

Vorblatt

Ziel und Inhalt der Gesetzesinitiative:

Das in §1 DSG 2000 verankerte Grundrecht auf Datenschutz bewirkt keinen schrankenlosen Anspruch auf Geheimhaltung personenbezogener Daten, sondern führt Gründe für Ausnahmen vom grundsätzlichen Geheimhaltungsschutz an. Beschränkungen können sich etwa bei überwiegenden berechtigten Interessen anderer gegenüber den schutzwürdigen Geheimhaltungsinteressen des Betroffenen ergeben. Werden Eingriffe zugunsten der „Interessen anderer“ (z.B. öffentlicher Interessen) durch eine staatliche Behörde vorgenommen, bedarf es dazu einer besonderen gesetzlichen Grundlage (vgl. Art. 8 Abs. 2 EMRK). Das Erfordernis einer ausdrücklichen gesetzlichen Ermächtigung zur Datenverwendung wurde aus dem DSG 1978 übernommen, wobei die Materialien dazu (EB zur RV 1975 zu § 6) ebenso wie das Bundeskanzleramt-Verfassungsdienst in einem Rundschreiben (GZ 810.099/1-V/1a/85) konkretisieren, dass dem Gesetz Datenarten und Betroffenen- sowie Empfängerkreise zu entnehmen sein müssen. Mit dem vorliegenden Entwurf soll im Wesentlichen der Übergangsbestimmung (im Verfassungsrang) des § 61 Abs. 4 des Bundesgesetzes über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000), BGBl. 165/1999, Rechnung getragen werden, wonach Datenanwendungen, die für die in § 17 Abs. 3 genannten Zwecke (hier vor allem Vorbeugung, Verhinderung oder Verfolgung von Straftaten im Sinne des § 17 Abs. 3 Z 5 notwendig sind, ab 1.1.2008 eine ausreichende gesetzliche Grundlage benötigen. Daher sollen die entsprechenden, ausreichend determinierten Bestimmungen im Sicherheitspolizeigesetz – SPG, BGBl. 1991/566, geschaffen werden.

Der vorliegende Gesetzentwurf enthält im Wesentlichen folgende Regelungen:

1. Schaffung von ausdrücklichen Regelungen für Datenanwendungen der Sicherheitsbehörden zu folgenden Zwecken:

1.1. Leitung, Koordination und Administration von Einsätzen und Erfüllung der ersten allgemeinen Hilfeleistungspflicht, sowie Personen- und Objektschutz;

1.2. Abwehr krimineller Verbindungen und gefährlicher Angriffe sowie deren Vorbeugung mittels Analyse;

1.3. Evidenthaltung von Wegweisungen und Betretungsverboten sowie von einstweiligen Verfügungen zum Schutz vor Gewalt in der Familie;

1.4. Evidenthaltung von Wegweisungen und Betretungsverboten in Schutzzonen;

2. Schaffung einer Bestimmung zur Errichtung einer zentralen Analysedatei über mit beträchtlicher Strafe bedrohte Gewaltdelikte, insbesondere sexuell motivierte Straftaten, einschließlich Übermittlungsermächtigung und Lösungsverpflichtung;

3. Neuregelung der Bestimmung über die Auskunftserteilung durch Betreiber öffentlicher Telekommunikationsdienste;

4. Modifizierung der Bestimmung über die Wiederholung einer Sicherheitsüberprüfung;

5. Anpassungen bei den Fahndungsausschreibungen insbesondere wegen der Weiterentwicklung des Schengener Informationssystems;

6. Adaptierung der Bestimmung über die erkennungsdienstliche Behandlung sowie

7. Legistische Anpassungen in der Bestimmung über die Sicherheitsakademie und in den Hauptstücken Ermittlungs- und Erkennungsdienst des SPG.

Alternativen:

Andere Wege zur Erreichung der angestrebten Ziele stehen nicht zur Verfügung.

Auswirkungen auf die Beschäftigung und den Wirtschaftsstandort Österreich:

Keine

Verhältnis zu Rechtsvorschriften der Europäischen Union:

Der Entwurf steht in keinem Widerspruch zu Rechtsvorschriften der Europäischen Union.

Besonderheiten des Normsetzungsverfahrens:

Keine.

Finanzielle Auswirkungen:

Für die Errichtung und den Betrieb der zentralen Analysedatei über mit beträchtlicher Strafe bedrohte Gewaltdelikte, insbesondere sexuell motivierte Straftaten werden laufende Ausgaben anfallen, die sich aus der Entrichtung einer jährlichen Lizenzgebühr, sowie aus zusätzlichem Personalbedarf für Dateneingabe, -pflege und -analyse zusammensetzen. Für die Vollziehung des neu gefassten § 53 Abs. 3a ist die einmalige Anschaffung eines IMSI-Catchers erforderlich. Hinsichtlich aller weiteren, insbesondere im Zusammenhang mit der Standortbestimmung im Rahmen der ersten allgemeinen Hilfeleistung anfallenden Ausgaben ist eine genaue Kostenberechnung in Ermangelung von Erfahrungswerten nicht möglich.

