Erläuterungen

Allgemeiner Teil

Hauptgesichtspunkte des Entwurfs

1. Die globalisierte Welt führt zu internationalen Verflechtungen und gegenseitigen Abhängigkeiten in allen Lebensbereichen. In diesem fortschreitenden Prozess wandelt sich die Auffassung von territorialen Beschränkungen und staatlichen Grenzen und zeigt sich in den letzten Jahren das verstärkt erkennbare Phänomen der Internationalisierung lokaler und nationaler Ereignisse. Kritische Aktivitäten bzw. Aussagen auf lokaler oder nationaler Ebene können auf einem anderen Kontinent Reaktionen hervorrufen, die von virtuellen Drohungen und Demonstrationen bis hin zu Gewalttaten reichen können. Die Staaten stehen heute einer vernetzten Bedrohung gegenüber, die durch einen transnationalen Terrorismus, die Verbreitung von Massenvernichtungswaffen und Cyber-Angriffen charakterisiert ist. Diese Vernetzung, die durch die modernen Kommunikationstechnologien weiter vorangetrieben wird, wirkt sich massiv auch auf den Bereich der Sicherheit aus.

Aufgabe des polizeilichen Staatsschutzes muss es sein, die im Staatsgebiet lebenden Menschen und die verfassungsmäßige Grundordnung zu schützen. Der verfassungsmäßig garantierte Schutz des Individuums steht in Teilbereichen in einem Spannungsverhältnis mit den Aufgaben der inneren Sicherheit. Dabei kann ein Eingriff in die individuellen Grundrechte nur unter Abwägung des Grundrechtsschutzes und den Erfordernissen der Aufrechterhaltung der inneren Sicherheit erfolgen.

Die Diversität der Bedrohungen und eine zunehmend von globalen Rahmenbedingungen abhängige Gefahrenlage erfordern einen modernen und vernetzten polizeilichen Staatsschutz. Wollen die Sicherheitsbehörden nicht nur auf Gefahren reagieren, sondern Bedrohungen aktiv schon im Vorfeld entgegentreten, dann müssen ihnen dazu auch entsprechende Mittel und Möglichkeiten an die Hand gegeben werden.

Dieses Anliegen ist auch im Arbeitsprogramm der österreichischen Bundesregierung 2013-2018 verankert, in dem die Schaffung besonderer bundesgesetzlicher Regelungen für den Staatsschutz als Maßnahme ausdrücklich vorgesehen ist (06 Sicherheit und Rechtsstaat, Inneres, S 81). Mit dieser Maßnahme soll eine effektive und effiziente Abwehr der Spionage und der Folgen von Extremismus und Terrorismus durch den Ausbau der präventiven und repressiven Mechanismen ermöglicht werden.

Mit dem vorliegenden Entwurf soll das Regierungsprogramm umgesetzt und eine bundesgesetzliche Regelung über die Organisation, Aufgaben und Befugnisse des Staatsschutzes geschaffen werden:

Während im ersten Hauptstück Regelungen zur Organisation der polizeilichen Staatsschutzbehörden verankert werden sollen, werden im zweiten Hauptstück jene Aufgaben taxativ genannt, die ausschließlich diesen Behörden zukommen: Dazu zählen die erweiterte Gefahrenerforschung und der Schutz vor verfassungsgefährdenden Angriffen, die staatsschutzrelevante Beratung sowie die umfassende Beurteilung und Analyse von polizeilich staatsschutzrelevanten Bedrohungen zur Information verfassungsmäßiger Einrichtungen. Die im dritten Hauptstück verankerten Datenverarbeitungsermächtigungen sollen den Bedürfnissen des polizeilichen Staatsschutzes soweit gerecht werden, als es in einem ausgewogenen Verhältnis mit dem Grundrecht auf Schutz des Privatlebens und Achtung der Privatsphäre (Art. 8 EMRK) vereinbar ist. Umfassende Regelungen zum Rechtsschutz einschließlich Informationspflichten für Betroffene und Berichtspflichten finden sich schließlich im vierten Hauptstück des Entwurfs.

2. Die in Artikel 2 des Entwurfs vorgesehenen Änderungen des Sicherheitspolizeigesetzes (SPG) berücksichtigen einerseits die erforderlichen Anpassungen an das Polizeiliche Staatsschutzgesetz (PStSG) und anderseits folgende wesentliche Punkte:

Der Einsatz von Bild- und Tonaufzeichnungsgeräten zur Dokumentation von Amtshandlungen, bei denen die Organe des öffentlichen Sicherheitsdienstes Befehls- und Zwangsgewalt ausüben, soll gesetzlich verankert werden. Zur Verfolgung strafbarer Handlungen und zur Kontrolle der Rechtmäßigkeit einer Amtshandlung kommt einer ausreichenden und an den technischen Möglichkeiten ausgerichteten Videodokumentation als Beweismittel wesentliche Bedeutung zu. Daher soll auf diese Art von Dokumentation, der die erforderliche Objektivität eines Sachbeweises inne wohnt, in Zukunft nicht verzichtet werden, um im Anlassfall, also wenn Zweifel an der Rechtmäßigkeit der Amtshandlung laut werden oder es gilt, strafbare Handlungen zu verfolgen, darauf zurückgreifen zu können.

Zudem soll die Möglichkeit geschaffen werden, bei der Sicherheitsbehörde vorhandenes Videomaterial (§ 54 Abs. 5) auch zur Verfolgung von bestimmten Verwaltungsübertretungen zu verwenden, um

insbesondere Verwaltungsübertretungen nach dem PyrotechnikG 2010 bei Sportgroßveranstaltungen, die ein großes Gefahrenpotential darstellen, wie der Entschließung betreffend Reglementierung pyrotechnischer „Signalstifte“, 61/E, 25. GP vom 10. Dezember 2014 und den diesbezüglichen Ausführungen im Bericht des Ausschusses für innere Angelegenheiten, AB 411 BlgNR 25. GP, zu entnehmen ist, im Nachhinein aufklären zu können.

In § 21 Abs. 2a soll die Aufgabe und der Umfang des Einschreitens von Organen des öffentlichen Sicherheitsdienstes an Bord von Zivilluftfahrzeugen festgelegt sowie in § 75 Abs. 1a eine ausdrückliche gesetzliche Grundlage im SPG für die Verarbeitung von Spuren, die auf Grundlage der Strafprozessordnung ermittelt worden sind, zum Zweck ihrer Zuordnung zu einer Person geschaffen werden.

