

## 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. Nr.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. Ergänzung der Auskunftspflicht durch Betreiber öffentlicher Telekommunikationsdienste hinsichtlich von Standortdaten;

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 einem Personalbedarf für Dateneingabe, -pflege und -analyse zusammensetzen. Für die Vollziehung des neuen § 53 Abs. 3b 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 Großeinsätzen, 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 betrifft die Beauskunftung von Standortdaten zur Abwehr einer gegenwärtigen Gefahr. Hinsichtlich des Kostenersatzes wird auf die Überwachungskostenverordnung – ÜKVO, BGBl II Nr. 322/2004, abgestellt.

Die Kontrolle durch den Rechtsschutzbeauftragten wird ausgeweitet.

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,-- .

Personalbedarf (für Dateneingabe, -pflege und -analyse): voraussichtlich 6 Bedienstete

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.

Die angeführten Mehrbedarfe im Sach- und Personalbereich werden im Rahmen der bestehenden Budgets und Stellenpläne des Kapitels 11 abgedeckt.

**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 (§ 15b Abs. 1):**

Der Vorsitzende des Menschenrechtsbeirates (sein Vertreter) soll für die Erfüllung seiner Aufgaben eine Entschädigung erhalten, deren Höhe der Bundesminister für Inneres in der Menschenrechtsbeirats-Geschäftsordnung (MRB-GO), BGBl. II Nr. 395/1999 idF BGBl. II Nr. 260/2004, festsetzt.

**Zu Z 3 (§ 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 Betroffenen 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 doppelunktional 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 4 (§ 53 Abs. 3a):**

Zur Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder zur Abwehr gefährlicher Angriffe ist es für die Begründung der Auskunftspflicht ausreichend, den zu identifizierenden Anschluss durch einen bestimmten Zeitpunkt und die passive Teilnehmernummer, also jene des Empfängers, zu präzisieren. Nach der geltenden Rechtslage wird auf den „Zeitpunkt“ des Anrufes abgestellt, was in der Praxis manchmal nicht möglich ist, weil Auskunftspersonen keine minuten- oder gar sekundengenaue Zeitangabe machen können. Nunmehr wird vorgeschlagen, dass auf eine möglichst genaue Zeitspanne Bezug zu nehmen ist, die aus Gründen der Verhältnismäßigkeit nicht mehr als eine Stunde betragen darf.

**Zu Z 5 und 6 (§ 53 Abs. 3b und 3c):**

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 Tourengers 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 Daten einer von diesem Menschen mitgeführten Endeinrichtung zur Feststellung seines Standorts zu verlangen und erforderlichenfalls technische Mittel zu seiner Lokalisierung zum Einsatz zu bringen. 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. In Anlehnung an § 98 Telekommunikationsgesetz 2003 wird ausdrücklich festgehalten, dass die Sicherheitsbehörde die Verantwortung für die rechtliche Zulässigkeit der Anfrage übernimmt. Aus Gründen der Nachvollziehbarkeit ist dem Betreiber möglichst rasch die Dokumentation der Anfrage zu übermitteln. Der Rechtsschutzbeauftragte ist über derartige Auskunftsbegehren zu informieren.

Durch die Einfügung des neuen § 53 Abs. 3b wird der bisherige § 53 Abs. 3b zu § 53 Abs. 3c.

**Zu Z 7 und 8 (§ 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 zu Fahndungszwecken (Alarmfahndungen) 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, Katastropheneinsätzen und sonstigen Sonderlagen 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 Echteinsatz 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. Der Status von Kontakt- oder Begleitpersonen ist möglichst rasch abzuklären. Wenn sich aufgrund weiterer Ermittlungen herausstellt, dass eine Speicherung der Person nach einer anderen Ziffer, etwa als Verdächtiger gemäß Z 1 mangels Erhärtung des Verdachts, nicht zulässig ist, sind die Daten zu löschen. Unter zeugenschutzrelevanten Daten sind etwa Informationen über die schutzgewährende Stelle, eine allfällige neue Identität oder die Möglichkeiten zur Aussage vor Gericht zu verstehen. 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. Datenanwendungen, die auf Abs. 2 (und 6) gestützt werden, dürfen in Hinkunft nur nach Befassung des Rechtsschutzbeauftragten gemäß § 91c Abs. 2 geführt werden.

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 Betretungsverboten 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 DSG 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 9 und 10 (§ 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 nach der geltenden Rechtslage 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 11 (§ 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 12 (§ 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 entfremdeten österreichischen Reisepässen und Passersätzen in der Sachenfahndung dar und § 57 Abs. 1 Z 12 SPG für die Ausschreibung von entfremdeten 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 13 (§ 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 14 und 15 (§ 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. Die Adaptierung der korrespondierenden Löschungsbestimmung 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. Löschung der Daten vorgesehen. Es ist daher in § 58 Abs. 1 die fehlende Sperr/Löschungsverpflichtung aufzunehmen. Da bei ausländischen Pässen die Gültigkeitsdauer oft nicht eruierbar ist, muss eine allgemeine Formulierung gewählt werden.

**Zu Z 16 (§ 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 zusammenführen zu können. 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 unbekanntes Straftäter bei ihrer Tatausführung 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 Täters 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.