Erläuterungen

Allgemeiner Teil

1. Hauptgesichtspunkte des Entwurfes:

1.1. Allgemeines

Ziel dieses Gesetzesentwurfes ist es, ausdrückliche gesetzliche Ermächtigungen für Datenanwendungen der Sicherheitsbehörden für Zwecke der Vorbeugung, Verhinderung oder Verfolgung von Straftaten (vgl. § 17 Abs. 3 Z 5 DSG 2000) zu schaffen.

Mit der Übergangsbestimmung des § 61 Abs. 4 DSG 2000 im Verfassungsrang hat der Datenschutzgesetzgeber eine Bestimmung geschaffen, die es ermöglichen soll, bereichsspezifische Datenschutzbestimmungen und damit eine dem Art. 18 B-VG besser entsprechende Verrechtlichung des EDV-Einsatzes durch ausdrückliche gesetzliche Ermächtigungen über die zu verarbeitenden Datenarten, Betroffenenkreise und Empfänger der Daten zu schaffen.

Die notwendigen Arbeiten zur Anpassung des SPG an das Datenschutzgesetz 2000 wurden bereits insbesondere mit der SPG-Novelle 2002 in Angriff genommen.

Der Ablauf der verfassungsgesetzlichen Übergangsfrist des § 61 Abs. 4 DSG 2000 mit 31. Dezember 2007 für die Vornahme von Datenanwendungen, die für die in § 17 Abs. 3 DSG 2000 genannten Zweck notwendig sind, macht daher insbesondere eine Anpassung der Ermächtigung der Sicherheitsbehörden zur Ermittlung und Weiterverarbeitung von personenbezogenen Daten im SPG erforderlich.

1.2. Die Regelungen im SPG

Die Verwendung personenbezogener Daten im Rahmen des Ermittlungsdienstes ist in den §§ 53 ff. SPG geregelt. Lokale Datenanwendungen der Sicherheitsbehörden werden auf § 53 SPG gestützt. In Ergänzung zu dieser grundsätzlichen gesetzlichen Ermächtigung sollen im neuen § 53a die Datenanwendungen näher determiniert werden. Mit der Neuregelung werden insbesondere die bestehenden Einsatzleitsysteme, ein System zur Administration und Leitung von sicherheitspolizeilichen Großsätzen, die Analyseanwendungen und die für den Vollzug von Wegweisungen und Betretungsverboten erforderlichen lokalen Dateien näher beschrieben.

Ziel der auch international eingesetzten zentralen Anwendung zur Analyse von Gewaltverbrechen und Sexualdelikten ist die frühzeitige Erkennung von Serienzusammenhängen durch methodische Unterteilung, Bewertung und analytische Aufarbeitung des meist komplexen Tatgeschehens und der Vergleich mit bereits bekannten geklärten und ungeklärten Straftaten. Die Abfrageberechtigungen in diesem System sind auf besonders geschulte Bedienstete beschränkt, die in den betreffenden Deliktbereichen arbeiten. Zulässige Übermittlungen von Daten aus dieser Anwendung sind ausdrücklich geregelt. Die Fristen für die Löschung der personenbezogenen Daten sind nach Verhältnismäßigkeitserwägungen abgestuft.

Die Neuregelung der Bestimmung über die Auskunftserteilung durch Betreiber öffentlicher Telekommunikationsdienste nimmt eine Klarstellung zur Auskunft im Hinblick auf das TKG 2003 vor. Weiters sollen die Sicherheitsbehörden berechtigt sein, unter bestimmten Voraussetzungen Auskunft über Standortdaten zu verlangen. Hinsichtlich des Kostenersatzes wird auf die Tarife der Überwachungskostenverordnung – ÜKVO, BGBl II Nr. 322/2004, abgestellt.

Die weiteren vorgeschlagenen Regelungen betreffen erforderliche Anpassungen bei den Bestimmungen zur erkennungsdienstlichen Behandlung, bei der Wiederholung von Sicherheitsüberprüfungen, wenn Anhaltspunkte dafür vorliegen, dass die Vertrauenswürdigkeit eines bereits überprüften Menschen nicht mehr gegeben ist, bei der Ausstellung von Dokumenten im Rahmen einer Legende und bei der Organisation der Grundausbildung durch die Sicherheitsakademie. Weiters wird eine ausdrückliche Rechtsgrundlage für die Speicherung verlorener ausländischer Reisepässe und Passersätze in der Sachenfahndung getroffen.

1.3. Die Änderung des Grenzkontrollgesetzes betrifft nur eine Zitat Anpassung.

1.4. Die Änderung des Polizeikooperationsgesetzes soll es den Sicherheitsbehörden und den Organen des öffentlichen Sicherheitsdienstes insbesondere auch im Hinblick auf die Euro 2008 ermöglichen, Amtshilfe durch den Direktzugriff auf die von Sicherheitsorganisationen betriebenen gemeinsamen Informationssammlungen in Anspruch zu nehmen.

2. Kompetenzgrundlage:

Die vorgeschlagenen Regelungen stützen sich auf die Kompetenz des Bundes zur Gesetzgebung gemäß Art. 10 Abs. 1 Z 7 B-VG („Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit“).