Kompetenzgrundlage

Die Kompetenz des Bundes zur Erlassung eines diesem Entwurf entsprechenden Bundesgesetzes gründet sich auf Art. 10 Abs. 1 Z 7 („Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit“) und Z 14 („Organisation und Führung der Bundespolizei“) des Bundes-Verfassungsgesetzes (B-VG), BGBl. Nr. 1/1930.

Besonderer Teil

Artikel 1

Zu § 1:

Die Bestimmung soll die Tätigkeitsbereiche der polizeilichen Staatsschutzbehörden, konkret des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung und der Landesämter Verfassungsschutz, zum Ausdruck bringen. Durch den Hinweis, dass es sich um Tätigkeitsbereiche des polizeilichen Staatsschutzes handelt, soll klar gestellt werden, dass eine Zuständigkeit nur insofern besteht, als verfassungsmäßig nicht anderes vorgesehen ist (vgl. Art. 9a und 79 B-VG). Das Bundesamt besteht als besondere Teilorganisation der Generaldirektion für die öffentliche Sicherheit, vergleichbar mit dem Bundeskriminalamt. Es entfaltet seine Tätigkeit daher unter Leitung und gemäß den Weisungen des Bundesministers für Inneres und des Generaldirektors für die öffentliche Sicherheit. Demgegenüber stellen die neun Landesämter Verfassungsschutz eine Teilorganisation der Landespolizeidirektionen dar und entfalten ihre Tätigkeit, sofern eine solche nicht ausdrücklich dem Bundesamt vorbehalten ist, unter Leitung und gemäß den Weisungen des Bundesministers für Inneres, des Generaldirektors für die öffentliche Sicherheit und des Landespolizeidirektors. Die Organisationsgewalt des Bundesministers für Inneres (Art. 77 Abs. 3 B-VG) bleibt daher uneingeschränkt erhalten. Der in Abs. 4 verankerte Aufgabenvorbehalt kann mittels (genereller) Weisung, insbesondere aus Gründen der Zweckmäßigkeit und Wirtschaftlichkeit, erfolgen. Ebenso kann es sich im Sinne eines effizienten Vollzugs als sinnvoll erweisen, die Landesämter mit der Durchführung einzelner Ermittlungen oder sonstiger Maßnahmen, etwa von Objektschutzmaßnahmen, zu beauftragen und sich regelmäßig darüber berichten zu lassen, um einen österreichweiten koordinierten Vollzug sicherzustellen. Mit Abs. 5 soll klar gestellt werden, wem die Auftraggebereigenschaft (iSd § 4 Z 4 DSG 2000) für die Verwendung personenbezogener Daten zukommt; auch wenn die in diesem Gesetz - von der Sonderregelung in § 8 abgesehen - genannten Aufgaben und Ermächtigungen bestimmten Organisationseinheiten vorbehalten bleiben, sind die Amtshandlungen der dahinter stehenden Behörde zuzurechnen.

Zu § 2:

Die Leitung des Bundesamtes obliegt einem Direktor, der gleichzeitig auch die Funktion des Informationssicherheitsbeauftragten nach dem Informationssicherheitsgesetz (§ 7 InfoSiG) für den Wirkungsbereich des Bundesministeriums für Inneres innehat. Für die Ernennung als Direktor sind neben der Voraussetzung eines abgeschlossenen Studiums der Rechtswissenschaften auch besondere fachliche Kenntnisse im Bereich des polizeilichen Staatsschutzes, die sich insbesondere aus einer mehrjährigen einschlägigen Berufserfahrung ergeben können, erforderlich. Die Organisation der Landesämter richtet sich nach den Organisationsvorschriften der Landespolizeidirektionen.

Aus den in § 1 Abs. 2 beschriebenen Tätigkeitsbereichen lässt sich entnehmen, dass Bediensteten bei Staatsschutzbehörden ein für eine Sicherheitsbehörde sehr spezifisches Tätigkeitsfeld zukommt, das zudem in einem frühen Stadium gewisse Ermittlungsschritte erfordert. Daraus ergibt sich die Notwendigkeit, dass alle Bediensteten des Bundesamtes und der Landesämter innerhalb von zwei Jahren nach Dienstbeginn eine spezielle Ausbildung absolvieren müssen, deren Inhalt aus Gründen der Transparenz mit Verordnung des Bundesministers für Inneres festgelegt wird.

Da im Bundesamt und den Landesämtern auch Bedienstete in Leitungsfunktionen beschäftigt sind, die keine Organe des öffentlichen Sicherheitsdienstes sind, dient die Absolvierung der Ausbildung nach Abs. 3 - zusätzlich zu Schulungen etwa in den Bereichen Waffengebrauchsrecht und Einsatztraining sowie der für den allgemeinen Verwaltungsdienst ohnehin verpflichtend vorgeschriebenen Grundausbildung (vgl. etwa §§ 25 ff BDG) - auch als Grundlage für eine allfällig notwendige Ermächtigung zur Ausübung von Befehls- und Zwangsgewalt. Unter Leitungsfunktion fällt jede Funktion von einem Referatsleiter aufwärts.

Dem Wesen einer Staatsschutzbehörde inhärent ist der Zugang zu vertraulicher Information. Daher soll sich jeder Bedienstete vor Beginn seiner Tätigkeit einer Sicherheitsüberprüfung unterziehen müssen. Je nachdem, welche Funktion der Bedienstete anstrebt, soll er sich einer Überprüfung für den Zugang zu geheimer oder streng geheimer Information zu unterziehen haben.

Zu § 3:

Wie das Bundeskriminalamt oder das Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung soll auch das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung über eine eigenständige Geschäftsordnung verfügen. In der Geschäftsordnung hat der Direktor festzulegen, wem die Genehmigung von Entscheidungen, die für den Bundesminister für Inneres, nicht für den Direktor des Bundesamtes gezeichnet werden, zukommt, in welchen Angelegenheiten ihm die Genehmigung vorbehalten ist und wem die Genehmigung im Fall der Verhinderung zukommt. Vor Erlassung der Geschäftsordnung sowie jeder Änderung derselben ist der Generaldirektor für die öffentliche Sicherheit zu befassen. Der Weisungszusammenhang zum Bundesminister für Inneres bleibt auf diese Weise unberührt. Nähere Regelungen zur Geschäftsordnung der Landesämter obliegen dem Landespolizeidirektor (§ 12 Abs. 2 SPG).