In § 58d Abs. 1 Z 3 soll hinsichtlich der Opfer die Verarbeitung der Datenart „Wohnanschriften“ bei Hausanlagen mit mehreren Wohnungen ohne Türbezeichnung, bei Einfamilienhäusern und ähnlichen Häusern ohne Hausnummernbezeichnung erfolgen.

**Zu Z 17 und 18 (§ 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 19 (§ 65 Abs. 6):**

Es ist notwendig, in der erkennungsdienstlichen Evidenz auch Staatangehörigkeit, Dokumentendaten und Gefährlichkeitshinweise aufzunehmen. Dokumentendaten sind im Rahmen von Personenfeststellungen 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 20 und 21 (§ 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 22 und 23 (§ 91c Abs. 1 und 2):**

Zur Verbesserung des Rechtsschutzes ist nach der Ermittlung von Standortdaten gemäß § 53 Abs. 3b eine Information des Rechtsschutzbeauftragten und bei der Führung von Datenanwendungen nach § 53a Abs. 2 und 6 - das bedeutet bei lokal und im Informationsverbund geführten Analyseanwendungen - eine Vorabkontrolle vorgesehen.

**Zu Z 24 (§ 94 Abs. 23):**

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

**Zu Z 25 (§ 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 26:**

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.

## Textgegenüberstellung

## Geltende Fassung

## Vorgeschlagene Fassung

## Artikel I

## Änderung des Sicherheitspolizeigesetzes

§ 11. (1) ...

(2) Der Sicherheitsakademie obliegt die Durchführung der Grundausbildung und der Ausbildung von Lehr- und Führungskräften für die in Abs. 1 genannten Bediensteten. ...

(3) bis (7) ...

§ 15b. (1) Die Mitglieder und Ersatzmitglieder des Menschenrechtsbeirates werden mit deren Zustimmung vom Bundesminister für Inneres für eine Funktionsperiode von drei Jahren bestellt; sie üben ihre Funktion ehrenamtlich aus. Diese endet durch Ablauf der Funktionsperiode, durch Abberufung seitens des Bundesministers für Inneres oder durch Verzicht oder Tod des Mitglieds.

(2) ...

§ 22. (1) bis (2) ...

(3) ... die §§ 57 und 58 sowie die Bestimmungen über den Erkennungsdienst bleiben jedoch unberührt.

(4) ...

§ 53. (1) bis (3) ...

(3a) Die Sicherheitsbehörden sind berechtigt, von den Betreibern öffentlicher Telekommunikationsdienste Auskunft über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses zu verlangen, wenn sie diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben benötigen. Die Bezeichnung dieses Anschlusses kann für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder die Abwehr gefährlicher Angriffe auch durch Bezugnahme auf ein von diesem Anschluß geführtes Gespräch durch Bezeichnung des Zeitpunktes und der passiven Teilnehmernummer erfolgen. Die ersuchte Stelle ist verpflichtet, die

§ 11. (1) ...

(2) Der Sicherheitsakademie obliegt die Bereitstellung der Grundausbildung und der Ausbildung von Lehr- und Führungskräften für die in Abs. 1 genannten Bediensteten. ...

(3) bis (7) ...

§ 15b. (1) Die Mitglieder und Ersatzmitglieder des Menschenrechtsbeirates werden mit deren Zustimmung vom Bundesminister für Inneres für eine Funktionsperiode von drei Jahren bestellt; sie üben ihre Funktion ehrenamtlich aus. Dem Vorsitzenden und dem Vertreter des Vorsitzenden gebührt für die Erfüllung ihrer Aufgaben eine Entschädigung, deren Höhe in der Verordnung gemäß § 15c Abs. 6 festgelegt wird. Die Funktion endet mit Ablauf der Funktionsperiode, durch Abberufung seitens des Bundesministers für Inneres oder durch Verzicht oder Tod des Mitglieds.

(2) ...

§ 22. (1) bis (2) ...

(3) ... die §§ 53 Abs. 1, 53 a Abs. 2 bis 4 und 6, 57, 58 und 58a bis d, sowie die Bestimmungen über den Erkennungsdienst bleiben jedoch unberührt.

(4) ...

§ 53. (1) bis (3) ...

(3a) Die Sicherheitsbehörden sind berechtigt, von den Betreibern öffentlicher Telekommunikationsdienste Auskunft über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses zu verlangen, wenn sie diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben benötigen. Die Bezeichnung dieses Anschlusses kann für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder die Abwehr gefährlicher Angriffe auch durch Bezugnahme auf ein von diesem Anschluß geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmernummer erfolgen. Die ersuchte Stelle ist

**Geltende Fassung**

Auskunft unverzüglich und kostenlos zu erteilen.

**Vorgeschlagene Fassung**

verpflichtet, die Auskunft unverzüglich und kostenlos zu erteilen.

(3b) Ist auf Grund bestimmter Tatsachen anzunehmen, dass eine gegenwärtige Gefahr für das Leben oder die Gesundheit eines Menschen besteht, sind die Sicherheitsbehörden zur Hilfeleistung oder Abwehr dieser Gefahr darüber hinaus berechtigt, von den Betreibern im Mobilfunkbereich Auskunft über Standortdaten der von dem gefährdeten Menschen mitgeführten Endeinrichtung zu verlangen sowie technische Mittel zur ihrer Lokalisierung zum Einsatz zu bringen. Die Sicherheitsbehörde trifft die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens, dessen Dokumentation dem Betreiber unverzüglich, spätestens innerhalb von 24 Stunden nachzureichen ist. Die ersuchte Stelle ist verpflichtet, die Auskünfte unverzüglich und gegen Ersatz der Kosten nach § 7 Z 4 der Überwachungskostenverordnung – ÜKVO, BGBl. II Nr. 322/2004, zu erteilen.