3. Finanzielle Auswirkungen:

3.1. laufende Ausgaben:

VICLAS-Datenbank:

Lizenzgebühr pro Jahr: ca. €15.000,-- .

zusätzlicher Personalbedarf (für Dateneingabe, -pflege und -analyse):

| Anzahl | Wertigkeit | Jahreswert | Summe |
|--------|------------|-------------|-------------|
| 1 | A1/3 | €61.619,00 | €61.619,-- |
| 1 | E2a/7 | €50.116,00 | €50.116,-- |
| 3 | E2a/5 | €50.116,00 | €150.348,-- |
| 1 | A3 | €33.906,00 | €33.906,-- |
| 6 | | €195.757,00 | €295.989,-- |

| | |
|-------------------|-------------|
| Personalausgaben: | €295.989,-- |
|-------------------|-------------|

| | |
|-----------------------------------|-------------|
| zzgl. 20% Verwaltungsgemeinkosten | €59.198,-- |
| zzgl. 12% Sachkosten | €35.519,-- |
| zzgl. Raum-/Bürokosten | €12.196,-- |
| | €106.912,-- |

| | |
|---------------|-------------|
| Sachausgaben: | €106.912,-- |
|---------------|-------------|

| | |
|-----------------|-------------|
| Gesamtausgaben: | €402.901,-- |
|-----------------|-------------|

3.2. einmalige Ausgaben:

Neuankauf eines IMSI-Catchers: ca. €600.000,--.

Kosten für EPS-web:

Die erforderliche Software steht aufgrund der Kooperation mit dem Bayerischen Staatsministerium des Innern kostenlos zu Verfügung. Im BMI ist eine entsprechende Web-Farm zu errichten, dazu werden voraussichtlich zwei bis drei Web-Server zusätzlich angeschafft werden müssen. Die Kosten für einen Server belaufen sich auf ca. 10.000,-- €. Die Schulungen sollen mit Multiplikatoren noch vor der EM 2008 durchgeführt werden, dazu fallen ev. Gebühren nach der RGV an.

Besonderer Teil

Zu Artikel 1 (Änderung des Sicherheitspolizeigesetzes)

Zu Z 1 (§ 11 Abs. 2):

Mit dieser Änderung soll ermöglicht werden, dass im Rahmen der Bereitstellung der Grundausbildung einzelne Ausbildungen bzw. Teile davon auch durch externe Einrichtungen, wie z.B. Fachhochschulen oder Universitäten durchgeführt werden können. Die Terminologie wird damit auch an § 25 Abs. 2 BDG angepasst.

Zu Z 2 (§ 22 Abs. 3):

Unter dem Paragraphentitel „vorbeugender Schutz von Rechtsgütern“ ist in Abs. 3 normiert, dass den Sicherheitsbehörden - unbeschadet ihrer Aufgaben nach der Strafprozessordnung - die Klärung gefährlicher Angriffe (Identität des Verantwortlichen und maßgebliche Umstände) im Dienste der Sicherheitspolizei obliegt, soweit dies zur Vorbeugung weitere gefährlicher Angriffe durch den

Betreffenden notwendig ist und kein bestimmter Mensch der strafbaren Handlung verdächtig ist. Im Grundsatz geht der Gesetzgeber davon aus, dass von einem Täter solange Wiederholungsgefahr ausgeht und damit (auch) eine sicherheitspolizeiliche Aufgabe besteht, als seine Täterschaft unbekannt ist, die Tat also ungeklärt ist; außer, wenn wegen der Art (Umstände) der Tat durch den unbekanntes Täter mit weiteren gefährlichen Angriffen nicht zu rechnen ist. (Siehe auch Pkt. 5 des Allgemeinen Teils der RV 1991 und Dearing/Haller, Das österreichische Gewaltschutzgesetz, 105f.) Die Aufgabe besteht unbeschadet der Aufgaben nach der StPO, sodass die Ermittlungstätigkeit nach einem gefährlichen Angriff in vielen Fällen doppelfunktional sein wird. Die sicherheitspolizeiliche Klärungsaufgabe im Dienste der Vorbeugung endet gemäß § 22 Abs. 3 aber dann, wenn sie sich gegen eine bestimmte Person als Verdächtigen richtet. Grund für diese Abgrenzung sind die einem Verdächtigen zur Sicherung eines fairen Verfahrens nach Art. 6 EMRK zustehenden Verfahrensgarantien. Die Regelungen zur Zentralen Informationssammlung und zum Erkennungsdienst sind bereits nach der geltenden Rechtslage von dieser Einschränkung ausgenommen. Die mit dieser Novelle nunmehr ausdrücklich benannten, in lokalen und im Informationsverbund betriebenen sicherheitsbehördlichen Datenanwendungen, die (auch) dem vorbeugenden Rechtsgutschutz dienen, sind hier zu ergänzen.