Zu § 4:

Die in den Ziffern 1 bis 5 genannten Funktionen soll das Bundesamt als Zentralstelle im nationalen Bereich kraft Gesetzes wahrnehmen. Davon umfasst sind jene Funktionen, deren österreichweite Zentralisierung am Gebiet des polizeilichen Staatsschutzes angezeigt erscheint. Die Funktionen übt das Bundesamt als Teilorganisation der Generaldirektion für die öffentliche Sicherheit für den Bundesminister für Inneres aus. Durch den Verweis auf die Legaldefinition des § 74 Abs. 1 Z 8 StGB wird klargestellt, dass unter Computersystem iSd § 4 Z 1 jede Vorrichtung, die Daten automationsunterstützt verarbeitet, zu verstehen ist (vgl. Jerabek/Reindl-Krauskopf/Schroll in WK^2 StGB § 74 Rz 58 ff). Nähere Regelungen über die internationale Zusammenarbeit des Bundesamtes mit ausländischen Sicherheitsdienststellen und Sicherheitsorganisationen nach § 4 Z 5 finden sich in den Bestimmungen über die internationale polizeiliche Amtshilfe.

Zu § 5:

Sowohl beim Bundesamt als auch bei den Landesämtern handelt es sich nach wie vor um Organisationseinheiten der Sicherheitsbehörden (Art. 78a B-VG), an deren Aufgaben und Befugnissen auf dem Gebiet der Sicherheitspolizei sich durch dieses Bundesgesetz nichts ändert, soweit nicht Besonderes bestimmt ist. Das hat zur Folge, dass etwa die Aufgabe der Gefahrenabwehr und die damit einhergehenden Befugnisse, die in diesem Bundesgesetz nicht geregelt werden, wie bisher auf Grundlage des Sicherheitspolizeigesetzes erfolgen.

Zu § 6:

Die erweiterte Gefahrenerforschung für die Gruppierung soll unverändert vom SPG ins PStSG übernommen werden, da sich die Aufgabe in der Praxis bewährt hat und ausschließlich vom Bundesamt und den Landesämtern wahrgenommen wird.

Anders verhält es sich mit der erweiterten Gefahrenerforschung für die Einzelperson gemäß § 21 Abs. 3 Z 1 SPG. Die mit der SPG-Novelle 2011, BGBl. I Nr. 13/2012, eingeführte Regelung hat sich aus mehreren Gründen als nicht zielführend erwiesen:

Zum einen verlangt die erste Alternative des § 21 Abs. 3 Z 1 SPG als Vorverhalten, dass sich die Person für Gewalt ausgesprochen hat, und zwar entweder öffentlich oder in schriftlicher oder elektronischer Kommunikation. Eine direkte Aussage gegenüber einem staatlichen Organ, selbst gegenüber den Strafverfolgungsbehörden, reicht somit nicht aus, obwohl eine solche Aussage ebenso Anlass genug zur Beobachtung der Person gäbe. Die zweite Alternative des § 21 Abs. 3 Z 1 SPG verlangt nicht nur die Beschaffung von Kenntnissen, sondern – kumulativ dazu – auch von konkreten Mitteln; damit wird sogar etwas mehr verlangt, als für die Erfüllung des Tatbestandes des § 278f Abs. 2 StGB.

Zum anderen muss die Gefahrenprognose die Möglichkeit von Verbrechen iSd § 17 StGB befürchten lassen, die den Einsatz von Gewalt vorsehen. Die Prognose, die Zielperson werde Spionage (§§ 252, 256

StGB) oder Proliferation begehen oder führend an einem Landfriedensbruch teilnehmen, reicht für den derzeitigen § 21 Abs. 3 Z 1 SPG nicht aus.

Auch die vom Bundesamt in Auftrag gegebene Evaluierung der vom Bundesamt erstellten Bedarfsanalyse im Hinblick auf Rechtsgrundlagen für die Staatsschutzarbeit von ALES (Austrian Center for Law Enforcement Sciences) kommt zum Schluss, dass ganz allgemein die derzeitige Aufgabe „Erweiterte Gefahrenerforschung im Hinblick auf Einzelpersonen“ als zu eng erscheint und eine sinnvolle Wahrnehmung durch das Bundesamt bei potentiell gefährlichen Einzelpersonen nach geltender Rechtslage kaum möglich ist.

Mit dem vorliegenden Entwurf soll die bisherige Aufgabe der erweiterten Gefahrenerforschung bei Einzelpersonen im vorbeugenden Schutz von Rechtsgütern angesiedelt werden, eingeschränkt auf verfassungsgefährdende Angriffe, sofern ein begründeter Gefahrenverdacht besteht.

Für die Aufgabe bedarf es somit hinreichender Anhaltspunkte für die Annahme, dass ein verfassungsgefährdender Angriff vorbereitet werde (§ 22 Abs. 2 SPG). Es muss also ein begründeter Gefahrenverdacht bestehen, dass der Betroffene einen verfassungsgefährdenden Angriff in absehbarer Zeit begehen werde. Das Erfordernis eines begründeten Gefahrenverdachts bedeutet dabei mehr als die bloße Möglichkeit oder Nichtausschließbarkeit eines Angriffes, aber weniger als mit Gewissheit zu erwarten (vgl. Hauer/Keplinger, SPG[4], § 22 Anm 10.1).

