichen Daten eingegeben hat. Hingegen können Daten der zweiten Gruppe auch von anderen Stellen ergänzend eingegeben werden. Sind daher im Europol-Informationssystem bereits Daten gemäß Abs. 2 zu einer Person gespeichert, so steht dies der Eingabe weiterer Daten nach Abs. 2 nicht entgegen; stehen allerdings die einzugebenden Daten in Widerspruch zu den bereits eingegebenen Daten, hat sich die Nationale Europol-Stelle mit jener Stelle, die solche Daten bereits eingegeben hat, hinsichtlich der weiteren Vorgangsweise abzustimmen. Der Beschluss sieht keine Verfahrensweisen für den Fall vor, dass keine Einigung über die Richtigkeit der Daten erzielt werden kann. Dieser Umstand wird allerdings dadurch relativiert, als die Letztverantwortung bei der ursprünglich eingebenden Stelle liegt.

Zu einem Übergang der Datenverantwortlichkeit kann es jedoch dadurch kommen, dass jene Stelle, die den Datensatz ursprünglich eingegeben hat, diesen nunmehr aus dem Informationssystem löschen will. Wenn nun eine andere Stelle diesen Datensatz um Daten nach Abs. 2 ergänzt hat, so können die Identitätsangaben nach Abs. 1 weiter gespeichert bleiben; die Verantwortung für Richtigkeit und Rechtmäßigkeit des gesamten Datensatzes geht allerdings auf die Stelle über, die als nächste eine Ergänzung des Datensatzes vorgenommen hat (Abs. 6).

Zu § 10 (Arbeitsdateien zu Analysezwecken)

Die Arbeitsdateien zu Analysezwecken von Europol (Art. 14 bis 16 des Beschlusses) finden sich bereits in den Art. 10 bis 12 des Europol-Übereinkommens und stellen für Europol ein unverzichtbares Mittel dar.

Welche Daten an Europol übermittelt werden dürfen, richtet sich nach jenen Bestimmungen, wie sie für die Verarbeitung von Daten zum Zwecke der Verhütung, Analyse oder Bekämpfung von Straftaten gelten (Art. 14 Abs. 3 des Beschlusses). Daran anknüpfend dürfen die Sicherheitsbehörden nur solche Daten übermitteln, die sie nach § 53a SPG („Datenanwendungen der Sicherheitsbehörden“) verarbeiten dürfen.

Während eines laufenden Analyseprojekts haben nur jene Personen Zugang zu den verarbeiteten Daten, die am Analyseprojekt teilnehmen: das sind außer den Analytikern und sonstigen Bediensteten von Europol Verbindungsbeamte und Sachverständige der unmittelbar von der Analyse betroffenen Mitgliedstaaten oder von Mitgliedstaaten, von denen die Informationen stammen. Die anderen Mitgliedstaaten erfahren jedoch über ein von Europol eingerichtetes Indexsystem vom Analyseprojekt. Nach Abschluss des Analyseprojekts werden im Falle von allgemeinen und strategischen Analysen alle Mitgliedstaaten in vollem Umfang von den Ergebnissen der Arbeit in Kenntnis gesetzt. Handelt es sich hingegen um eine operative Analyse zu Einzelfällen, die nicht alle Mitgliedstaaten betreffen, so werden nur die am Analyseprojekt beteiligten und die von ihm betroffenen Mitgliedstaaten von seinem Ergebnis informiert. Es ist die Aufgabe von Europol, sich um die Gewinnung von Informationen aus Drittstaaten und Organisationen zu bemühen, soweit solche Daten zu Analysen benötigt werden.

Nach Abs. 2 ist die Übermittlung sensibler Daten (§ 4 Z 2 DSG 2000) nur zulässig, wenn sie für die Analysetätigkeit unbedingt notwendig sind. Eine derartige Notwendigkeit ergibt sich etwa hinsichtlich von Daten zum Sexualleben schon daraus, dass Europol auch für bestimmte Sexualstraftaten zuständig ist, insbesondere im Zusammenhang mit Menschenhandel.

Abs. 3 sieht die Möglichkeit vor, Daten unter Auflagen nach § 8 Abs. 3 PolKG zu übermitteln. Erhält im umgekehrten Fall die Nationale Europol-Stelle Daten unter Auflagen übermittelt, ist sie an diese gebunden. Sie hat aber die Möglichkeit, die übermittelnde Stelle zu ersuchen, die Daten auch für andere Zwecke zu verwenden, sofern sie dazu gesetzlich ermächtigt ist. Die Festlegung von Auflagen erfolgt mittels so genannter „handling codes“ von Europol.

Zu § 11 (Verwendung von Daten aus Europol Datenverarbeitungssystemen durch Sicherheitsbehörden)

Von wenigen möglichen Ausnahmen abgesehen ist die Nationale Europol-Stelle die einzige Kontaktstelle zu Europol. Über sie erfolgen die Eingabe und der Abruf von Daten aus dem Europol-Informationssystem sowie die Übermittlung von Daten an das Europol Analysesystem und an die sonstigen Datenverarbeitungssysteme von Europol. Diese über die Nationale Europol-Stelle eingeholten Informationen sollen aber in erster Linie den Sicherheitsbehörden zukommen. Mit dieser Bestimmung soll daher klargestellt werden, dass die Sicherheitsbehörden diese Daten verwenden dürfen.

Abs. 2 und 3 stellen weiters klar, dass auch die Sicherheitsbehörden allfällige Auflagen zu beachten oder sich um die Zustimmung der übermittelnden Stelle zu bemühen haben, um die Daten auch für andere Zwecke als jene, zu denen sie übermittelt wurden, verwenden zu dürfen, sofern sie dazu gesetzlich ermächtigt sind.

Zu § 12 (Speicher- und Löschungsfristen)

Nach Ablauf von drei Jahren soll jedenfalls geprüft werden, ob eine gespeicherte Information weiterhin zur Aufgabenerfüllung notwendig ist. Für Daten im Europol-Informationssystem erfolgt diese Überprüfung durch die eingebende Stelle, in den sonstigen Dateien durch Europol. Sind die Daten weiterhin notwendig, könnten die Daten gespeichert bleiben und es hat nach längstens drei Jahren eine neuerliche Bedarfsprüfung zu erfolgen. Wird festgestellt, dass die Daten nicht mehr erforderlich sind oder sind ex lege die Voraussetzungen für ihre Speicherung wegfallen, werden sie automatisch gelöscht (Abs. 1).

Löscht eine Sicherheitsbehörde Daten, die an Europol übermittelt worden sind, so ist die Nationale Europol-Stelle darüber zu informieren, die dies Europol mitteilt.