(3b) ...

(4) und (5) ...

**Zulässigkeit der Verarbeitung durch Fundbehörden**

§ 53a. ...

(3c) ...

(4) und (5) ...

**Zulässigkeit der Verarbeitung durch Fundbehörden**

§ 53b. ...

**Datenanwendungen der Sicherheitsbehörden**

§ 53a. (1) Die Sicherheitsbehörden dürfen für die Leitung, Administration und Koordination von Einsätzen, insbesondere von sicherheitspolizeilichen Schwerepunktionen, Fahndungen oder ordnungsdienstlichen Anlässen sowie für den Personen- und Objektschutz und die Erfüllung der ersten allgemeinen Hilfeleistungspflicht Daten über natürliche und juristische Personen sowie Sachen und Gebäude verarbeiten. Es dürfen zu Personen, die von einer Amtshandlung betroffen sind, zu Einbringern von Anträgen, Anzeigen oder sonstigen Mitteilungen, zu gefährdeten Personen oder Institutionen und zu Zeugen und anderen Personen, die im Zuge einer Amtshandlung zu verständig sind, die erforderlichen Identifikations- und Erreichbarkeitsdaten verarbeitet werden sowie zu gefahndeten Personen auch Lichtbild und eine allenfalls vorhandene Beschreibung des Aussehens und ihrer Kleidung. Darüber hinaus dürfen die erforderlichen Sachdaten einschließlich KFZ - Kennzeichen, Angaben zu Zeit, Ort, Grund und Art des Einschreitens sowie Verwaltungsdaten verarbeitet werden.

(2) Die Sicherheitsbehörden dürfen für die Abwehr krimineller Verbindungen oder gefährlicher Angriffe sowie zur Vorbeugung gefährlicher Angriffe, wenn

### Geltende Fassung

### Vorgeschlagene Fassung

nach der Art des Angriffs eine wiederholte Begehung wahrscheinlich ist, mittels operativer oder strategischer Analyse

1. zu Verdächtigen
  - a) Namen,
  - b) frühere Namen,
  - c) Aliasdaten,
  - d) Namen der Eltern,
  - e) Geschlecht,
  - f) Geburtsdatum und Ort,
  - g) Staatsangehörigkeit,
  - h) Wohnanschrift/Aufenthalt,
  - i) sonstige zur Personenbeschreibung erforderliche Daten,
  - j) Dokumentendaten,
  - k) Beruf und Qualifikation/Beschäftigung/Lebensverhältnisse,
  - l) erkennungsdienstliche Daten,
  - m) Informationen über wirtschaftliche und finanzielle Verhältnisse einschließlich damit im Zusammenhang stehender Daten juristischer Personen und
  - n) sachbezogene Daten zu Kommunikations- und Verkehrsmittel sowie Waffen einschließlich Registrierungsnummer/Kennzeichen,
2. zu Opfern oder Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie Opfer einer mit beträchtlicher Strafe bedrohten Handlung werden können, die Datenarten 1. a) bis k) sowie Gründe für die Viktimisierung und eingetretener Schaden,
3. zu Zeugen die Datenarten 1. a) bis j) und zeugenschutzrelevante Daten,
4. zu Kontakt- oder Begleitpersonen, die nicht nur zufällig mit Verdächtigen in Verbindung stehen und bei denen ausreichende Gründe für die Annahme bestehen, dass über sie Informationen zu Verdächtigen beschafft werden können, die Datenarten 1. a) bis n) bis zur Klärung der Beziehung zu Personen gemäß Z 1, sowie
5. zu Informanten und sonstigen Auskunftspersonen die Datenarten 1. a) bis j),

**Geltende Fassung****Vorgeschlagene Fassung**

sowie tat- und fallbezogene Informationen und Verwaltungsdaten verarbeiten, auch wenn es sich um besonders schutzwürdige Daten im Sinne des § 4 Z 2 DSGVO 2000 handelt.

(3) Zur Evidenthaltung von Wegweisungen, Betretungsverboten und einseitigen Verfügungen zum Schutz vor Gewalt in der Familie sind die Sicherheitsbehörden ermächtigt, zu Personen, gegen die eine derartige Maßnahme verfügt wurde, Namen, Geburtsdatum und Ort, Geschlecht, Verhältnis zur gefährdeten Person, Staatsangehörigkeit, Wohnanschrift, zu gefährdeten Personen Namen, Geburtsdatum und Ort, Geschlecht, Staatsangehörigkeit, Beziehung zum Gefährder, Wohnanschrift und Erreichbarkeitsdaten sowie Art der Maßnahme, Bereich (Anschrift, nähere Beschreibung), auf den sich die Maßnahme bezieht, bestimmte Tatsachen, auf die sich die Maßnahme stützt (insbesondere vorangegangener gefährlicher Angriff), Geltungsdauer der Maßnahme, Verstöße gegen verfügte Maßnahmen, Abbestelle für Zwecke der Zustellung der Aufhebung des Betretungsverbot oder einer einseitigen Verfügung nach § 382b EO, und Verwaltungsdaten zu verarbeiten. Die Daten von Gefährdern sind längstens nach drei Jahren, jene von Opfern längstens nach einem Jahr zu löschen. Bei mehreren Speicherungen bestimmt sich die Löschung nach dem Zeitpunkt der letzten Speicherung.