Mit der Einführung einer Definition eines verfassungsgefährdenden Angriffes in Abs. 2 sollen die Tatbestände, die für einen vorbeugenden Schutz im Bereich des polizeilichen Staatsschutzes in Frage kommen, taxativ aufgezählt werden, also ein konkret auf die Aufgabe des Verfassungsschutzes und der Terrorismusbekämpfung zugeschnittener Straftatenkatalog geschaffen werden. Davon umfasst sollen jene gerichtlich strafbaren Handlungen sein, die mit Extremismus (z.B. nach dem Verbotsgesetz), Terrorismus (z.B. Terroristische Vereinigung, Ausbildung für terroristische Zwecke), Proliferation (z.B. Unerlaubter Umgang mit Kernmaterial, radioaktiven Stoffen oder Strahleneinrichtungen, §§ 79 bis 82 Außenwirtschaftsgesetz), nachrichtendienstlicher Tätigkeit (z.B. Geheimer Nachrichtendienst zum Nachteil Österreichs) oder Spionage (z.B. Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses zugunsten des Auslandes) in Verbindung stehen. Je nach Delikt oder Deliktsgruppe ist zusätzlich noch eine bestimmte Motivlage („weltanschaulich oder religiös motiviert“) oder ein bestimmtes Ziel des Angriffes (verfassungsmäßige Einrichtungen oder kritische Infrastrukturen) erforderlich, um von einem verfassungsgefährdenden Angriff sprechen zu können. Wie beim gefährlichen Angriff nach § 16 Abs. 2 SPG wird auf die rechtswidrige Verwirklichung abgestellt, wodurch zum Ausdruck gebracht wird, dass zwar ein tatbestandsmäßiges und rechtswidriges, aber kein schuldhaftes Verhalten erforderlich ist.

Mit der Ziffer 3 von Abs. 1 soll die Entgegennahme von Informationen von Dienststellen inländischer Behörden, etwa dem Heeres-Nachrichtenamt oder dem Abwehramt, oder von ausländischen Sicherheitsbehörden oder Sicherheitsorganisationen (§ 2 Abs. 2 und 3 PolKG) sowie von Organen der Europäischen Union oder Vereinten Nationen über Personen, die im Verdacht stehen, im Ausland einen Sachverhalt verwirklicht zu haben, der einem verfassungsgefährdenden Angriff entspricht, für die daran anknüpfende Verarbeitung dieser Informationen nach § 10 als Aufgabe der Staatsschutzbehörden verankert werden. Diese Aufgabe trägt der Tatsache Rechnung, dass in einer globalisierten Welt auch die Aufgabe des Schutzes der österreichischen Bevölkerung vor verfassungsgefährdenden Angriffen global betrachtet werden muss und sich mögliche Gefährder und damit einhergehende Gefahren örtlich rasch verschieben können. Zu diesem Zweck erlässt etwa auch der Rat der Europäischen Union in regelmäßigen Abständen Durchführungsverordnungen zur Durchführung des Art. 2 Abs. 3 der Verordnung (EG) Nr. 2580/2001 über spezifische, gegen bestimmte Personen und Organisationen gerichtete restriktive Maßnahmen zur Bekämpfung des Terrorismus, zuletzt am 26. März 2015. Die an diese Aufgabe anknüpfenden Datenverarbeitungsermächtigungen beschränken sich auf § 10; besondere Ermittlungsmaßnahmen nach § 11 kommen dafür nicht in Betracht, wenn nicht zusätzliche Umstände hinzutreten, die eine Aufgabe nach § 6 Abs. 1 Z 1 oder 2 begründen.

Zu § 7:

Die staatsschutzrelevante Beratung auf dem Gebiet des polizeilichen Staatsschutzes soll als Teil der schlichten Hoheitsverwaltung durch entsprechende Öffentlichkeitsarbeit erfolgen und sich unmittelbar an potentiell betroffene juristische oder natürliche Personen wenden, die von potentiellen Gefahren durch verfassungsgefährdende Angriffe bedroht sind. Zu denken ist dabei etwa an Betreiber kritischer Infrastrukturen, die über effektive Schutzmaßnahmen vor Cyberangriffen oder derzeit gängige modi operandi informiert werden sollen, sowie an Unternehmen, die über mögliche Gefahren durch Wirtschafts- und Industriespionage und allgemeine Verhaltensregeln aufgeklärt werden sollen. Besonders geschulte Beamte des Bundesamtes oder der Landesämter stellen ihre Sachkenntnis zur Verfügung, um

potentiell Betroffene in die Lage zu versetzen, sich bestmöglich selbst durch effektive Maßnahmen zu schützen.

Zu § 8:

Die „Information verfassungsmäßiger Einrichtungen“ wird aus dem SPG (§ 93a) herausgelöst und in adaptierter Form als Aufgabe im PStSG verankert.

Aufgabe des Bundesamtes sowie der Landesämter soll es künftig sein, staatsschutzrelevante Bedrohungslagen, also Gefährdungen verfassungsmäßiger Einrichtungen oder deren Handlungsfähigkeit, der Bevölkerung durch terroristische, weltanschauliche oder politisch motivierte Kriminalität, durch Spionage und nachrichtendienstliche Tätigkeit, durch Proliferation, illegalen Handel mit Kriegsmaterial sowie Waffen, Schieß- und Sprengmittel rechtzeitig zu erkennen und dahingehend zu beurteilen, ob sich daraus eine staatsschutzrelevante Bedrohung ergibt, worüber die in Abs. 2 und 3 genannten verfassungsmäßigen Einrichtungen zu informieren wären. Dasselbe gilt für verfassungsgefährdende Entwicklungen im Ausland, worunter Vorgänge zu verstehen sind, bei denen Angehörige verfeindeter Gruppierungen gegeneinander vorgehen oder sich etwa religiös oder weltanschaulich motivierte Demonstrationen oder Straftaten von verfeindeten Gruppen bis hin zu Gewalttaten ereignen. Auch deren Auswirkungen fließen im Hinblick auf ein etwaiges Bedrohungspotenzial in Österreich in die Beurteilung ein. Von der Erfüllung dieser Aufgabe ist der Informationsaustausch mit ausländischen Sicherheitsbehörden (§ 2 Abs. 3 PolKG) erfasst. Hingegen ausdrücklich nicht erfasst ist der Vollziehungsbereich des Bundesministers für Landesverteidigung und Sport, insbesondere die Zuständigkeiten, die sich aus dem Militärbefugnisgesetz (MBG) ergeben. So sind beispielsweise im Sinne des § 20 MBG sämtliche Informationen von sicherheitspolitischer Bedeutung aufklärungsfähig, wozu insbesondere die internationale Krisenbeobachtung oder die Beurteilung der militärstrategischen Lage zählen.