Würden durch die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt, so unterbleibt diese Löschung selbst nach Ablauf der zuvor angeführten Fristen. Eine Verwendung der Daten ist dann nur mit Zustimmung des Betroffenen zulässig. Zu denken ist hier beispielsweise an mögliche Opfer von Straftaten (Abs. 3).

Zu § 13 (Verwendung von Protokolldaten)

Nach Art. 18 des Beschlusses hat Europol geeignete Kontrollmechanismen einzuführen, mit denen die Rechtmäßigkeit der Datenabfragen aus den automatisierten Dateien, die zur Verarbeitung personenbezogener Daten verwendet werden, überprüft werden kann. Den Mitgliedstaaten hat Europol auf deren Ersuchen Zugang zu den Protokolldaten zu gewähren. Näheres regelt der Verwaltungsrat nach Anhörung der gemeinsamen Kontrollinstanz.

Die auf diese Weise erhobenen Daten dürfen von der nationalen Kontrollinstanz, der gemeinsamen Kontrollinstanz sowie von Europol nur zu diesem Zweck verwendet werden und sind nach 18 Monaten zu löschen, es sei denn, die Daten werden für eine laufende Kontrolle weiterhin benötigt.

Zu § 14 (Nationale Kontrollinstanz)

Jeder Mitgliedstaat hat eine nationale Kontrollinstanz zu bezeichnen, der nach Maßgabe des nationalen Rechts die Kontrolle der Zulässigkeit der Eingabe und des Abrufs personenbezogener Daten sowie der Übermittlung dieser Daten an Europol durch die Nationale Europol-Stelle und die österreichischen Verbindungsbeamten obliegt (Art. 33 des Beschlusses, Art. 23 des Übereinkommens). Wie schon bisher in Vollziehung des Art. 23 Europol-Übereinkommen soll diese Aufgabe der Datenschutzkommission zukommen.

Dazu hat die Datenschutzkommission Zugriff auf die von der Nationalen Europol-Stelle und den Verbindungsbeamten eingegebenen Daten im Informationssystem. Selbstverständlich ist zu diesem Zweck Zugang zu den Diensträumen und Akten zu gewähren.

Zu § 15 (Gemeinsame Kontrollinstanz)

Die gemeinsame Kontrollinstanz setzt sich aus höchstens zwei Vertretern der nationalen Kontrollinstanzen der Mitgliedstaaten zusammen. Diese werden auf fünf Jahre ernannt. Für jeden von der Nationalen Kontrollinstanz zu entsendenden Vertreter ist ein Stellvertreter zu nominieren. Im Übrigen kann davon ausgegangen werden kann, dass sich die Nationale Kontrollinstanz bei der Entsendung von Mitgliedern am Beschluss orientieren wird. Die Mitgliedstaaten haben die Unabhängigkeit der Mitglieder der gemeinsamen Kontrollinstanz zu gewährleisten; daher wird in Abs. 1 ausdrücklich festgelegt, dass diese bei ihrer Aufgabenerfüllung an keine Weisungen gebunden sind. Die Nationale Europol-Stelle und die nationale Kontrollinstanz haben die gemeinsame Kontrollinstanz auf deren Verlangen bei der Erfüllung ihrer Aufgaben zu unterstützen.

Zu § 16 (Auskunftsrecht)

Wie schon nach Art. 19 des Europol-Übereinkommens räumt auch Art. 30 des Beschlusses jeder Person das Recht ein, kostenlos bei der nationalen Behörde des Mitgliedstaates seiner Wahl Auskunft darüber zu verlangen, ob bei Europol sie betreffende Daten gespeichert sind. Nationale Behörde ist jene, die nach nationalem Recht die Auskunftsverpflichtung in sicherheits- oder kriminalpolizeilichen Aufgabenbereichen zu erfüllen hat.

Die befasste nationale Behörde – für Österreich ist das die Nationale Europol-Stelle – hat das Ersuchen an Europol weiterzuleiten. Die Frist für die Erledigung beträgt drei Monate ab Einlangen. Vor der Beantwortung durch Europol ist der Nationalen Europol-Stelle Gelegenheit zur Stellungnahme zu geben. Diese hat sich bei Vorliegen der in Abs. 2 taxativ angeführten Gründe gegen eine Beantwortung auszusprechen hat. Hierbei hat immer eine Interessenabwägung stattzufinden.

Zu § 17 (Recht auf Richtigstellung oder Löschung von Daten)

Neben dem Recht auf Auskunft räumt Art. 31 des Beschlusses (Art. 20 des Übereinkommens) das Recht auf Richtigstellung und Löschung gegenüber Europol ein. Jede Person ist berechtigt, Europol zu ersuchen, sie betreffende fehlerhafte Daten zu berichtigen. Über die getroffenen Veranlassungen wird sie verständigt und sie kann sich für den Fall, dass sie damit nicht einverstanden ist, an die gemeinsame Kontrollinstanz wenden.

Zu § 18 (Beschwerderecht)

Europol hat in seiner Beantwortung des Auskunftsbegehrens auf die Möglichkeit einer Beschwerde an die gemeinsame Kontrollinstanz hinzuweisen (Art. 32 des Beschlusses, Art. 19 Abs. 6 des Übereinkommens). Diese kann auch befasst werden, wenn Europol den Antrag nicht binnen einer Frist von drei Monaten erledigt. Die Beschwerde ist bei der gemeinsamen Kontrollinstanz einzubringen. Wird die Beschwerde bei der Nationalen Europol-Stelle oder direkt bei Europol eingebracht, ist die Beschwerde an die gemeinsame Kontrollinstanz weiterzuleiten.

Zu §19 (Kontrollbefugnisse)

In Umsetzung des Art. 30 Abs. 7 des Beschlusses (Art. 24 Abs. 4 des Übereinkommens) wird jedermann das Recht eingeräumt, sich an die gemeinsame Kontrollinstanz zu wenden, um überprüfen zu lassen, ob Europol ihn betreffende personenbezogene Daten rechtmäßig verwendet.

Die nationale Kontrollinstanz kann um Prüfung hinsichtlich solcher Daten ersucht werden, die durch die österreichische Nationale Kontaktstelle oder österreichische Verbindungsbeamte eingegeben wurden.

3. Teil Grenzüberschreitende Zusammenarbeit

Zu § 20 (Nationale Kontaktstelle)

„Nationale Kontaktstellen" sind jene von den einzelnen Mitgliedstaaten benannten Stellen, die zum automatisierten Vergleich von DNA-Profilen, daktyloskopischen Daten und zum automatisierten Abruf von Daten aus nationalen Fahrzeugregistern berechtigt sind. Für Österreich wird der Bundesminister für Inneres als die nationale Kontaktstelle bestimmt. Die Organisationseinheit, die diese Aufgabe für den Bundesminister wahrnimmt, ist das Bundeskriminalamt.