(4) Zur Evidenthaltung von Wegweisungen und Betretungsverboten in Schutzzonen sind die Sicherheitsbehörden ermächtigt, zu Personen, gegen die eine derartige Maßnahme verfügt wurde, Namen, Geburtsdatum und Ort, Geschlecht, Staatsangehörigkeit, Wohnanschrift, sowie Art der Maßnahme, Bereich (Anschrift, nähere Beschreibung), auf den sich die Maßnahme bezieht, bestimmte Tatsachen, auf die sich die Maßnahme stützt (insbesondere vorangegangener gefährlicher Angriff), Geltungsdauer der Maßnahme und Verwaltungsdaten zu verarbeiten.

(5) Soweit wegen eines sprengelübergreifenden Einsatzes eine gemeinsame Verarbeitung durch mehrere Sicherheitsbehörden erforderlich ist, dürfen Datenanwendungen gemäß Abs. 1 im Informationsverbundsystem geführt werden. Die Daten sind nach Beendigung und Evaluierung des Einsatzes, längstens jedoch nach einem Jahr zu löschen. Übermittlungen der gemäß Abs. 1 verarbeiteten Daten sind nur zulässig, wenn hierfür eine ausdrückliche gesetzliche Ermächtigung besteht.

(6) Soweit eine gemeinsame Verarbeitung durch mehrere

### Geltende Fassung

### Vorgeschlagene Fassung

Sicherheitsbehörden erforderlich ist, dürfen Datenanwendungen gemäß Abs. 2 im Informationsverbundsystem geführt werden. Daten gemäß Abs. 2 Z 1 sind längstens nach drei Jahren, Daten nach Abs. 2 Z 2 und 3 längstens nach einem Jahr, Daten gemäß Abs. 2 Z 4 bis zur Klärung der Beziehung zum Verdächtigen, längstens aber nach drei Jahren und Daten gemäß Abs. 2 Z 5 längstens nach drei Jahren zu löschen, bei mehreren Speicherungen nach derselben Ziffer bestimmt sich die Löschung nach dem Zeitpunkt der letzten Speicherung. Übermittlungen sind an Sicherheitsbehörden, Staatsanwaltschaften und Gerichte für Zwecke der Strafrechtspflege und im Übrigen nur zulässig, wenn hierfür eine ausdrückliche gesetzliche Ermächtigung besteht.

### Legende

**§ 54a.** (1) Soweit Bundesbehörden, Behörden der mittelbaren Bundesverwaltung oder Bürgermeister gesetzlich zur Ausstellung von Urkunden berufen sind, haben sie auf Verlangen des Bundesministers für Inneres zum vorbeugenden Schutz von Menschen nach § 22 Abs. 1 Z 5 und zum Zwecke verdeckter Ermittlungen (§ 54 Abs. 3) Urkunden herzustellen, die über die Identität eines Menschen täuschen.

(2) ... Die Sicherheitsbehörden haben jede Anwendung der Urkunden im Rechtsverkehr zu dokumentieren und diese im Falle missbräuchlicher Verwendung oder, sobald sie zur Aufgabenerfüllung nicht mehr benötigt werden, einzuziehen; Urkunden zum vorbeugenden Schutz von Menschen nach § 22 Abs. 1 Z 5 sind spätestens nach drei Jahren einzuziehen. ....

(3) ...

### Fälle der Sicherheitsüberprüfung

**§ 55a.** (1) bis (3) ...

(4) Solange die Voraussetzungen nach Abs. 1 bis 3 erfüllt sind, darf eine Sicherheitsüberprüfung nach drei Jahren wiederholt werden. Sicherheitsüberprüfungen gemäß Abs. 2 Z 4 sind nach zwei Jahren zu wiederholen.

### Legende

**§ 54a.** (1) Soweit Bundesbehörden, Behörden der mittelbaren Bundesverwaltung, durch Gesetz eingerichtete Körperschaften oder Anstalten des öffentlichen Rechts oder Bürgermeister gesetzlich zur Ausstellung von Urkunden berufen sind, haben sie auf Verlangen des Bundesministers für Inneres zum vorbeugenden Schutz von Menschen nach § 22 Abs. 1 Z 5 und zum Zwecke verdeckter Ermittlungen (§ 54 Abs. 3) Urkunden herzustellen, die über die Identität eines Menschen täuschen.

(2) ... Die Sicherheitsbehörden haben jede Anwendung der Urkunden im Rechtsverkehr zu dokumentieren und diese im Falle missbräuchlicher Verwendung oder, sobald sie zur Aufgabenerfüllung nicht mehr benötigt werden, einzuziehen; Urkunden zum vorbeugenden Schutz von Menschen nach § 22 Abs. 1 Z 5 sind nach Maßgabe des im Einzelfall durch den Bundesminister für Inneres festzulegenden Gefährdungszeitraumes einzuziehen. ...

(3)...