Die Pflicht zur Information der in Abs. 2 und 3 genannten Personen trifft die Spitze der zuständigen Behörde, also den Bundesminister bzw. den Landespolizeidirektor. Durch die Information über staatsschutzrelevante Bedrohungen sollen die verfassungsmäßigen Einrichtungen bei der Erfüllung ihrer gesetzlichen Aufgaben unterstützt werden. Durch die Information über Umstände, die für die Wahrung des Ansehens der Vertretungskörper von Bedeutung sind, sollen die Genannten vor Schritten bewahrt werden, die dem Ansehen des Vertretungskörpers als solchem Schaden zufügen würden.

Zu § 9:

Mit § 9 wird klargestellt, dass Grundvoraussetzung jeder Verwendung personenbezogener Daten die Erforderlichkeit zur Erfüllung einer Aufgabe nach diesem Bundesgesetz ist. Die Wahrung der Verhältnismäßigkeit bei Verwendung personenbezogener Daten ergibt sich zwar bereits aus dem Verweis in § 5, wodurch die Bestimmung des § 51 SPG auch im Bereich des Staatsschutzes zur Anwendung gelangt. Anregungen im Begutachtungsverfahren aufgreifend soll die Wahrung der Verhältnismäßigkeit bei Verwendung personenbezogener Daten aber zusätzlich ausdrücklich den Bestimmungen über die Datenverwendung im PStSG vorangestellt werden. Ermächtigungen zur Datenverarbeitung nach anderen Bundesgesetzen, etwa dem SPG, bleiben von der Regelung des PStSG unberührt.

Zu § 10:

§ 10 Abs. 1 enthält als Grundsatzbestimmung eine allgemeine Ermächtigung zur Ermittlung und Weiterverarbeitung personenbezogener Daten im Rahmen des (sicherheitspolizeilichen) Ermittlungsdienstes auf dem Gebiet des polizeilichen Staatsschutzes und knüpft hinsichtlich der Zwecke an taxativ aufgezählte Aufgaben an. Begrenzt wird die Verarbeitungsermächtigung durch die spezifischen Regelungen der folgenden Absätze sowie der besonderen Bestimmungen für die Ermittlung nach § 11. Als Grundsatzbestimmung für das gesamte dritte Hauptstück stellt Abs. 1 ausdrücklich klar, dass sensible Daten nach § 4 Z 2 DSG 2000 nur insoweit ermittelt und weiterverarbeitet werden dürfen, als diese unbedingt für die Erfüllung der Aufgabe erforderlich sind. Die Weiterverarbeitung der Daten iS einer Speicherung erfolgt nach den Vorschriften des § 13a SPG. Sollen die auf Grundlage des § 10 (und § 11) ermittelten Daten auch in einer gesonderten Datenanwendung gespeichert werden, müssen die Voraussetzungen des § 12 Abs. 1 und 2 vorliegen, sofern es sich nicht um die Datenverarbeitung im Zusammenhang mit dem Schutz kritischer Infrastruktur oder verfassungsmäßiger Einrichtungen handelt, die weiterhin im SPG (§ 53a) verbleiben soll.

Die Abs. 2 bis 4 sind dem § 53 Abs. 2, 3 und 5 SPG nachgebildet, wobei im Sinne der Verhältnismäßigkeit je nach Erforderlichkeit zur Aufgabenerbringung eine Einschränkung auf bestimmte Aufgaben in den einzelnen Ermächtigungen erfolgt. Wie im SPG wird den Staatsschutzbehörden ein automatisierter Datenabgleich iSd § 141 StPO („Rasterfahndung“) ausdrücklich untersagt.

Abs. 5 übernimmt mit einer geringfügigen Änderung im Wortlaut die Bestimmung des § 53 Abs. 4 SPG ins PStSG. Mit dem geänderten Wortlaut wird explizit auf Ermittlungen im Internet Bedacht genommen und zwar insoweit, als es sich um die Ermittlung von im Internet öffentlich zugänglichen Daten handelt. Damit soll hinsichtlich der Terminologie eine Parallele zu den öffentlichen Orten gemäß § 27 Abs. 2 SPG hergestellt werden. Unter „öffentlich zugänglichen Daten" sind all jene zu verstehen, die einem nicht von vornherein bestimmten Personenkreis im Internet zugänglich sind. Das bedeutet, dass von der Ermittlungsermächtigung jedenfalls die Ermittlung all jener Daten umfasst ist, die beim Surfen im Netz, in offenen Foren, Blogs oder Newsgroups jedermann zugänglich sind. Aber auch das Ermitteln in Foren oder sozialen Netzwerken, bei denen sich derjenige, der einen Zugang haben möchte, zwar mittels Nickname anmelden muss, ansonsten aber keine zusätzliche Sicherungsschranke vorhanden ist, ist von der Ermächtigung des Abs. 5 umfasst. Dass alleine das Zulegen eines Nickname für den Zutritt zu einem Forum dazu führen soll, die Daten als nicht-öffentlich zu beurteilen und daraus ein schutzwürdiges Geheimhaltungsinteresse abzuleiten, kann mit Blick auf die Literatur (Peter Burgstaller, Soziale Netzwerke- Eine rechtliche Einführung, lex:itec 02-03/12, 17; Henrichs/Wilhelm, Polizeiliche Ermittlungen in sozialen Netzwerken, Kriminalistik 1/2010, 35) und die Entscheidung des deutschen Bundesverfassungsgerichts, das sich in der Entscheidung vom 27. Februar 2008, 1 BvR 370/07 sehr ausführlich mit Ermittlungen im Internet auseinandersetze, verneint werden: Danach besteht im Internet kein schutzwürdiges Vertrauen *eines Kommunikationsteilnehmers in die Identität und Wahrhaftigkeit seiner Kommunikationspartner, da hierfür keinerlei Überprüfungsmechanismen bestehen*. Jedem Teilnehmer ist bewusst, so dass Bundesverfassungsgericht weiter, *dass er die Identität seiner Partner nicht kennt oder deren Angaben über sich jedenfalls nicht überprüfen kann. Sein Vertrauen darauf, dass er nicht mit einer staatlichen Stelle kommuniziert, ist in der Folge nicht schutzwürdig* (Rz 311).