Zu § 21 (DNA-Analysedatei)

Der Prüm-Beschluss verpflichtet alle Mitgliedstaaten, bis längstens 26. August 2011 nationale Datenbanken für den automatisierten Vergleich von DNA-Profilen, den automatisierten Abruf von daktyloskopischen Daten aus der nationalen Datenbanken sowie den automatisierten Abruf von Daten aus den nationalen Fahrzeugregistern zu schaffen. Solche Datenbanken bestehen in Österreich bereits seit längerer Zeit in Form der zentralen erkennungsdienstlichen Evidenz nach § 75 SPG und der zentralen Zulassungsevidenz nach § 47 Abs. 4 KFG.

In diesem Sinne wird jener Teil der von den Sicherheitsbehörden gemäß § 75 SPG verarbeiteten Daten, die die DNA-Profile bestimmter Menschen (Personenprofile) und die DNA-Profile Unbekannter (offene Spuren) enthalten, als DNA-Analysedatei definiert. In dieser dürfen DNA-Profile nur in Form eines Buchstaben- oder Zahlencodes, der eine Reihe von Identifikationsmerkmalen des nicht codierten Teiles einer analysierten menschlichen Molekularstruktur an den verschiedenen DNA-Loci abbildet, gespeichert werden, wobei im nicht codierten Teil der DNA keine genetischen Informationen über funktionale Eigenschaften eines Organismus enthalten sein dürfen. DNA-Profile dürfen keine Daten enthalten, auf Grund derer eine Person unmittelbar identifiziert werden kann. Stattdessen sind DNA-Profile derart mit Kennungen zu versehen, dass sie den Datensatz als den eines bekannten Menschen oder einer offenen Spur erkennen lassen, weiters eine Zuordnung zur den Identitätsdaten eines bestimmten Menschen ermöglichen sowie ihn als ein von inländischen Sicherheitsbehörden ermitteltes Datum ausweist.

Zu § 22 (Verwendung der Daten der DNA-Analysedateien)

Nach Abs. 1 hat der Bundesminister für Inneres den nationalen Kontaktstellen der anderen Mitgliedstaaten zur Aufklärung und Verfolgung gerichtlich strafbarer Handlungen den Zugriff auf die DNA-Analysedatei im Datenfernverkehr in der Weise zu eröffnen, dass sie automatisiert alle in der DNA-Analysedatei verarbeiteten DNA-Profile mit ihren eigenen vergleichen können.

Zu unterscheiden ist einerseits, ob es sich um den Vergleich offener Spuren handelt, das sind Spuren, die noch keiner Person zugeordnet werden können und die als solche zu kennzeichnen sind, und andererseits dem Vergleich von Personenprofilen, das sind DNA-Profile, die einer bestimmten Person zugeordnet werden können:

Offene Spuren können nicht nur im Einzelfall, sondern auch in großer Anzahl gleichzeitig mit offenen Spuren in DNA-Analysedateien anderer Mitgliedstaaten verglichen werden. Dagegen dürfen Personenprofile nur dann mit von Sicherheitsbehörden anderer Mitgliedstaaten verarbeiteten DNA-Profilen verglichen werden, wenn dies im konkreten Einzelfall erforderlich ist.

Nach Abs. 2 ist der Bundesminister für Inneres ermächtigt, zur Aufklärung und Verfolgung von gerichtlich strafbaren Handlungen die in der DNA-Analysedatei verarbeiteten DNA-Profile im Wege des Datenfernverkehrs automatisiert mit allen in den Analysedateien der anderen Mitgliedstaaten verarbeiteten DNA-Profilen zu vergleichen. Auch hier ist zu unterscheiden, ob es sich um offene Spuren oder um Personenprofile handelt.

Abs. 3 regelt das weitere Vorgehen nach Durchführung eines Vergleiches offener Spuren oder von Personenprofilen: bei einem Treffer, also dem Übereinstimmen von DNA-Profilen in anderen Analysedateien, sind der Nationalen Kontaktstelle des abrufenden Mitgliedstaats jene Fundstellendatensätze (DNA-Profile samt Kennungen), mit denen Übereinstimmung festgestellt worden ist, auf automatisierte Weise zu übermitteln. Kann keine Übereinstimmung festgestellt werden, so ist die Nationale Kontaktstelle darüber ebenso auf automatisierte Weise zu informieren.

Abs. 4 stellt klar, dass im Falle der Übereinstimmung die entsprechenden Daten von den Sicherheitsbehörden weiterverarbeitet werden dürfen.

Der Vergleich darf nur zur Verfolgung von Straftaten und nach Maßgabe des Rechts des abrufenden Mitgliedstaates erfolgen. Damit ist es nicht notwendig, alle entsprechenden Rechtsvorschriften aller anderen Mitgliedstaaten zu kennen, um auf deren DNA-Analyse-Dateien zugreifen zu können. Jede nationale Kontaktstelle kann daher unter denselben Bedingungen auf die DNA-Analyse-Dateien in anderen Mitgliedstaaten zugreifen, wie sie für den Zugriff auf die eigene DNA-Analyse-Datei gelten.

Die Übermittlung von über DNA-Fundstellendatensätzen hinausgehenden Daten richtet sich nach den bestehenden Amts- und Rechtshilfebestimmungen. Die Anfrage wird nach dem nationalen Recht des anfragenden Mitgliedstaates in Form eines Amts- oder Rechtshilfeersuchens gestellt. Österreich kann diese Anfrage bei Treffern im Rahmen der polizeilichen Amtshilfe nach § 6 ff. Polizeikooperationsgesetz bzw. gemäß §§ 3 und 5 Polizeikooperationsgesetz eingehende Anfragen auf dieser Rechtsgrundlage beantworten.

Zu § 23 (Ermittlung erkennungsdienstlicher Daten zu Zwecken der Amtshilfe)

Wenn ein Mitgliedstaat für ein laufendes Ermittlungs- oder Strafverfahrens das DNA-Profil einer bestimmten Person benötigt und bekannt ist, dass sich diese Person in Österreich aufhält, so ist Amtshilfe durch die Gewinnung und Untersuchung molekulargenetischen Materials und der Übermittlung des dabei gewonnenen DNA-Profils zu leisten.

Die Leistung der Rechtshilfe ist an die in Abs. 2 genannten Bedingungen geknüpft.