### Fälle der Sicherheitsüberprüfung

**§ 55a.** (1) bis (3) ...

(4) Solange die Voraussetzungen nach Abs. 1 bis 3 erfüllt sind, darf eine Sicherheitsüberprüfung nach drei Jahren wiederholt werden. Sicherheitsüberprüfungen gemäß Abs. 2 Z 4 sind nach zwei Jahren zu wiederholen. Bei Vorliegen von Anhaltspunkten, wonach ein Mensch nicht mehr vertrauenswürdig sein könnte, ist die Sicherheitsüberprüfung vor Ablauf dieser Fristen zu wiederholen.

**Geltende Fassung****Zentrale Informationssammlung; Zulässigkeit der Ermittlung, Verarbeitung und Übermittlung****§ 57. (1)...**

1. bis 11a. ...

12. dem Betroffenen ein ausländischer Reisepass oder Paßersatz entfremdet worden ist.

(2) Wenn der Zweck einer Datenverarbeitung nicht in der Speicherung von Personendaten gemäß Abs. 1 besteht, dürfen die Sicherheitsbehörden Namen, Geschlecht, Geburtsdatum sowie Geburtsort und Wohnanschrift von Menschen erfassen und zusammen mit Sachen oder rechtserheblichen Tatsachen im Rahmen der Zentralen Informationssammlung für Auskünfte auch an andere Behörden speichern, sofern dies für die Erreichung des Zweckes der Datenverarbeitung erforderlich ist. Hiebei darf die Auswählbarkeit dieser personenbezogenen Daten aus der Gesamtmenge der gespeicherten Daten nicht vorgesehen sein.

(3) ...

**Zentrale Informationssammlung; Sperren des Zugriffes und Löschen****§ 58. (1) ...**

1. bis 7.

8. in den Fällen der Z 10, wenn der Betroffene seine Zustimmung widerruft oder die Speicherung ihren Zweck erfüllt hat;

9. und 10.

(2)...

**Vorgeschlagene Fassung****Zentrale Informationssammlung; Zulässigkeit der Ermittlung, Verarbeitung und Übermittlung****§ 57. (1) ...**

1. bis 11a. ...

12. der Betroffene einen ausländischen Reisepass oder Passersatz verloren hat oder ihm ein solcher entfremdet wurde.

(2) Wenn der Zweck einer Datenverarbeitung nicht in der Speicherung von Personendaten gemäß Abs. 1 besteht, dürfen die Sicherheitsbehörden Namen, Geschlecht, Geburtsdatum sowie Geburtsort und Wohnanschrift von Menschen erfassen und zusammen mit Sachen oder rechtserheblichen Tatsachen im Rahmen der Zentralen Informationssammlung für Auskünfte auch an andere Behörden speichern, sofern dies für die Erreichung des Zweckes der Datenverarbeitung erforderlich ist.

(3) ...

**Zentrale Informationssammlung; Sperren des Zugriffes und Löschen****§ 58. (1) ...**

1. bis 7

8. in den Fällen der Z 10, wenn die Speicherung ihren Zweck erfüllt hat;

9. und 10;

11. in den Fällen der Z 12, wenn die Speicherung ihren Zweck erfüllt hat.

(2)...

**Zentrale Analysedatei über mit beträchtlicher Strafe bedrohte Gewalttätige, insbesondere sexuell motivierte Straftaten**

**§ 58d. (1)** Die Sicherheitsbehörden sind ermächtigt, zur Vorbeugung und Verhinderung von mit Strafe bedrohter Handlungen gegen Leib und Leben sowie gegen die sexuelle Integrität und Selbstbestimmung unter Androhung oder Anwendung von Gewalt sowie zur frühzeitigen Erkennung von diesbezüglichen Serienzusammenhängen mittels Analyse personenbezogener Daten in einem vom Bundesminister für Inneres betriebenen Informationsverbundsystem zu

## Geltende Fassung

### Vorgeschlagene Fassung

verarbeiten. Es dürfen Informationen zu Tötungsdelikten, Sexualstraftaten unter Anwendung von Gewalt, Vermisstenfällen, wenn die Gesamtumstände auf ein Verbrechen hindeuten und zu verdächtigem Ansprechen von Personen, wenn konkrete Anhaltspunkte für eine mit sexuellem Motiv geplante mit Strafe bedrohte Handlung vorliegen, verarbeitet werden. Nachstehende Datenarten dürfen zu den ausgewiesenen Betroffenenkreisen verarbeitet werden, auch wenn es sich um besonders schutzwürdige Daten im Sinne des § 4 Z 2 DSG 2000 handelt:

1. zu Verdächtigen
  - a) Namen,
  - b) frühere Namen,
  - c) Geschlecht,
  - d) Geburtsdatum und Ort,
  - e) Staatsangehörigkeit,
  - f) Wohnanschriften,
  - g) Aliasdaten,
  - h) Hinweis auf gerichtliche Verurteilungen und Maßnahmen sowie polizeiliche Vorerkenntnisse,
  - i) Beruf und Qualifikation/Beschäftigung/Lebensverhältnisse,
  - j) Personenbeschreibung,
  - k) erkennungsdienstliche Daten und
    - l) Verhaltensweisen,
2. zu Vermissten die Datenarten Z 1.a) bis f), i) bis k) und
3. zu Opfern die Datenarten Z 1.c) bis e), i) und j) sowie f) ohne Tür- bzw. Hausnummernbezeichnung

Darüber hinaus dürfen tat- und fallbezogene Daten inklusive Spuren, Beziehungsdaten und Hinweise, Objektdaten und andere sachbezogene Daten, etwa zu Waffen oder Kraftfahrzeugen sowie Verwaltungsdaten verarbeitet werden. Die Abfrageberechtigungen sind auf jenen Personenkreis zu beschränken, der mit der Bearbeitung der zu erfassenden Deliktsbereiche befasst ist.