Zu Z 3 (§ 53 Abs. 3a):

Diese Bestimmung berechtigt die Sicherheitsbehörden unter bestimmten Voraussetzungen, von Betreibern öffentlicher Kommunikationsdienste Auskunft über Namen, Anschrift und Teilnehmernummer zu einem bestimmten Anschluss zu verlangen. Die nunmehrige Hinzufügung der „sonstigen Kontaktinformation“ entspricht dem Wortlaut des § 92 Abs. 3 Z 3 lit. d des Telekommunikationsgesetzes 2003 (TKG 2003) und dient daher der terminologischen Anpassung an diese Regelung. Zur Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder zur Abwehr gefährlicher Angriffe sind die Sicherheitsbehörden darüber hinaus berechtigt, von den Betreibern Auskunft über die oben angeführten Stammdaten zu verlangen, und zwar auch dadurch, dass sie auf ein von einem bestimmten Anschluss aus geführtes Gespräch Bezug nehmen. Nach der geltenden Rechtslage muss auf den konkreten Zeitpunkt des Hilfe auslösenden Ereignisses abgestellt werden, was in der Praxis kaum möglich ist. Manche Telekommunikationsbetreiber vertreten die Ansicht, nur eine minutengenaue Zeitangabe berechtige sie zur Auskunftserteilung, eine Information, die Auskunftspersonen oft nicht geben können. Nunmehr wird vorgeschlagen, dass auf eine dem Anlass nach sachgerechte und verhältnismäßige Zeitspanne Bezug zu nehmen ist, damit die Betreiber in die Lage versetzt werden, ihre Auskunftspflicht zu erfüllen. Standortdaten unterliegen gemäß § 93 TKG 2003 dem Kommunikationsgeheimnis. Der Begriff des Kommunikationsgeheimnisses ist nicht ident zu setzen mit dem, was der historische Gesetzgeber zum Schutz des Fernmeldegeheimnisses mit Art. 10a StGG 1867 unter Richtervorbehalt gestellt hat. Wie auch der OGH in seiner Entscheidung vom 19.12.2005, 14 Os 103/05m, festgestellt hat, schützt das Fernmeldegeheimnis des Art. 10a StGG die Vertraulichkeit der Kommunikation auf dem Übertragungsweg, auf dem sich die Kommunikationspartner vor Zugriffen nicht ausreichend schützen können, nicht jedoch vor Eingriffen außerhalb davon. Vorgänge außerhalb des Übertragungsbereichs sind nicht Gegenstand des Fernmeldegeheimnisses. Solange Standortdaten nicht auf dem Übertragungsweg abgefangen werden sollen, sondern durch Erhebung beim Diensteanbieter gewonnen werden, liegt kein Eingriff in das Fernmeldegeheimnis des Art. 10a StGG vor. Nur Inhaltsdaten sind dem Fernmeldegeheimnis iSd Art. 10a StGG zuzurechnen, ihre Erhebung ist unter Gesetzes- und Richtervorbehalt zu stellen (vgl. dazu Wessely, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht, ÖJZ 1999, 491). Hinkünftig sollen Betreiber auch dann Standortdaten eines Mobiltelefons bekannt geben können, wenn zuvor kein Notruf einer hilfsbedürftigen Person beim Betreiber eines Notrufdienstes eingelangt ist (vgl. § 98 TKG 2003). Beispielsweise sei hier der in der Praxis immer wieder vorkommende Fall des am Abend nicht zurückgekehrten Tourengegers oder Wanderers genannt, der zwar ein Mobiltelefon mitführt, aber infolge eines Unfalls selbst zu telefonieren nicht mehr imstande ist. Darüber hinaus sollen die Sicherheitsbehörden dann, wenn eine gegenwärtige Gefahr für das Leben oder die Gesundheit eines Menschen vorliegt, dazu berechtigt sein, von den Betreibern Auskunft über Standortdaten und die Mobilteilnehmerkennung (IMSI) zu verlangen. Die Mobilteilnehmerkennung ist deshalb nötig, damit erforderlichenfalls technische Mittel zur Lokalisierung einer von einem Menschen mitgeführten Endeinrichtung zum Einsatz gebracht werden können. Es muss sich um eine aktuelle Gefahr handeln, die im Lichte der Verhältnismäßigkeit der Maßnahme auf andere Art und Weise nicht oder nicht rasch genug abgewendet werden kann.

Zu Z 4 und 5 (§ 53a):

Zu Abs. 1: Die Sicherheitsbehörden betreiben derzeit auf § 53 SPG gestützte und beim Datenverarbeitungsregister gemeldete, lokale Datenanwendungen (z.B. Einsatzleitsysteme), die zur Koordination und Dokumentation von Amtshandlungen aber auch zur Erfüllung der Aufgaben in den Bereichen der ersten allgemeinen Hilfeleistungspflicht (§ 19), dem vorbeugenden Schutz von

Rechtsgütern (§ 22) und der Fahndung (§ 24) dienen. Nunmehr sollen für diese Anwendungen ausreichend determinierte Grundlagen im Sinne des Datenschutzgesetzes geschaffen werden, einschließlich der Benennung von Betroffenenkreisen und Datenarten. Aber auch bei der Leitung und Koordination von sprengelübergreifenden Einsätzen, insbesondere bei Großeinsätzen, großen Schadensereignissen und Katastropheneinsätzen, Sonderlagen und Sofortfahndungen soll ein Einsatz-Protokoll-System (EPS-web) zur Anwendung kommen, das erforderlichenfalls als Informationsverbundsystem betrieben werden kann. Im Besonderen in Hinblick auf die EURO 08 ist die Installierung eines solchen Systems notwendig. Die Praxistauglichkeit des Systems wurde während der Fußball WM 06 in Deutschland im Echteininsatz erprobt und festgestellt. Für die Führung einer Datenanwendung im Informationsverbundsystem bei sprengelübergreifenden Einsätzen gilt das zu Abs. 5 und 6 Gesagte.