Zu § 24 (Verwendung daktyloskopischer Daten)

Ähnlich wie auch bei DNA-Daten hat der Bundesminister für Inneres den nationalen Kontaktstellen anderer Mitgliedstaaten den Zugriff auf die gemäß § 75 SPG verarbeiteten daktyloskopischen Daten im Wege des Datenfernverkehrs im Einzelfall zum Zwecke des Vergleichs mit von ihnen selbst ermittelten daktyloskopischen Daten zu ermöglichen. Dabei wird zwischen einem daktyloskopischen Datum, das in einem Mitgliedstaat vorliegt, und den daktyloskopischen Daten in den Dateien eines anderen Mitgliedssstaates verglichen.

Anders als bei DNA-Profilen ist es aber auf Grund des unterschiedlichen technischen Verfahrens nicht möglich, bereits beim ersten Vergleich eine eindeutige Zuordnung des übermittelten daktyloskopischen Datums mit dem entsprechenden Fundstellendatensatz bei der empfangenden Stelle vorzunehmen. Zur endgültigen Zuordnung muss daher ein Set annähernd übereinstimmender Fundstellendatensätze von der empfangenden Stelle an die abrufende Stelle übermittelt werden. Vergleich und Übermittlung der annähernd übereinstimmenden Fundstellendatensätze erfolgen automatisiert, d.h., dass dieser Vergleich durch ein technisches Verfahren ohne Einbeziehung eines Beamten erfolgt. Bei der abrufenden Stelle erfolgt dann die eindeutige Zuordnung des daktyloskopischen Datums (Verifikation) zu einem der automatisiert übermittelten Fundstellendatensätze durch einen Experten der abrufenden Stelle.

Der automatisierte Abruf darf nur im Einzelfall und nur zur Verhinderung und Verfolgung von Straftaten und nach Maßgabe des Rechts des abrufenden Mitgliedstaates erfolgen.

Abs. 2 stellt klar, dass der Bundesminister für Inneres ermächtigt ist, zur Abwehr gefährlicher Angriffe und zur Aufklärung gerichtlich strafbarer Handlungen die von Sicherheitsbehörden ermittelten daktyloskopischen Daten mit jenen zu vergleichen, die von den Sicherheitsbehörden anderer Mitgliedstaaten verarbeitet werden. Kommt es bei einem solchen Vergleich zu einer Übereinstimmung, dürfen diese Daten und dazu gehörige Informationen von den Sicherheitsbehörden weiterverarbeitet werden.Im Falle einer Übereinstimmung von daktyloskopischen Daten richtet sich die Übermittlung von über daktyloskopischen Daten samt zugehöriger Kennung hinausgehenden Daten nach den bestehenden Amts- und Rechtshilfeübereinkommen.

Zu § 25 (Abfragen aus Zulassungsevidenzen)

Anders als beim automatisierten Vergleich von DNA-Profilen und daktyloskopischen Daten handelt es sich in diesem Fall nicht nur um die bloße Mitteilung, dass ein passender Fundstellendatensatz vorhanden ist (Treffer), sondern es können direkt Kfz-Daten gelesen werden (Lesezugriff). Die für den Abruf vorgesehenen Daten sind die Eigentümer(Halter-)daten sowie die Fahrzeugdaten. Anhand eines bekannten vollständigen Kfz-Kennzeichens oder einer vollständigen Fahrgestellnummer können also die vollständigen Fahrzeugdaten (Marke, Type,…) und die Eigentümer(Halter-)daten abgerufen werden.

Der automatisierte Abruf darf nur zur Verhinderung und Verfolgung von Straftaten, zur Aufklärung oder Verfolgung von solchen Verstößen, die bei der abrufenden Vertragspartei in die Zuständigkeit der Gerichte oder Staatsanwaltschaften fallen oder zur Abwehr von Gefahren für die öffentliche Sicherheit und jeweils nur im Einzelfall erfolgen. Das heißt, die abrufende Stelle darf jeweils nur einen

automatisierten Abruf aus den Fahrzeugregistern der anderen Mitgliedstaaten vornehmen. Die Beurteilung der Zulässigkeit des Abrufs erfolgt nach Maßgabe des Rechts der abrufenden Stelle.

Abs. 3 stellt klar, dass die Sicherheitsbehörden zur Abwehr gefährlicher Angriffe und zu kriminalpolizeilichen Zwecken ermächtigt sind, im Wege des Bundesministers für Inneres Abfragen aus Fahrzeugregistern der anderen Mitgliedstaaten zu tätigen.

§ 26 Verwendung von Protokolldaten

Anders als nach § 11 PolKG sind Protokollierungsdaten zwei Jahre aufzubewahren.

Zu § 27 (Einschreiten auf Hoheitsgebiet anderer Mitgliedstaaten)

Der Beschluss 2008/617/JI des Rates vom 23. Juni 2008 über die Verbesserung der Zusammenarbeit zwischen den Spezialeinheiten der Mitgliedstaaten der Europäischen Union in Krisensituationen, Amtsblatt Nr. L 210 vom 6.8.2008, S. 73 – 75, sieht vor, dass Spezialeinheiten der Polizei zur operativen Bekämpfung beispielsweise von Terrorlagen in anderen Mitgliedstaaten zum Einsatz gebracht werden können. Zu derartigen Einsätzen sind allerdings nur geeignete Bedienstete zu entsenden, also solche, die auf Grund ihrer speziellen Ausbildung zur Beendigung gefährlicher Angriffe besonders geeignet erscheinen. Die Entsendung in einen Mitgliedstaat ist nur auf Ersuchen eines Mitgliedstaates und nur mit Zustimmung des Bundesministers für Inneres zulässig.

Neben dem eingangs erwähnten Beschluss sieht auch der Prüm-Beschluss operative Einsatzformen vor; dem folgend können mit Zustimmung des Bundesministers für Inneres zur Intensivierung der polizeilichen Kooperation Organe des öffentlichen Sicherheitsdienstes in einen anderen Mitgliedstaat entsandt und mit der gemeinsamen Wahrnehmung von Aufgaben zur Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit oder der Kriminalpolizei im aufnehmenden Mitgliedstaat betraut werden.

Gemäß § 15 Abs. 3 PolKG dürfen die Organe des öffentlichen Sicherheitsdienstes im Ausland keine Handlungen setzen, die Anordnungen einer zuständigen ausländischen Behörde widersprechen.

Da also sowohl der Prüm-Beschluss als auch der Beschluss über den Einsatz von Sondereinheiten jeweils bestimmte polizeiliche Einsatzformen zum Regelungsgegenstand haben, wird vorgeschlagen, diese gemeinsam zu regeln (§§ 27 und 28).