Eine Ermittlung von öffentlich zugänglichen Daten im Internet gestützt auf Abs. 5 kommt weiters nur bei rein passiv-rezeptiven Erheben von Daten in Betracht; sollen Daten aktiv durch Kommunikation mit einem anderen ermittelt werden, also durch gezielte Interaktion mit anderen Nutzern iS einer Einholung von Auskünften, dann sind die Voraussetzungen für eine verdeckte Ermittlung nach § 11 zu prüfen.

Ebenso kann auf Abs. 5 keine Ermittlung von nicht öffentlichen Daten gestützt werden. Darunter sind Ermittlungen etwa in geschlossenen Foren zu verstehen, für die es kennzeichnend ist, dass sie nur einem beschränkten Teilnehmerkreis offen stehen (Stichwort „Freunde") und die Teilnahme an der Kommunikation in der Regel an die Erteilung einer gesonderten Berechtigung (eventuell unter Verwendung einer Verschlüsselung) geknüpft ist.

Zu § 11:

Für die Erfüllung der Aufgaben der erweiterten Gefahrenerforschung und des vorbeugenden Schutzes vor verfassungsgefährdenden Angriffen nennt § 11 taxativ besondere Ermittlungsmaßnahmen. Grundvoraussetzung für die jeweilige Maßnahme ist, dass vor ihrem Beginn die Ermächtigung des Rechtsschutzbeauftragten eingeholt und erteilt wird. Zusätzlich soll durch den Verweis auf § 9 im Einleitungssatz ausdrücklich zum Ausdruck gebracht werden, dass die im konkreten Fall eingesetzte Ermittlungsmaßnahme in einem angemessenen Verhältnis zum Anlass, nämlich zur befürchteten Straftat, stehen muss.

Die Ermittlungsmaßnahmen nach den Z 1 bis 3 entsprechen den derzeit bereits im Rahmen der Aufgabenerfüllung der erweiterten Gefahrenerforschung nach § 21 Abs. 3 SPG vorgesehenen Ermächtigungen. Durch den Verweis auf die Bestimmungen des SPG soll vermieden werden, Definitionen und alle weiteren Voraussetzungen sowie Einschränkungen, die sich bereits aus dem SPG ergeben, im PStSG neuerlich zu nennen.

Der Einsatz von Kennzeichenerkennungsgeräten (Z 4) soll auch zu Zwecken des Staatsschutzes zulässig sein. Im Unterschied zum Einsatz nach dem SPG erfolgt beim Einsatz dieser Geräte zur Erfüllung der Aufgaben nach dem PStSG kein Abgleich mit KFZ-Kennzeichen aus dem zentralen KFZ-Fahndungsdatenbestand, sondern mit KFZ-Kennzeichen, die in der Datenanwendung nach § 12 Abs. 1 verarbeitet werden. Eine Protokollierung aller KFZ-Kennzeichen, die durch das Kennzeichenerkennungssystem erfasst werden, erfolgt dabei ebenso wenig wie nach dem SPG. Nur Treffer werden protokolliert und solange gespeichert, als dies zur Erfüllung der Aufgabe erforderlich ist.

Die Notwendigkeit zur Einholung von Auskünften zu IP-Adressen (Z 5) hat sich auch für den Bereich der erweiterten Gefahrenerforschung in der Vergangenheit klar gezeigt, da sich die Aktivitäten der betroffenen Personen sehr stark vom realen in das virtuelle Leben verlagern. Daher ist es in Zukunft notwendig, IP-Adressen und die dahinterstehende Person durch die Einholung von Auskünften bei den Betreibern öffentlicher Telekommunikationsdienste und sonstigen Diensteanbietern ausforschen zu können. Nur dadurch kann etwa Postings im Internet, die einen verfassungsgefährdenden Angriff befürchten lassen, nachgegangen werden.

Durch die Verankerung der Zulässigkeit zur Einholung einer Auskunft zu Standortdaten im Bereich der erweiterten Gefahrenerforschung bzw. des vorbeugenden Schutzes vor verfassungsgefährdenden Angriffen werden die Behörden in die Lage versetzt, etwa bei verfassungsgefährdenden Angriffen, die zwar noch nicht in das Stadium der Vorbereitung (§ 16 Abs. 3 SPG) gelangt sind, aber doch schon sehr wahrscheinlich sind, den aktuellen Standort des potentiellen Gefährders auszuforschen. Zudem erlaubt es, mittels Standortdaten herauszufinden, ob eine vom Bundesamt als radikal eingestufte Person wieder in Österreich eingereist ist, mit der die Gefahr eines verfassungsgefährdenden Angriffs verbunden wäre.

Für beide Fälle der Einholung einer Auskunft (IP-Adresse und Standortdaten) ist der Kreis der potentiell Betroffenen ausdrücklich im Gesetz genannt: Diese Daten dürfen nur zu einer Gruppierung nach § 6 Abs. 1 Z 1, Betroffenen nach § 6 Abs. 1 Z 2 sowie zu deren Kontakt- oder Begleitpersonen (§ 12 Abs. 1 Z 4) eingeholt werden.

Die Erfahrungen mit Ermittlungen beim Verdacht der Teilnahme an Kampfhandlungen im Ausland haben gezeigt, wie wichtig Informationen zu möglichen Reisebewegungen der Betroffenen sind. Daher wird die Ermächtigung zur Einholung von Auskünften bei Personenbeförderungsunternehmen (Z 6), also natürlichen oder juristischen Personen, die gewerbsmäßig Personentransporte durchführen oder Transportmittel zur Verfügung stellen oder vermitteln, zu von ihnen erbrachten Leistungen ausdrücklich gesetzlich verankert. Zur Erteilung der Auskunft wären demnach beispielsweise Fluggesellschaften, Reisebüros oder Mietwagenfirmen verpflichtet. Eine Anregung aus dem Begutachtungsverfahren aufgreifend werden die zulässigerweise einzuholenden Daten taxativ genannt.