Zu Abs. 2: Mit der SPG - Novelle 2002, BGBl I Nr. 104/2002, wurde § 53 Abs. 1 Z 4 SPG dahingehend erweitert, dass die Verarbeitung personenbezogener Daten auch für die Vorbeugung gefährlicher Angriffe mittels Kriminalitätsanalyse zulässig ist, wenn nach der Art des Angriffes eine wiederholte Begehung wahrscheinlich ist. Es wird zwischen strategischer Analyse, die in der Erstellung von Lagebildern über Stand, Ursachen und Entwicklungstendenzen in bestimmten Kriminalitätsbereichen besteht, und der operativen Analyse unterschieden. Bei operativen Analysen werden personenbezogene Daten über gefährliche Angriffe mit umfangreichen Informationen zum Tathergang verarbeitet, um durch Vergleich von Straftaten mit ähnlichem modus operandi Serientaten zu erkennen und in komplexen Fällen neue Ermittlungsansätze zu finden oder Strukturen krimineller Verbindungen sichtbar zu machen. Der Mehrwert der Analyse liegt darin, dass aus dem Zusammenführen bruchstückhafter Informationen neue Erkenntnisse gewonnen werden können, die es erlauben, eine Gefahr zu erkennen und auf sie zu reagieren, anstatt erst im Nachhinein einzuschreiten, wenn sich eine zunächst unbekannte sicherheitspolizeiliche Gefahr realisiert hat. Kriminalitätsanalyse erweist sich damit als Instrumentarium zur Erfüllung der Aufgabe des vorbeugenden Schutzes von Rechtsgütern.

Die besondere datenschutzrechtliche Sensibilität von (operativer) Kriminalitätsanalyse liegt darin, dass nicht nur Informationen über Täter, Verdächtige oder Gefährder verarbeitet werden. Die Betroffenenkreise sind neben Verdächtigen auch Begleitpersonen, Kontaktpersonen, Zeugen, Informanten und Opfer. Es wird daher für diese international gebräuchliche und anerkannte Methode zur sicherheitspolizeilichen Aufgabenerfüllung eine den Analysedateien von Europol nachgebildete gesetzliche Grundlage geschaffen. (Siehe dazu den Rechtsakt des Rates vom 3. November 1998 über die Durchführungsbestimmungen für die von Europol geführten Arbeitsdateien zu Analyse Zwecken, ABl. 1999 C 26/01). Für Datenanwendungen, die nicht im Informationsverbund geführt werden, gelten für Übermittlung und Löschung die allgemeinen Bestimmungen der §§ 56 und 63, andernfalls gilt das zu Abs. 5 und 6 Gesagte.

Zu Abs. 3: Schon auf Basis der geltenden Rechtslage werden für den Vollzug des Gewaltschutzgesetzes Wegweisungen und Betretungsverbote im Sinne des § 38a SPG, gestützt auf § 53 SPG, in lokalen Evidenzen jener Sicherheitsbehörde gespeichert, in deren Sprengel derartige Anordnungen erlassen wurden, damit beim Einschreiten - vor allem bei der zu erstellenden Gefährlichkeitsprognose - rasche und spezifische Informationen vorliegen, um verhältnismäßig vorgehen zu können. Bei den zum Gefährder gespeicherten Datenarten handelt es sich um jene Daten, die für eine eindeutige Identifizierung des Gefährders und für die Erstellung der Gefährlichkeitsprognose im Einzelfall erforderlich sind. Darüber hinaus ist die Speicherung von Daten über Grund, Umfang und Art der Maßnahme, frühere Maßnahmen und Vormerkungen, Verstöße gegen Maßnahmen und allfällige Strafen, Erreichbarkeitsdaten und Verwaltungsdaten zulässig. Zu gefährdeten Personen werden nur eingeschränkt personenbezogene Daten verarbeitet. Mit der SPG-Novelle 2004 wurde in § 58c die Ermächtigung zur Führung einer im Informationsverbundsystem betriebenen zentralen Gewaltschutzdatei geschaffen, in der aus datenschutzrechtlichen Gründen auf die Verarbeitung von Opfernamen verzichtet wurde, bloß eine einjährige Speicherdauer und nur eingeschränkt Übermittlungsempfänger vorgesehen sind. Es ist daher notwendig, auch weiterhin lokale Evidenzen für den Vollzug des Gewaltschutzgesetzes zu führen.

Zu Abs. 4: Darüber hinaus ist es für den Vollzug von Wegweisungen und Betretungsverböten in Schutzzonen gemäß § 36a SPG erforderlich, Daten zu Personen zu verarbeiten, gegen die eine derartige Maßnahme verfügt wurde. Die Informationen werden benötigt, damit die Sicherheitsbehörde die Anordnung eines Betretungsverbotes gemäß § 36a Abs. 4 überprüfen und Verstöße gegen die Anordnung gemäß § 84 Abs. 1 Z 4 ahnden kann.