Zu § 28 (Einschreiten von Organen von Sicherheitsbehörden eines Mitgliedstaates im Inland)

In Abs. 1 wird festgelegt, dass der Bundesminister für Inneres ermächtigt ist, um Unterstützung durch geeignete Organe des öffentlichen Sicherheitsdienstes eines Mitgliedstaates zu ersuchen und deren Hilfe in Anspruch zu nehmen. Voraussetzung ist, dass der Einsatz dem Schutz von Leben, Gesundheit oder Eigentum dient und Gefahr im Verzug vorliegt oder zur Bewältigung einer Massenveranstaltung, Katastrophe oder eines schweren Unglücksfalles notwendig ist. Wie schon bei § 27 wird es auch hier erforderlich sein, dass bei Einsätzen nach Abs. 1 nur solche Polizeikräfte zum Einsatz gebracht werden, die auf Grund ihrer speziellen Ausbildung zur Beendigung gefährlicher Angriffe besonders geeignet erscheinen.

Darüber hinaus kann der Bundesminister für Inneres zur Intensivierung der polizeilichen Kooperation Organe ausländischer Sicherheitsbehörden mit Zustimmung des Entsendestaates mit der Wahrnehmung von Aufgaben zur Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit oder der Kriminalpolizei gemeinsam mit Organen der öffentlichen Sicherheit betrauen. Die Dienstverrichtung kann etwa in Form eines gemeinsamen Streifendienstes oder gemeinsam besetzter Kontroll-, Auswertungs- und Observationsgruppen erfolgen.

Die Organe der Sicherheitsbehörden des Mitgliedsstaates unterliegen bei ihren Einsätzen nach Abs. 1 und 2 der Leitung und den Weisungen der österreichischen Sicherheitsbehörden. In Bezug auf ihr Einschreiten im Inland sind weiters die Regelungen des § 17 PolKG (Besonderer Rechtsschutz) anzuwenden.

Den Organen von Sicherheitsbehörden anderer Mitgliedstaaten kommen dabei aber nicht etwa Ermächtigungen zur Anforderung von militärischen Assistenzkräften zu.

Zu § 29 (Befugnisse auf fremdem Hoheitsgebiet)

In Abs. 1 wird klargestellt, dass den in Österreich einschreitenden Sicherheitsorganen dieselben Befugnisse und auch dieselbe Verantwortlichkeit für ihr Handeln zukommen wie österreichischen Organen des öffentlichen Sicherheitsdienstes. Das gilt auch in Bezug auf Straftaten, die sie begehen oder die ihnen gegenüber begangen werden. Darüber hinaus nennt Abs. 2 bestimmte Berechtigungen der ausländischen Organe. So ist insbesondere hervorzuheben, dass ausländische Organe jegliche der ihnen zugewiesen Dienstwaffen in Österreich mitführen dürfen, gegebenenfalls also auch verbotene oder als Kriegsmaterial einzustufende Waffen, beispielsweise vollautomatische Schusswaffen.

Die Berechtigungen und Verpflichtungen nach Abs. 3 gelten auch für die Teilnahme an gemeinsamen Schulungen und Einsatzübungen.

Nach Abs. 4 sind auch die eingesetzten Fahrzeuge jenen des österreichischen öffentlichen Sicherheitsdienstes gleichgestellt (§§ 26 und 26a StVO).

Die österreichischen Organe des öffentlichen Sicherheitsdienstes sind ihrerseits ermächtigt, ihre Uniformen, Dienstwaffen, Munition, sonstige Zwangsmittel, Transportmittel und sonstige für den Einsatz notwendige Ausrüstungsgegenstände zu dem Einsatz, zu dem sie zur Unterstützung entsandt wurden, mitzunehmen, sofern dies nach dem Recht des ersuchenden Mitgliedstaates zulässig ist und bindendes Völkerrecht dem nicht entgegen steht.

4. Teil Nutzung des Visa-Informationssystems durch Sicherheitsbehörden

Zu § 30 (Zugriffsberechtigung auf VIS-Daten)

Mit der Entscheidung 2004/512/EG des Rates vom 8. Juni 2004 zur Errichtung des Visa-Informationssystems (VIS) wurde beschlossen, ein Visa-Informationssystem für den Austausch von Visa-Daten zwischen Mitgliedstaaten zu schaffen.

Diese Bestimmung ermächtigt die Sicherheitsbehörden, im Wege des Bundesministers für Inneres im Einzelfall und für Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer Straftaten nach den §§ 278b und 278c StGB sowie sonstiger schwerwiegender Straftaten, wie sie im Anhang 1 Teil A des EU-JZG angeführt sind, die in Abs. 1 angeführten Daten aus dem VIS abzufragen.

Werden Daten unrechtmäßig verwendet, haftet der Bund nach den Bestimmungen des Amtshaftungsgesetzes. Einer eigenen Haftungsregelung bedarf es nicht, weil im Gegensatz zu den Regelungen im 2. 3. und 5 ausschließlich österreichische Sicherheitsbehörden tätig sind und nur Abfragen und Übermittlungen (§§ 30 und 31) erfolgen. Hier greifen die bestehenden Haftungsregelungen, ohne dass es dafür Abweichungen bedarf.

Der Vollständigkeit wegen ist darauf hinzuweisen, dass die Eingabe von Visa-Daten ausschließlich durch die Visa-Behörden auf Grundlage der Verordnung (EG) Nr. 767/2008 vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung) erfolgt.

Zu § 31 (Übermittlung an Drittstaaten und Sicherheitsorganisationen)

Die Übermittlung personenbezogener Daten an Sicherheitsbehörden von Drittstaaten und internationalen Sicherheitsorganisationen ist nur unter eingeschränkten Voraussetzungen zulässig, nämlich in dringenden Fällen ausschließlich für Zwecke der Verhütung und Aufdeckung terroristischer Straftaten oder sonstiger schwerwiegender Straftaten und nur mit Zustimmung jenes Mitgliedstaates, der die Daten in das VIS eingegeben hat.

Zu § 32 (Auskunft und Richtigstellung)

Soll Auskunft über Daten erteilt werden, die von einem anderen Mitgliedstaat in das VIS eingegeben worden sind, ist dem Mitgliedstaat, der die Daten eingegeben hat, vor Auskunftserteilung Gelegenheit zur Stellungnahme zu gegeben. Sind abgefragte Daten von einer österreichischen Behörde, die keine Sicherheitsbehörde ist, eingegeben worden, ist vor Auskunftserteilung deren Zustimmung einzuholen.