Im Sinne der Verhältnismäßigkeit ist die Einholung von Verkehrsdaten, Zugangsdaten und Standortdaten, die nicht einer Auskunft nach Abs. 1 Z 5 unterliegen, über einen bestimmten Zeitraum nur unter erschwerten Bedingungen zulässig. Es wird daher vorgeschlagen, dass die Einholung dieser Daten zur Vorbeugung eines verfassungsgefährdenden Angriffs, dessen Verwirklichung mit beträchtlicher Strafe bedroht (§ 17 SPG) ist, streng an die Erforderlichkeit gebunden wird und zusätzlich die Erfüllung der Aufgabe durch Einsatz anderer Ermittlungsmaßnahmen iSd § 11 Abs. 1 Z 1 bis 6 aussichtslos wäre. Die Notwendigkeit dieser Ermittlungsmaßnahme zeigt sich insbesondere im Zusammenhang mit der Rückkehr von Jihadkämpfern aus Syrien. Diese Maßnahme schafft die Grundlage zu ermitteln, mit welchen Personen der Betroffene vor der Abreise kommuniziert hat, um mögliche Schlepper sowie Personen, die den Betroffenen radikalisiert oder rekrutiert haben, ausfindig machen zu können. Ebenfalls sind seine Kontakte während des Aufenthalts im Ausland nach Österreich von besonderer Bedeutung für das Erkennen von Gefahrenpotential, da es sich dabei um Unterstützer, Mittäter, Geldgeber, zukünftige Jihadisten, die er angeworben hat, handeln könnte. Und schließlich kommt dem Wissen, wen der Betroffene nach seiner Rückkehr kontaktiert, im Lichte der Beurteilung, ob sich im Inland eine staatsschutzrelevante Aufgabe stellt, besonderes Gewicht zu.

In der Ermächtigung hat der Rechtsschutzbeauftragte festzulegen, für welchen (vergangenen und künftigen) Zeitraum die Verbindungsdaten eingeholt werden dürfen. In Anlehnung an die Bestimmung des § 138 Abs. 3 StPO hat das Bundesamt die der Ermittlungsmaßnahme zugrunde liegende Ermächtigung des Rechtsschutzbeauftragten bei seinem Ersuchen um Auskunft nach Abs. 1 Z 7 anzuführen und gleichzeitig der um Auskunft ersuchten Stelle neben der Verpflichtung nach Abs. 2 die Verpflichtung zur Geheimhaltung der Maßnahme aufzutragen.

Fallen während einer Ermittlungsmaßnahme die Voraussetzungen weg, ist die Maßnahme unverzüglich zu beenden.

Abs. 2 legt schließlich noch fest, dass die angefragten Stellen zur Auskunft verpflichtet sind und für bestimmte Auskünfte ein Kostenersatz, der sich nach der Überwachungskostenverordnung richtet, gebührt.

Zu § 12:

In § 12 Abs. 1 wird die vom Bundesamt und den Landesämtern im Informationsverbund geführte Datenanwendung verankert und durch Nennung von Betroffenenkreisen, Datenarten, Qualitätssicherungsmaßnahmen und Löschungsfristen näher determiniert. Die Führung einer gemeinsamen Datenanwendung versetzt den Staatsschutz in die Lage, österreichweit mögliche Bedrohungen und Gefahren ehestens zu erkennen, Querverbindungen zwischen einzelnen verfassungsgefährdenden Angriffen und dahinterliegenden Strukturen herstellen zu können sowie neue Ermittlungsansätze zu gewinnen. Aus der Datenanwendung und ihrem Zweck ergibt sich keine Ermächtigung, Daten zu ermitteln. Vielmehr setzt die Aufnahme von Daten in die Datenanwendung eine Ermächtigung zur Ermittlung derselben unter den Voraussetzungen und nach Maßgabe der §§ 10 und 11 PStSG bzw. nach dem SPG oder der StPO voraus.

Zu einer Gruppierung nach § 6 Abs. 1 Z 1 dürfen jene taxativ aufgezählten Daten gespeichert werden, die sich auf die Gruppierung selbst beziehen, also deren Aufenthalt oder Rechtsform. Natürliche Personen, die mit der Gruppierung in Verbindung stehen und die nicht schon nach Abs. 1 Z 2 oder 3 verarbeitet werden dürfen, werden nach Abs. 1 Z 4 verarbeitet, womit die Verpflichtung verbunden ist, den „Status“ dieser Personen möglichst rasch zu klären.

Unter Betroffenen nach § 6 Abs. 1 Z 2 sind jene natürlichen Personen zu verstehen, bei denen aufgrund bestimmter Anhaltspunkte ein begründeter Gefahrenverdacht besteht, dass sie einen verfassungsgefährdenden Angriff begehen werden.

Unter Verdächtige eines verfassungsgefährdenden Angriffs nach der Z 3 fallen sowohl Personen, gegen die im Zusammenhang mit der Abwehr eines gefährlichen Angriffs, der unter einen Tatbestand eines verfassungsgefährdenden Angriffs fällt, oder einer kriminellen Verbindung im Sinne des SPG ermittelt wird, als auch nach der StPO Verdächtige und Beschuldigte einer gerichtlich strafbaren Handlung, die unter die Definition des verfassungsgefährdenden Angriffs fällt, sowie Personen, die im Ausland im Verdacht stehen, einen verfassungsgefährdenden Angriff begangen zu haben (§ 6 Abs. 1 Z 3). Zu diesem Betroffenenkreis dürfen zwar die gleichen Datenarten wie zu Betroffenen nach der Z 2 verarbeitet werden; die Verarbeitung dient aber einer anderen Aufgabenerfüllung als bei Betroffenen nach Z 2 (Abwehr oder Aufklärung nach Maßgabe von SPG/StPO und nicht Vorbeugung), woran sich auch unterschiedliche Löschungsfristen knüpfen, weshalb Verdächtige als eigener Betroffenenkreis ausgewiesen werden sollen.

Kontakt- oder Begleitpersonen nach Z 4 sind Personen, bei denen nicht nur zufällig eine Verbindung zu einer Gruppierung nach der Z 1 oder Personen nach der Z 2 oder 3 besteht und über diesen Konnex ermittlungsrelevante Informationen zu diesen Personen oder Gefährdungen beschafft werden sollen. Wie der Z 4 sowie Abs. 3 letzter Satz zu entnehmen ist, sind die Ermittler ausdrücklich angehalten, den „Status“ dieser Personen möglichst rasch zu klären und ihre Daten zu löschen, wenn keine Gründe für die Annahme mehr vorliegen, dass über sie ermittlungsrelevante Informationen beschafft werden können (vgl. Weiss in Thanner/Vogl, SPG^2, § 53a Anm 22).