Zu Abs. 5 und 6: Die oben beschriebenen Einsatzprotokollierungssysteme müssen, wenn es sich um sprengelübergreifende Ereignisse oder Einsätze handelt wie etwa die Euro 2008 oder ein am Flughafen Schwechat (NÖ) eintreffender Staatsgast, auch im Informationsverbundsystem (§ 4 Z 13 DSGVO 2000) geführt werden. Dasselbe gilt für Analysen im Sinne des Abs. 2, die von zwei oder mehreren

Sicherheitsbehörden bei regionalen Kriminalitätsphänomenen oder in Form von österreichweiten Lagebildern erfolgen. Es sind besondere Lösungsfristen und bei Informationsverbundsystemen nach Abs. 2 auch die Übermittlungsempfänger ausdrücklich ausgewiesen.

Durch die Einfügung des neuen § 53a wird der bisherige § 53a zu § 53b.

Zu Z 6 und 7 (§ 54a Abs. 1 und 2):

In § 54a Abs. 1 sind die ausstellenden Behörden für eine Legende, nämlich die Bundesbehörden, Behörden der mittelbaren Bundesverwaltung und der Bürgermeister genannt. Die Sozialversicherungsträger und andere Selbstverwaltungskörper wie z.B. Kammern sind nicht unter die genannten Behörden zu subsumieren. Für den vorbeugenden Schutz von Menschen gem. § 22 Abs. 1 Z 5 und zum Zwecke verdeckter Ermittlungen (§ 54 Abs. 3) ist es absolut erforderlich, dass auch Selbstverwaltungskörper für diese Zwecke Urkunden ausstellen dürfen. Insbesondere die e-card ist für verdeckte Ermittler und legendierte Personen im Zeugenschutzprogramm unerlässlich, weshalb eine entsprechende Ergänzung vorgeschlagen wird.

Urkunden zum Schutz von Menschen nach § 22 Abs. 1 Z 5 (Zeugen und allenfalls deren Angehörige) sind spätestens nach drei Jahren einzuziehen. Da Zeugenschutzmaßnahmen nur im Bereich der organisierten Kriminalität und der Schwerstkriminalität zur Anwendung kommen, ist regelmäßig von mehreren Jahren erhöhter Gefährdungslage von Schutzpersonen auszugehen. Daher hat die Frist von drei Jahren zu entfallen und es soll künftig im Einzelfall auf den zu erwartenden Gefährdungszeitraum des Betroffenen abgestellt werden.

Zu Z 8 (§ 55a Abs. 4):

Es soll von den starren Fristen hinsichtlich der Wiederholung der Sicherheitsüberprüfungen insofern abgegangen werden, als bei Vorliegen von Anhaltspunkten, die Zweifel an der Vertrauenswürdigkeit des Betroffenen rechtfertigen, auch schon vorher mit einer weiteren Überprüfung reagiert werden kann. Diese Ergänzung ist in Anlehnung an § 134a Abs. 4 Luftfahrtgesetz vorgenommen worden.

Zu Z 9 (§ 57 Abs. 1 Z 12):

Art. 100 Abs. 3 lit. e des Schengener Durchführungsübereinkommens (SDÜ) sieht die Ausschreibung von gestohlenen und verlorenen Dokumenten im Schengener Informationssystem vor. Innerstaatlich stellt das Passgesetz (§ 22b) die Grundlage für die Ausschreibung von verlorenen und entforderten österreichischen Reisepässen und Passersätzen in der Sachenfahndung dar und § 57 Abs. 1 Z 12 SPG für die Ausschreibung von entforderten ausländischen Reisepässen und Passersätzen. Es fehlt aber bislang die ausdrückliche Rechtsgrundlage für die Speicherung verlorener ausländischer Reisepässe und Passersätze in der Sachenfahndung, die nunmehr vorgeschlagen wird.

Zu Z 10 (§ 57 Abs. 2):

Diese Regelung enthält die Grundlage für Sachinformationssysteme und insbesondere für die automationsunterstützte Sachenfahndung. Die Sicherheitsbehörden werden ermächtigt, Sachen oder rechterhebliche Tatsachen mitsamt Identitätsdaten (Namen, Anschrift...) von Menschen zu speichern, falls dies erforderlich ist, wobei der Zweck in der Speicherung von Sachdaten liegt. Eine Abfrage nach den Identitätsdaten ist bislang ausdrücklich ausgeschlossen. Hinsichtlich österreichischer Reisepässe (inkl. Fremden und Konventionsreisepässen, die nach dem Fremdenpolizeigesetz ausgestellt wurden) sind mit der Passgesetznovelle 2006 spezialgesetzliche Regelungen (§§ 22a und 22b PassG) geschaffen worden, die eine Abfrage auch nach dem Namen, Geburtsdatum und anderen personenbezogenen Daten ermöglichen. Da die betroffenen Personen die Seriennummern von gestohlenen Gegenständen oder die Nummern von gestohlenen oder verlorenen ausländischen Dokumenten oftmals nicht wissen und diese Nummern auch nicht ohne weiteres in Erfahrung gebracht werden können, ist eine Ausweitung der Abfragemöglichkeit aus der Sachenfahndung unbedingt notwendig. Im Übrigen speichern viele Schengenmitgliedsstaaten gestohlene Dokumente im SIS nur mit den Daten der geschädigten Person, aber ohne Dokumentennummer. Daher wird vorgeschlagen, den letzten Satz in § 57 Abs. 2 SPG zu streichen.