Weiters ist jene Stelle, die Daten in das VIS eingegeben hat, zu informieren, wenn sich Anhaltspunkte ergeben, wonach im VIS verarbeitete Daten unrichtig sein könnten.

5. Teil Schengener Informationssystem

Zu § 33 (Schengener Informationssystem)

Die zentrale Bestimmung des Abs. 1 ermächtigt die Sicherheitsbehörden, zum Zweck der EU-weiten Ausschreibung von Personen und Sachen gemeinsam eine zentrale Datenanwendung, das nationale Schengener Informationssystem (N.SIS II) zu führen und den zuständigen Stellen der anderen Mitgliedstaaten im Wege des zentralen Schengener Informationssystems (CS.SIS) Daten zur Verfügung zu stellen. Weiters sind sie ermächtigt, Ausschreibungen der zuständigen Stellen anderer Mitgliedstaaten im Wege des zentralen Schengener Informationssystems zu ermitteln und in ihrem Schengener Informationssystem (N.SIS II) weiter zu verarbeiten und zu benützen. Dabei kommt dem Bundesminister für Inneres die Aufgabe eines Betreibers gemäß § 50 DSG 2000 zu.

Abs. 2 nennt jene Daten, die im Schengener Informationssystem eingegeben werden dürfen. Andere als die genannten personenbezogenen Daten dürfen in eine SIS-Ausschreibung nicht eingegeben werden.

Nach Abs. 3 dürfen Lichtbilder und Fingerabdrücke ausschließlich zur Überprüfung der Identität nach einer alphanumerischen Abfrage verwendet werden. Sobald die technischen und unionsrechtlichen

Voraussetzungen vorliegen, dürfen auch Fingerabdrücke als Auswahlkriterium für eine Abfrage verwendet werden.

Nach Abs. 4 hat eine Ausschreibung im Schengener Informationssystem bestimmte Daten jedenfalls und andere nur soweit zu enthalten, als diese verfügbar sind. Jedenfalls haben aufzuscheinen: Nachname(n) und Vorname(n), Geburtsname(n) und frühere(r) Name(n), Aliasnamen, Geschlecht und die zu ergreifende Maßnahme.

Überhaupt dürfen nach Abs. 5 Ausschreibungen im Schengener Informationssystem nur vorgenommen werden, wenn dies im Hinblick auf die Maßnahme unbedingt geboten erscheint.

Nach Abs. 6 darf dem Bundesminister für Justiz sowie den Gerichten und Staatsanwaltschaften eine Abfrageberechtigung aus dem Schengener Informationssystem eingeräumt werden, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Darüber hinaus sehen das Fremdenpolizeigesetz (FPG) und das Zollrechts-Durchführungsgesetz (ZollR-DG) Abfrageberechtigungen für Abgabenbehörden des Bundesministeriums für Finanzen aus dem Schengener Informationssystem vor: für Finanzämter im Rahmen ihrer Zuständigkeit zur Kontrolle der illegalen Arbeitnehmerbeschäftigung sowie für Finanzstrafbehörden nach § 102 Abs. 4 FPG und für Zollämtern im Rahmen ihrer Zuständigkeit zur Durchführung operativer Kontrollen und der Zollfahndungstätigkeit nach §§ 14, 22 und 29 ZollR-DV.

Daten, die gemäß Abs. 1 von den Sicherheitsbehörden verarbeitet werden, dürfen von diesen nicht an Behörden von Drittstaaten oder internationalen Organisationen weitergegeben werden (Abs. 7).

Nach Abs. 8 dürfen personenbezogenen Daten, welche die rassische Herkunft, die politischen oder religiösen oder andere Anschauungen einer Person erkennen lassen oder welche die Gesundheit oder das Sexualleben betreffen, nicht im SIS gespeichert werden.

Zu § 34 (Zusatzinformationen)

Nach § 4 Abs. 1 Bundeskriminalamt-Gesetz (BKA-G) ist das Sirene-Büro im Bundeskriminalamt angesiedelt.

Bei Ausschreibungen von Personen für Zwecke der Übergabehaft im Schengener Informationssystem ist beispielsweise auch eine Kopie des Europäischen Haftbefehles einzugeben. Fakultativ kann eine Übersetzung in eine oder mehrere Amtssprachen der Europäischen Union eingegeben werden. Um diese Eingabe zu ermöglichen haben die Sicherheitsbehörden dem Sirene-Büro die entsprechenden Unterlagen zu übermitteln.

Zu § 35 (Ausschreibung von Personen zum Zwecke der Übergabe oder Auslieferung)

Nach Abs. 1 haben die Sicherheitsbehörden auf Ersuchen der Gerichte oder Staatsanwaltschaften Daten zu Personen in das Schengener Informationssystem einzugeben, nach denen mit Europäischem Haftbefehl zum Zwecke der Übergabe oder nach denen für Zwecke der Auslieferung gesucht wird. Während Ausschreibungen für Zwecke der Übergabehaft auf Grund eines Europäischen Haftbefehles nach dem EU-JZG erfolgen, richten sich Ausschreibungen für Zwecke der Auslieferungshaft nach den Bestimmungen des Auslieferungs- und Rechtshilfegesetzes.

Nach Abs. 2 sind auch Personen, nach denen zum Zwecke der Übergabehaft mit Haftbefehl gefahndet wird, in das Schengener Informationssystem einzugeben, wenn in einem Übereinkommen zwischen der EU und einem Drittstaat eine Ausschreibung seiner Haftbefehle im Schengener Informationssystem vorgesehen ist.

Der Ausschreibung auf Grund eines Europäischen Haftbefehls ist die Kopie des Haftbefehles anzufügen.

Weiters hat die ausschreibende Sicherheitsbehörde anderen Mitgliedstaaten die in Abs. 4 genannten Zusatzinformationen zu übermitteln. Diese Informationen bieten jedem Schengener Staat die Möglichkeit einer nochmaligen Prüfung, ob die Festnahme der Person in seinem Hoheitsbereich rechtlich zulässig ist.

Für den Fall, dass die Durchführung der Übergabehaft auf Grund anderer gesetzlicher Bestimmungen oder internationaler Verpflichtungen nicht möglich ist, ist in Abs. 5 vorgesehen, dass die ausschreibende Sicherheitsbehörde das Sirene-Büro jenes Mitgliedstaates, der die Ausschreibung veranlasst hat, zu ersuchen hat, die Ausschreibung dem entsprechend zu kennzeichnen. Solcher Art gekennzeichnete Ausschreibungen gelten als Ausschreibungen zur Aufenthaltsermittlung.