(2) Die Übermittlung von Daten ist an Staatsanwaltschaften und Gerichte für Zwecke der Strafrechtspflege und an Justizanstalten nach Maßgabe des Strafvollzugsgesetzes zulässig. Im Übrigen sind Übermittlungen nur zulässig, soweit hierfür eine ausdrückliche gesetzliche Ermächtigung besteht.



### Geltende Fassung

### Vorgeschlagene Fassung

(3) Die Daten von Vermissten sind zu löschen, wenn der Grund für ihre Speicherung weggefallen ist, längstens aber nach 20 Jahren. Daten von Opfern sind längstens 20 Jahre, von Verdächtigen längstens 30 Jahre nach Aufnahme in die Datei zu löschen.

#### Erkennungsdienstliche Behandlung

**§ 65.** (1) Die Sicherheitsbehörden sind ermächtigt, einen Menschen, der im Verdacht steht, eine mit Strafe bedrohte Handlung begangen zu haben, erkennungsdienstlich zu behandeln, wenn er im Rahmen einer kriminellen Verbindung tätig wurde oder dies sonst auf Grund von Umständen in der Person des Betroffenen oder nach der Art der begangenen mit Strafe bedrohten Handlung zur Vorbeugung gefährlicher Angriffe des Betroffenen erforderlich scheint.

(2) bis (4) ...

(5) Die Sicherheitsbehörden haben jeden, den sie erkennungsdienstlich behandeln, schriftlich darüber in Kenntnis zusetzen, wie lange erkennungsdienstliche Daten aufbewahrt werden und welche Möglichkeiten vorzeitiger Löschung (§§ 73 und 74) bestehen. In den Fällen des Abs. 1 ist der Betroffene außerdem darauf hinzuweisen, dass die erkennungsdienstliche Behandlung deshalb erfolgte, um der Begehung gefährlicher Angriffe durch sein Wissen um die Möglichkeit seiner Wiedererkennung entgegenzuwirken.

(6) Die Sicherheitsbehörden sind ermächtigt, Namen, Geschlecht, frühere Namen, Geburtsdatum, Geburtsort, Namen der Eltern und Aliasdaten eines Menschen (erkennungsdienstliche Identitätsdaten), den sie erkennungsdienstlich behandelt haben, zu ermitteln und zusammen mit den erkennungsdienstlichen Daten und mit dem für die Ermittlung maßgeblichen Grund zu verarbeiten. In den Fällen des Abs. 1 sind die Sicherheitsbehörden ermächtigt, eine Personensfeststellung vorzunehmen.

#### Erkennungsdienstliche Behandlung

**§ 65.** (1) Die Sicherheitsbehörden sind ermächtigt, einen Menschen, der im Verdacht steht, eine mit Strafe bedrohte Handlung begangen zu haben, erkennungsdienstlich zu behandeln, wenn er im Rahmen einer kriminellen Verbindung tätig wurde oder dies wegen der Art oder Ausführung der Tat oder der Persönlichkeit des Betroffenen zur Vorbeugung weiterer gefährlicher Angriffe erforderlich scheint

(2) bis (4) ...

(5) Die Sicherheitsbehörden haben jeden, den sie erkennungsdienstlich behandeln, schriftlich darüber in Kenntnis zusetzen, wie lange erkennungsdienstliche Daten aufbewahrt werden und welche Möglichkeiten vorzeitiger Löschung (§§ 73 und 74) bestehen.

(6) Die Sicherheitsbehörden sind ermächtigt, Namen, Geschlecht, frühere Namen, Geburtsdatum, Geburtsort, Staatsangehörigkeit, Namen der Eltern, Ausstellungsbehörde, Ausstellungsdatum und Nummer mitgeführter Dokumente, allfällige Hinweise über die Gefährlichkeit beim Einschreiten einschließlich sensibler Daten, soweit deren Verwendung zur Wahrung lebenswichtiger Interessen anderer notwendig ist und Aliasdaten eines Menschen (erkennungsdienstliche Identitätsdaten), den sie erkennungsdienstlich behandelt haben, zu ermitteln und zusammen mit den erkennungsdienstlichen Daten und mit dem für die Ermittlung maßgeblichen Grund zu verarbeiten. In den Fällen des Abs. 1 sind die Sicherheitsbehörden ermächtigt, eine Personensfeststellung vorzunehmen.

### Geltende Fassung

#### Zentrale erkennungsdienstliche Evidenz

§ 75. (1) Die Sicherheitsbehörden sind ermächtigt, die von ihnen gemäß den §§ 65 Abs. 1, 65a und 66 Abs. 1 ermittelten erkennungsdienstlichen Daten, die allenfalls vorhandenen erkennungsdienstlichen Identitätsdaten (§ 65 Abs. 6) und den für die Ermittlung maßgeblichen Grund im Rahmen einer Zentralen erkennungsdienstlichen Evidenz zu verarbeiten.

(2) ...