Zu Z 11 und 12 (§ 58 Abs. 1 Z 8 und 11):

In der Verarbeitungsermächtigung des § 57 Abs. 1 Z 10 entfiel mit der SPG - Novelle 2002 die Zustimmung des Betroffenen zur Verarbeitung seiner Daten, aber die Adaptierung der korrespondierenden Lösungsbestimmung ist unterblieben, was nunmehr nachgeholt wird.

Für entfremdete oder verlorene ausländische Pässe (die nicht unter das Passgesetz fallen) ist aufgrund eines redaktionellen Versehens in § 58 Abs. 1 keine Regelung für die Sperre bzw. Lösungs der Daten vorgesehen. Es ist daher in § 58 Abs. 1 die fehlende Sperr/Lösungsverpflichtung aufzunehmen. Da bei ausländischen Pässen die Gültigkeitsdauer oft nicht eruierbar ist, muss eine allgemeine Formulierung gewählt werden.

Zu Z 13 (§ 58d):

Bei dieser zentralen Anwendung zur Analyse von Gewaltverbrechen und sexuell motivierten strafbaren Handlungen handelt es sich um eine Datenanwendung, die auf dem in Kanada entwickelten System „VICLAS“ (Violent Crime Linkage Analysis System) beruht und dazu dient, schwere Gewaltdelikte und Sexualstraftaten, bei denen Grund zur Annahme erhöhter Wiederholungsgefahr besteht, zu analysieren und gegebenenfalls Serienstraftaten auch überregional effektiv und schnell zusammenzuführen. Dies geschieht durch Analyse der vorhandenen Täter- und Opferinformationen, insbesondere dem Täterverhalten und dem Modus operandi sowie anhand forensischer Daten. Das System wird auch in verschiedenen Ländern der europäischen Union wie in Deutschland, Dänemark, Frankreich, Großbritannien, Niederlande und Schweden eingesetzt. Aufgrund einer standardisierten Fallbeschreibung sollen im Wesentlichen die festgestellten Verhaltensmuster der bekannten oder unbekanntem Straftäter bei ihrer Tatusführung abgebildet werden. Darauf aufbauend können dann geschulte polizeiliche Fallanalytiker mit gezielten Recherchen im System Gemeinsamkeiten zu bereits abgespeicherten Fällen herausfiltern (Tat-Tat-Zusammenhänge). In geeigneten Fällen wird damit die so genannte „Handschrift“ eines Rückfalltäters identifiziert, was zum Erkennen weiterer Tat-Täter-Zusammenhänge führen kann und somit ein wichtiges Hilfsmittel bei der Ermittlungstätigkeit und Verhinderung von Straftaten darstellt. Es können auf diese Weise Präventionsansätze in Bezug auf Wiederholungs- oder Rückfalltäter gewonnen werden, und die Beobachtung der Kriminalitätsentwicklung in verschiedenen Deliktsfeldern der Gewaltkriminalität wird ermöglicht. Produkte von Fallanalysen können sein: Gefährdungsanalysen, Gefährlichkeitseinstufungen von Tätern, Eingrenzungen des Täterwohnortes und Täterprofilierungen bei Tötungsdelikten und sexuell motivierten Gewaltdelikten.

Zu Z 14 und 15 (§ 65 Abs. 1 und 5):

Mit der Änderung des § 65 Abs. 1 durch die SPG Novelle 2002 (vgl. die entsprechenden EB zur RV, 1138 BlgNR, XXI.GP) sollte erreicht werden, dass eine erkennungsdienstliche Behandlung bei Verdacht einer Einzelstraftat nicht nur dann zulässig ist, wenn beim Betroffenen konkrete Anhaltspunkte für eine Wiederholungsgefahr oder der Gefahr der Begehung anderer gefährlicher Angriffe bestehen, sondern auch wenn eine für bestimmte Deliktsbereiche typische (statistische) Rückfallsgefahr vorliegt. Die Art des begangenen Delikts oder konkrete Umstände bei der Tatbegehung sollten Maßstab für die Beurteilung der Wahrscheinlichkeit der Begehung weiterer gefährlicher Angriffe darstellen. Zu dieser Fassung des § 65 Abs.1 hat der Verwaltungsgerichtshof in mehreren Erkenntnissen (etwa VwGH vom 16. Juli 2003, 2002/01/0592 oder VwGH vom 7. Oktober 2003, 2003/01/0191) festgehalten, dass die aktuelle Textierung des § 65 - insbesondere auch wegen des unverändert gebliebenen § 65 Abs. 5 letzter Satz - eine rein abstrakte Betrachtungsweise verbiete. Für die Zulässigkeit einer erkennungsdienstlichen Behandlung nach § 65 Abs. 1 sei es immer erforderlich, eine konkrete fallbezogene Prognose zu treffen, bei der sich die Behörde mit den Einzelheiten des von ihr im Sinne der ersten Voraussetzung des § 65 Abs. 1 angenommenen Verdacht, mit den daraus unter Bedachtnahme auf die Persönlichkeit des Betroffenen zu ziehenden Schlüssen hinsichtlich der Wahrscheinlichkeit, dass er gefährliche Angriffe begehen werde, und mit der Frage des daraus abzuleitenden Erfordernisses einer „Vorbeugung“ durch eine erkennungsdienstliche Behandlung auseinander zu setzen habe. Im Rahmen dieser Überlegungen komme es „auch“ auf die Art des Delikts an. § 65 Abs. 5 zweiter Satz bezweckt, dass dem Betroffenen der vorbeugende Charakter der erkennungsdienstlichen Behandlung (entsprechend der sicherheitspolizeilichen Aufgabenstellung des § 22 Abs. 2) nochmals vor Augen geführt werden soll. Da dieser Satz für die Frage, ob die Maßnahme zur Vorbeugung künftiger gefährlicher Angriffe des Betroffenen erforderlich scheint, keinen Mehrwert bringt, kann er gestrichen werden. Darüber hinaus soll durch die Neufassung von § 65 Abs. 1 klargestellt werden, dass – abgesehen von der Tatbegehung im Rahmen einer kriminellen Verbindung – konkrete Anhaltspunkte für die Wahrscheinlichkeit der Wiederholung oder Begehung anderer gefährlicher Angriffe entweder in der Person des Betroffenen selbst oder in der Art oder Ausführung der Tat liegen können. Es genügt im zweiten Fall eine abstrakte Form von Wahrscheinlichkeit, die an der verwirklichten Tat anknüpft und den Schluss rechtfertigt, dass die Tat nach der allgemeinen Lebenserfahrung kein Einzelfall bleiben wird.