Nach Abs. 6 kommen einer Ausschreibung gemäß Abs. 1 und 2 die Wirkungen einer Anordnung der Festnahme und ihrer Ausschreibung nach den Bestimmungen der Strafprozessordnung 1975 zu. Wird daher eine Person auf Grund einer Ausschreibung gemäß Abs. 1 oder 2 im Inland betreten, so ist sie festzunehmen, der Staatsanwaltschaft unverzüglich zu verständigen und in die Justizanstalt des zuständigen Gerichtes einzuliefern.

Zu § 36 (Behandlung von Ausschreibungen eines Mitgliedstaates zum Zwecke der Übergabe oder Auslieferung gesuchter Personen)

Diese Bestimmung regelt den Fall, dass eine Ausschreibung für Zwecke der Festnahme wegen einer die Festnahme ausschließenden Entscheidung - oder im Falle einer Ausschreibung zum Zwecke der Auslieferungshaft wegen einer noch nicht abgeschlossenen Prüfung - einer österreichischen Justizbehörde nicht vollzogen werden darf. Diesfalls ist die im Schengener Informationssystem aufscheinende Ausschreibung der Übergabe- oder Auslieferungshaft als Ausschreibung zur Aufenthaltsermittlung zu behandeln.

Zu § 37 (Ausschreibung von Abgängigen)

Diese Bestimmung legt zunächst die näheren Voraussetzungen für die Speicherung von Daten jener Personen im SIS fest, die den Sicherheitsbehörden gegenüber als vermisst (abgängig) gemeldet wurden. Im EKIS auf der Grundlage des § 57 Abs. 1 Z 7 bis 9 SPG verarbeitete Daten werden daher analog für die Veranlassung einer SIS-Ausschreibung heranzuziehen sein. Darüber hinaus werden nach dieser Ausschreibungskategorie auch Daten von Personen aufgenommen, bei denen die Voraussetzungen für eine Unterbringung in einer Anstalt nach den §§ 3 und 8 des Unterbringungsgesetzes bzw. für eine Vorführung im Sinne des § 46 SPG vorliegen.

Die aus Anlass einer positiven SIS-Abfrage zu treffenden Maßnahmen haben sich am nationalen Recht, für Österreich somit im Wesentlichen an den einschlägigen Regelungen des SPG, des Unterbringungsgesetzes und in Bezug auf abgängige Minderjährige des ABGB auszurichten.

Wird eine als abgängig ausgeschriebene Person aufgefunden, ist dem ausschreibenden Sirene-Büro der Aufenthalt des Abgängigen mitzuteilen. Bei Volljährigen bedarf die Mitteilung der Einwilligung des Aufgefundenen. Jedenfalls zulässig ist, das ausschreibende Sirene-Büro sowie die Person, die den Betroffenen als abgängig gemeldet hat, darüber zu informieren, dass die Person aufgefunden wurde, ohne dass dabei Angaben zum Aufenthaltsort mitgeteilt werden. Damit soll sichergestellt werden, dass in diesem Abgängigkeitsfall die bestehende Ausschreibung gelöscht wird und keine neuerliche Ausschreibung erfolgt.

Zu § 38 (Ausschreibung von Personen, die im Hinblick auf ihre Teilnahme an einem Gerichtsverfahren gesucht werden)

Diese Regelung ermöglicht die Speicherung von Daten jener Personen, die vor einem Gericht wegen eines gegen ihre Person eingeleiteten Strafverfahrens zu erscheinen haben oder denen ein Strafurteil oder eine Anordnung zum Antritt einer Freiheitsstrafe zuzustellen ist. Zweck der SIS-Ausschreibung ist die Feststellung des Aufenthaltsortes dieser Personen, um ihnen gerichtliche Verfügungen zustellen zu können.

Zu § 39 (Ausschreibung von Personen und Sachen zum Zwecke der verdeckten Kontrolle)

Nach dieser Bestimmung werden die Sicherheitsbehörden ermächtigt, zur Abwehr gefährlicher Angriffe sowie zur Aufklärung und Verfolgung gerichtlich strafbarer Handlungen Personen für Zwecke einer verdeckten Kontrolle auszuschreiben, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass eine Person eine im Anhang 1 Teil A zum EU-JZG genannte Straftat plant oder begeht oder die Gesamtbeurteilung einer Person, insbesondere aufgrund der bisher von ihr begangenen Straftaten erwarten lässt, dass sie künftig eine im Anhang 1 Teil A zum EU-JZG angeführte Straftat begehen wird.

Zulässig ist auch die Ausschreibung von Land-, Wasser- und Luftfahrzeugen und Containern für verdeckte Kontrollen im Schengener Informationssystem, wenn Anhaltspunkte dafür vorliegen, dass eine Verbindung zu den in Abs. 1 angeführten Fällen besteht.

Bei Vorliegen einer Ausschreibung nach Abs. 1 sind die Sicherheitsbehörden ermächtigt, die in Abs. 3 angeführten Informationen verdeckt zu ermitteln und der ausschreibenden Stelle zu übermitteln. Die Eingabe dieser Informationen in das Schengener Informationssystem allein zum Zweck der Übermittlung dieser Daten an die ausschreibende Stelle ist allerdings nicht zulässig.

Diese Ausschreibungskategorie dient in erster Linie der sicherheitspolizeilichen Aufgabenstellung der Gefahrenabwehr und der Möglichkeit, durch Evidenthaltung personenbezogener Daten gefährlichen Angriffen auf Rechtsgüter vorzubeugen; sie kann auch für Zwecke der Strafverfolgung in Anspruch genommen werden.

Zu § 40 (Ausschreibung von Sachen zur Sicherstellung oder Beweissicherung)

In dieser Ausschreibungskategorie können die in Abs. 2 ausgewiesenen Gegenstände in das Schengener Informationssystem zum Zwecke der Sicherstellung oder zur Beweissicherung im Strafverfahren aufgenommen werden. Ergibt eine Abfrage das Vorliegen einer Sachenfahndungsausschreibung von

Sicherheitsbehörden eines anderen Mitgliedstaates, ist der ausschreibende Mitgliedstaat über die Auffindung zu informieren. Weiters sind ihm die näheren Umstände bekannt zu geben. In diesem Zusammenhang kann es notwendig auch sein, personenbezogene Daten wie insbesondere in wessen Gewahrsam sich der Gegenstand befindet oder befand, bekannt zu geben.

Sofern keine Sicherstellungsanordnung vorliegt, sind die Sicherheitsbehörden von sich aus ermächtigt, eine Sicherstellung unter den Voraussetzungen des § 110 Abs. 3 StPO vorzunehmen. Die weitere Vorgangsweise richtet sich ausschließlich nach den Bestimmungen über die Sicherstellung oder die Beschlagnahme von Sachen im Strafverfahren.