#### Befassung des Rechtsschutzbeauftragten

§ 91c. (1) Die Sicherheitsbehörden sind verpflichtet, den Rechtsschutzbeauftragten von jeder Ermittlung personenbezogener Daten durch verdeckte Ermittlung (§ 54 Abs. 3), durch den verdeckten Einsatz von Bild- oder Tonaufzeichnungsgeräten (§ 54 Abs. 4) oder durch Verarbeiten von Daten, die andere mittels Einsatz von Bild- und Tonaufzeichnungsgeräten er- und übermittelt haben (§ 53 Abs. 5) unter Angabe der für die Ermittlung wesentlichen Gründe in Kenntnis zu setzen. Für derartige Maßnahmen im Rahmen der erweiterten Gefahrenforschung gilt Abs. 3. Darüber hinaus ist der Rechtsschutzbeauftragte über den Einsatz von Kennzeichenerkennungsgeräten (§ 54 Abs. 4b) zu informieren.

(2) Sicherheitsbehörden, die die Überwachung öffentlicher Orte mit Bild- und Tonaufzeichnungsgeräten im Sinne des § 54 Abs. 6 und 7 beabsichtigen, haben unverzüglich den Bundesminister für Inneres zu verständigen. Dieser hat dem Rechtsschutzbeauftragten Gelegenheit zur Äußerung binnen drei Tagen zu geben. Der tatsächliche Einsatz der Bild- und Tonaufzeichnungsgeräte darf erst nach Ablauf dieser Frist oder Vorliegen einer entsprechenden Äußerung des Rechtsschutzbeauftragten erfolgen.

(3) ...

§ 94. (1) bis (22) ...

### Vorgeschlagene Fassung

#### Zentrale erkennungsdienstliche Evidenz

§ 75. (1) Die Sicherheitsbehörden sind ermächtigt, die von ihnen gemäß den §§ 65 Abs. 1, 65a, 66 Abs. 1 und 67 Abs. 1 erster Satz ermittelten erkennungsdienstlichen Daten, die allenfalls vorhandenen erkennungsdienstlichen Identitätsdaten (§ 65 Abs. 6) und den für die Ermittlung maßgeblichen Grund im Rahmen einer Zentralen erkennungsdienstlichen Evidenz zu verarbeiten. Personenbezogene Daten, die Sicherheitsbehörden nach anderen Bestimmungen rechtmäßig ermittelt haben, dürfen sie in der zentralen erkennungsdienstlichen Evidenz weiterverarbeiten, wenn deren Ermittlung und Verarbeitung für sicherheitspolizeiliche Zwecke zu dem Zeitpunkt zulässig wäre, in dem die Daten verwendet werden sollen.

(2) ...

#### Befassung des Rechtsschutzbeauftragten

§ 91c. (1) Die Sicherheitsbehörden sind verpflichtet, den Rechtsschutzbeauftragten von jeder Ermittlung personenbezogener Daten durch verdeckte Ermittlung (§ 54 Abs. 3), durch den verdeckten Einsatz von Bild- oder Tonaufzeichnungsgeräten (§ 54 Abs. 4), durch Verarbeiten von Daten, die andere mittels Einsatz von Bild- und Tonaufzeichnungsgeräten er- und übermittelt haben (§ 53 Abs. 5) oder durch Standortbestimmung (§ 53 Abs. 3b) unter Angabe der für die Ermittlung wesentlichen Gründe in Kenntnis zu setzen. Für derartige Maßnahmen im Rahmen der erweiterten Gefahrenforschung gilt Abs. 3. Darüber hinaus ist der Rechtsschutzbeauftragte über den Einsatz von Kennzeichenerkennungsgeräten (§ 54 Abs. 4b) zu informieren.

(2) Sicherheitsbehörden, die die Überwachung öffentlicher Orte mit Bild- und Tonaufzeichnungsgeräten im Sinne des § 54 Abs. 6 und 7 oder die Führung einer Datenanwendung gemäß § 53a Abs. 2 und 6 beabsichtigen, haben unverzüglich den Bundesminister für Inneres zu verständigen. Dieser hat dem Rechtsschutzbeauftragten Gelegenheit zur Äußerung binnen drei Tagen zu geben. Der tatsächliche Einsatz der Bild- und Tonaufzeichnungsgeräte oder die Aufnahme der Datenanwendung darf erst nach Ablauf dieser Frist oder Vorliegen einer entsprechenden Äußerung des Rechtsschutzbeauftragten erfolgen.“

(3) ...

§ 94. (1) bis (22) ...

**Geltende Fassung****Vorgeschlagene Fassung**

(23) Die §§ 11 Abs. 2, 15b Abs. 1, 22 Abs. 3, 53 Abs. 3b und 3c, 53a (neu) samt Überschrift, 53b samt Überschrift, 54a Abs. 1 und 2, 55a Abs. 4, 57 Abs. 1 Z 12 und Abs. 2, 58 Abs. 1 Z 8, 10 und 11, 58d samt Überschrift, 65 Abs. 1, 5 und 6, 75 Abs. 1, 91c Abs. 1 und 2, 96 sowie das Inhaltsverzeichnis in der Fassung des Bundesgesetzes BGBl. I Nr. XX/2007 treten mit 1. Jänner 2008 in Kraft.

**Übergangsbestimmungen****Übergangsbestimmungen**

§ 96. (1) ...

§ 96. (1) ...