Zu Z 16 (§ 65 Abs. 6):

Es ist notwendig, in der erkennungsdienstlichen Evidenz auch Staatsangehörigkeit, Dokumentendaten und Gefährlichkeitshinweise aufzunehmen. Dokumentendaten sind im Rahmen von Personalfeststellungen notwendig und Gefährlichkeitshinweise zum Schutz der Beamten. Diese Ergänzungen werden in Anlehnung an die in § 102 Abs. 1 Fremdenpolizeigesetz 2005 aufgezählten Datenarten vorgenommen.

Zu Z 17 und 18 (§ 75 Abs. 1):

In der Norm über die Zentrale erkennungsdienstliche Evidenz fehlt infolge eines redaktionellen Versehens die ausdrückliche Nennung der gemäß § 67 ermittelten DNA – Daten.

In einigen Materiengesetzen wie z.B. § 102 FPG, § 124 Abs. 5 Strafprozess-Reformgesetz oder § 131 Abs. 7 StVG sind Übermittlungen von erkennungsdienstlichen Daten für Zwecke der Sicherheitspolizei vorgesehen. Im SPG fehlt aber die entsprechende ausdrückliche „Weiterverarbeitungsermächtigung“, da in § 75 nur von Daten gesprochen wird, die die Sicherheitsbehörden selbst nach den Ermächtigungen des SPG ermittelt haben. Daher wird eine Ergänzung aufgenommen, wonach die entsprechenden personenbezogene Daten, die nach anderen Materien zulässigerweise er- und übermittelt wurden, für Zwecke der Sicherheitspolizei weiterverarbeitet werden dürfen.

Zu Z 19 (§ 94 Abs. 23):

Es handelt sich um die In-Kraft-Tretens-Bestimmung.

Zu Z 20 (§ 96 Abs. 2):

Die historisch erforderlich gewesene Bestimmung kann im Hinblick auf die Verlegung der Sicherheitsdirektion für das Bundesland NÖ in die Landeshauptstadt St. Pölten mangels Anwendungsbereich entfallen.

Zu Z 21:

Anpassung des Inhaltsverzeichnisses.

Zu Artikel 2 (Änderung des Grenzkontrollgesetzes):

Es handelt sich um die Anpassung eines Zitates, das durch die Novelle zum Sicherheitspolizeigesetz, BGBl. Nr. 158/2005, die eine Neuregelung der Bestimmungen über den Rechtsschutzbeauftragten im 3. Abschnitt des sechsten Teiles des SPG brachte, erforderlich geworden ist.

Zu Artikel 3 (Änderung des Polizeikooperationsgesetzes):

Durch die vorgeschlagene Regelung soll es den Sicherheitsbehörden sowie den ihnen beigegebenen, zugeteilten oder unterstellten Organen des öffentlichen Sicherheitsdienstes (insbesondere im Hinblick auf die Euro 2008) ermöglicht werden, Amtshilfe durch den Direktzugriff auf die von Sicherheitsorganisationen betriebenen gemeinsamen Informationssammlungen in Anspruch zu nehmen. So sollen die bei Interpol betriebenen Datenbanken über „gestohlene und verlorene Reisedokumente“ und „gestohlene Kraftfahrzeuge“ direkt den Exekutivorganen vor Ort – mithin ohne Befassung des Bundesministers für Inneres als oberste Sicherheitsbehörde – in der Form zugänglich gemacht werden, dass ein Hit – No Hit-System (vergleichbar dem System im Prümer Vertrag zur Abfrage von DNA-Daten) Abfragen an das Generalsekretariat über die von den Mitgliedsländern zur Verfügung gestellten Daten ermöglicht. Weiters wird in § 8 eine notwendige Anpassung eines Zitates vorgenommen.