Zu § 41 (Speicherfristen)

In das Schengener Informationssystem eingegebene Personenfahndungsausschreibungen sind längstens alle drei Jahre ab ihrer Eingabe von der eingebenden Stelle auf die Notwendigkeit der weiteren Speicherung hin zu prüfen.

Für Zwecke der verdeckten Kontrolle beträgt diese Frist in Bezug auf Personenausschreibungen ein Jahr und in Bezug auf Sachausschreibungen fünf Jahre.

Ausschreibungen von Sachen für Zwecke der Sicherstellung oder zur Beweissicherung in Strafverfahren sind längstens alle zehn Jahre daraufhin zu überprüfen, ob eine über diesen Zeitraum hinausgehende Speicherung erforderlich ist.

Zu § 42 (Richtigstellung und Ergänzung von Ausschreibungen)

Änderungen, Ergänzungen, Richtigstellungen und Aktualisierungen von Daten im Schengener Informationssystem dürfen Sicherheitsbehörden nur hinsichtlich der von ihnen selbst vorgenommenen Ausschreibungen durchführen. Liegen Anhaltspunkte dafür vor, dass Daten in Ausschreibungen anderer Mitgliedstaaten unrichtig oder unrechtmäßig gespeichert wurden, hat die Sicherheitsbehörde, die dies feststellt, der eingebenden Sicherheitsbehörde des Mitgliedstaates im Wege des Sirene-Büros unverzüglich, längstens aber innerhalb von 10 Tagen, dies mitzuteilen.

Die Abs. 3 und 4 regeln Zweifelsfälle hinsichtlich eingegebener personenbezogener Daten:

Kommen nach Abs. 3 Anhaltspunkte hervor, die Zweifel an der eindeutigen Unterscheidbarkeit ausgeschriebener Personen aufkommen lassen, hat die Sicherheitsbehörde, soweit es sich nicht ohnehin um eine von ihr selbst veranlasste Ausschreibung handelt, den Sachverhalt abzuklären. Die Sicherheitsbehörde hat, soweit dies zur eindeutigen Identifizierung einer von ihr ausgeschriebenen Person erforderlich ist, die Ausschreibung um zusätzliche Informationen zu ergänzen, um eine klare Unterscheidbarkeit zu gewährleisten.

Besteht dagegen nach Abs. 4 die Möglichkeit, dass eine von einer Ausschreibung nicht betroffene Person mit einer tatsächlich ausgeschriebenen verwechselt wird, darf die Sicherheitsbehörde mit ausdrücklicher Zustimmung des Betroffenen die Ausschreibung um dessen Namen, besondere unveränderliche körperliche Merkmale, Geburtsdatum und –ort, Geschlecht, Lichtbild, Fingerabdruck, Staatsangehörigkeit und Daten von Ausweisdokumenten ergänzen. Betroffene sind auf diese Möglichkeit hinzuweisen. Ihre Daten dürfen aber nur zur Feststellung, dass sie von der Ausschreibung nicht betroffen sind, verwendet werden.

Zu § 43 (Auskunftsrecht)

Vor einer Beauskunftung nach § 26 DSG ist dem Mitgliedstaat, der die Daten eingegeben hat, Gelegenheit zur Stellungnahme zu geben.

Zu § 44 (Verweisungen)

Verweisungsregelung.

Zu § 45 (Sprachliche Gleichbehandlung)

Die Einführung dieser Norm trägt den Bestrebungen des „gender mainstreaming“ Rechnung.

Zu § 46 (Inkrafttreten)

Das Inkrafttreten dieses Bundesgesetzes ist für den 1.1.2010 vorgesehen.

Artikel 2

Änderung des Polizeikooperationsgesetzes

Zu Z 1 (§ 8 Abs. 2):

Hier handelt es sich lediglich um eine Zitieranpassung, die wegen der Ersetzung des Europol-Übereinkommens durch den innerstaatlich umzusetzenden Europol-Beschluss erforderlich ist.

Zu Z 2 (§ 8 Abs. 4):

Wird eine Sicherheitsbehörde um Amtshilfe ersucht, so hat sie vor der Übermittlung der Daten die Zustimmung oder Genehmigung eines Gerichtes oder einer Staatsanwaltschaft einzuholen, soweit eine Übermittlung von Daten von einer solchen Zustimmung oder Genehmigung abhängig ist, beispielsweise nach dem EU-JZG oder dem ARHG.

Zu Z 3 (§ 20 Abs. 5):

Inkraftretensbestimmung.

Artikel 3

Änderung des Sicherheitspolizeigesetzes

Zu Z 1 und 2 (§ 58b Abs. 1 und 4)

Die Anfertigung und Speicherung eines Lichtbildes von Angehaltenen ist bei der Administration des Vollzuges im Hinblick auf die eindeutige Identifizierung der Betroffenen erforderlich, um eine Verwechslung mit anderen Insassen, insbesondere im Zusammenhang mit Entlassungs-, Abschiebungs- und Einlieferungsvorgängen oder Medikamentenverabreichung, Ausführungen etc., während der Haft mit größtmöglicher Wahrscheinlichkeit ausschließen zu können. Ein aktuelles Lichtbild etwa auf dem Häftlingsbegleitschein oder dem Haftbericht für die Sanitäter und den Amtsarzt soll die eindeutige Identifikation während des Vollzugs erlauben. Oftmals sind Angehaltene nicht einmal im Besitz eines Dokumentes zum Nachweis ihrer Identität, oder das Foto in Ausweis oder Pass ist für Zwecke der Wiedererkennung unbrauchbar.

So kommt es vor, dass Häftlinge mit falschem Namen eingeliefert werden und der Name während der Haft berichtigt wird, dass sich Häftlinge mit gleich oder ähnlich lautenden Namen - oftmals ohne Deutschkenntnisse - in Haft befinden, von denen einer entlassen wird und der andere in eine Justizanstalt zu überstellen ist oder ein bestimmter Häftling zwecks Medikamentenverabreichung (etwa im Substitutionsprogramm) zur Sanitätsstelle gerufen werden. In all diesen Fällen ist das Foto zur eindeutigen Wiedererkennung und zur Vermeidung von Verwechslungen - auch zum Schutz von Betroffenen - erforderlich.

Zu Z 3 (91c Abs. 1)

Im Sinne eines umfassenden kommissarischen Rechtsschutzes durch den Rechtsschutzbeauftragten soll es auch anlässlich der besonderen Ermittlungsform der sicherheitspolizeilichen Observation zu einer Befassung des Rechtsschutzbeauftragten kommen.