(2) Sofern am Tage des Inkrafttretens dieses Bundesgesetzes Sicherheitsdirektionen ihren Sitz außerhalb der Landeshauptstadt haben, kann dieser Zustand ungeachtet § 7 Abs. 1 aufrechterhalten werden.

(2) entfällt - Abs. 3 bis 6 werden zu Abs. 2 bis 5

(3) bis (6) ...

(2) bis (5) ...

**Artikel 2****Änderung des Grenzkontrollgesetzes**

§ 12. (1) ...

§ 12. (1) ...

(1a) Die Behörde ist ermächtigt, im Bereich von Grenzübergangsstellen zur Durchführung der Grenzkontrolle Bild- und Tonaufzeichnungsgeräte einzusetzen. Diese Maßnahme ist gut sichtbar anzukündigen. Die Behörde hat vom beabsichtigten Einsatz der Bild- und Tonaufzeichnungsgeräte unverzüglich den Bundesminister für Inneres zu verständigen. Dieser hat dem Rechtsschutzbeauftragten (§ 62a SPG) Gelegenheit zur Äußerung binnen drei Tagen zu geben. Mit dem Einsatz der Bild- und Tonaufzeichnungsgeräte darf erst nach Ablauf dieser Frist oder nach Vorliegen einer entsprechenden Äußerung des Rechtsschutzbeauftragten begonnen werden, es sei denn, es wären zur Abwehr schwerer Gefahr sofortige Ermittlungen erforderlich.

(1a) Die Behörde ist ermächtigt, im Bereich von Grenzübergangsstellen zur Durchführung der Grenzkontrolle Bild- und Tonaufzeichnungsgeräte einzusetzen. Diese Maßnahme ist gut sichtbar anzukündigen. Die Behörde hat vom beabsichtigten Einsatz der Bild- und Tonaufzeichnungsgeräte unverzüglich den Bundesminister für Inneres zu verständigen. Dieser hat dem Rechtsschutzbeauftragten (§ 91c SPG) Gelegenheit zur Äußerung binnen drei Tagen zu geben. Mit dem Einsatz der Bild- und Tonaufzeichnungsgeräte darf erst nach Ablauf dieser Frist oder nach Vorliegen einer entsprechenden Äußerung des Rechtsschutzbeauftragten begonnen werden, es sei denn, es wären zur Abwehr schwerer Gefahr sofortige Ermittlungen erforderlich.

(2) bis (6) ...

(2) bis (6) ...

**Inkrafttreten****Inkrafttreten**

§ 18. (1) bis (4)...

§ 18. (1) bis (4)...

(5) § 12 Abs. 1a in der Fassung des Bundesgesetzes BGBl. I Nr. XX/2007 tritt mit Ablauf des Tages der Kundmachung in Kraft.

## Geltende Fassung

## Vorgeschlagene Fassung

## Artikel 3

## Änderung des Polizeikooperationsgesetzes

§ 7. (1) bis (4) ...

§ 7. (1) bis (4) ...

(5) Die Sicherheitsbehörden sind ermächtigt, Amtshilfe durch das Verwenden von Daten, die von ausländischen Sicherheitsbehörden und Sicherheitsorganisationen in gemeinsam geführten Informationssammlungen verarbeitet werden, unmittelbar in Anspruch zu nehmen. Besondere Bestimmungen in völkerrechtlichen Verträgen bleiben davon unberührt.

§ 8. (1) ...

§ 8. (1) ...

(2) ...

(2) ...

1. bis 2....

1. bis 2....

3. die ersuchende Sicherheitsbehörde oder -organisation nicht für den gebotenen Schutz des Privatlebens (Art. 8 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten, BGBl. Nr. 210/1958, und § 1 des Datenschutzgesetzes, BGBl. Nr. 565/1978) des Betroffenen Sorge tragen oder ausdrückliche datenschutzrechtliche Auflagen der ersuchten Behörde mißachten werde, hat eine Übermittlung personenbezogener Daten im Rahmen der Amtshilfe zu unterbleiben. Für Mitgliedstaaten des Schengener Durchführungsübereinkommens oder des Europol-Übereinkommens sowie bei internationalen Fahndungen über richterlichen Auftrag kommen für eine solche Annahme nur bestimmte Tatsachen des Einzelfalls in Betracht.

3. die ersuchende Sicherheitsbehörde oder -organisation nicht für den gebotenen Schutz des Privatlebens (Art. 8 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten, BGBl. Nr. 210/1958, und § 1 des Datenschutzgesetzes 2000 – DSG 2000, BGBl. I Nr. 165/1999) des Betroffenen Sorge tragen oder ausdrückliche datenschutzrechtliche Auflagen der ersuchten Behörde mißachten werde, hat eine Übermittlung personenbezogener Daten im Rahmen der Amtshilfe zu unterbleiben. Für Mitgliedstaaten des Schengener Durchführungsübereinkommens oder des Europol-Übereinkommens sowie bei internationalen Fahndungen über richterlichen Auftrag kommen für eine solche Annahme nur bestimmte Tatsachen des Einzelfalls in Betracht.

(3) ...

(3) ...

§ 20. (1) bis (3) ...

§ 20. (1) bis (3) ...

(4) § 7 Abs. 5 in der Fassung des Bundesgesetzes BGBl. I Nr. XX/2007 tritt mit 1. Jänner 2008 in Kraft.