Die taxativ aufgezählten Datenarten entsprechen überwiegend der Bestimmung des § 53a SPG. Abweichungen ergeben sich insbesondere aus dem unterschiedlichen Zweck der Datenanwendung und den damit verbundenen Unterschieden bei den Betroffenenkreisen. Aufgrund der ausdrücklichen Ermächtigung dürfen auch sensible Daten im Sinne des § 4 Z 2 DSG 2000 zu allen Betroffenenkreisen verarbeitet werden, sofern dies unbedingt erforderlich ist und angemessene Vorkehrungen für die Geheimhaltung dieser Daten getroffen werden (vgl. § 9 PStSG).

Eine Datenanwendung erfüllt nur dann ihren Zweck, wenn die Qualität der darin enthaltenen Daten hoch gehalten wird. Eine verlässliche und handhabbare Qualitätssicherung ist daher unerlässlich. In diesem Sinn sollen Daten, bevor und während sie in der Datenanwendung verarbeitet werden, auf ihre Erheblichkeit und Richtigkeit geprüft werden. Erweisen sich Daten bei der periodisch stattfindenden Überprüfung als unrichtig, dann sind sie grundsätzlich entweder zu löschen oder richtig zu stellen. Eine Ausnahme davon soll für den Bereich des Staatsschutzes verankert werden, da sich diese bei ausländischen Staatsschutzbehörden als sinnvoll erwiesen hat: Ein einmal als Falschinformation identifizierter Datensatz soll anstelle der sofortigen Löschung als „unrichtig“ gekennzeichnet in der Datenanwendung erhalten bleiben, um bei nochmaligen Erhalt der Information sofort zu erkennen, dass es sich dabei um unrichtige Information handelt, etwa wenn es sich um die fälschliche Identifikation einer Person als Mitglied einer Terrorgruppe handelt. Die klare Kennzeichnung solcher Daten als unrichtig verhindert, dass sie irrtümlich als richtig weiterverarbeitet werden. Zuständig für die Aktualisierung oder Richtigstellung ist grundsätzlich jener Auftraggeber, der die Daten verarbeitet hat. Von diesem Grundsatz wird nur hinsichtlich jener Daten (Z 1 lit. a bis d und Z 2 lit. a bis j) abgegangen, deren Richtigkeit ein so hoher Stellenwert zukommt, dass auch ein anderer Auftraggeber diese Daten aktualisieren oder richtigstellen darf.

Abs. 3 legt fest, wann die Daten in der Datenanwendung nach Abs. 1 zu löschen sind. Die Löschungsfrist für die Gruppierung nach Z 1, den Betroffenen nach Z 2 sowie die dazugehörigen Personen nach Z 4 und 5 orientiert sich an der besonderen Löschungsregelung des § 13. Damit wird sichergestellt, dass die Daten in der Datenanwendung und im Akt gelöscht werden, wenn die zugrundeliegende Ermächtigung wegfällt bzw. die Frist nach Information des Betroffenen (§ 13 Abs. 2) abgelaufen ist, eine Weiterverarbeitung nach Ende der Ermächtigung nicht mehr erforderlich ist oder die Zustimmung des Rechtsschutzbeauftragten zur Weiterverarbeitung nicht erteilt wird, längstens aber nach sechs Jahren. Demgegenüber sind Daten von Verdächtigen nach Z 3 sowie allenfalls diesen zuordenbare Betroffene nach Z 4 und 5 längstens nach fünf Jahren zu löschen. Im Hinblick auf die Bedrohung, die von Verdächtigen eines verfassungsgefährdenden Angriffs ausgeht, ist eine Speicherdauer von längstens fünf

Jahren verhältnismäßig. Dem Auftrag in Abs. 1 Z 4, bei jeder Kontakt- und Begleitperson möglichst rasch eine Klärung der Beziehung zur Gruppierung bzw. zu den Personen nach Z 2 und 3 vorzunehmen, wird durch den letzten Satz von Abs. 3 Rechnung getragen, der anordnet, dass Daten zu Kontakt- oder Begleitpersonen jedenfalls sofort zu löschen sind, wenn keine Gründe für die Annahme mehr vorliegen, dass über sie für die Erfüllung der Aufgabe relevante Informationen beschafft werden können.

Abs. 4 weist die Übermittlungsempfänger aus. Rechtliche Grundlagen für den internationalen polizeilichen Austausch sind insbesondere im PolKG, EU-PolKG sowie im Europol-Übereinkommen zu finden.

Der Abs. 5 entspricht § 59 Abs. 2 SPG. Die Aufbewahrungsdauer der Protokolldaten orientiert sich an der in § 14 Abs. 5 DSG 2000 als Regelfall genannten Dauer von drei Jahren.

Wie für die Datenanwendungen in § 53a Abs. 2 SPG festgelegt, ist auch die Datenanwendung nach § 12 vor Aufnahme ihres Betriebes dem Rechtsschutzbeauftragten zur Stellungnahme nach § 91c Abs. 2 SPG vorzulegen.

Da im Rahmen von verdeckten Ermittlungen nach dem PStSG auch der Einsatz von Vertrauenspersonen künftig zulässig sein soll, bedarf es auch einer Regelung zur Evidenthaltung von Daten dieser Personen, nach Maßgabe des § 54b SPG. Mit der eigenständigen Verankerung in Abs. 7 soll erreicht werden, dass Daten zu Vertrauenspersonen, die dem Bundesamt oder den Landesämtern Informationen zu der ausschließlich sie betreffenden Aufgabenerfüllung nach dem PStSG oder SPG bzw. der StPO geben, von den übrigen Vertrauenspersonen nach dem SPG bzw. der StPO gesondert geführt werden.

Zu § 13:

§ 13 normiert eine besondere Regelung für die Löschung von Daten, die im Rahmen der Erfüllung der Aufgaben der erweiterten Gefahrenerforschung und des vorbeugenden Schutzes vor verfassungsgefährdenden Angriffen (§ 6 Abs. 1 Z 1 und 2) ermittelt wurden, wie sie derzeit in § 63 Abs. 1b SPG besteht. Dabei soll am Grundsatz, dass Daten zu löschen sind, wenn sich nach Ende der Ermächtigung weder nach dem PStSG noch nach dem SPG oder der StPO eine Aufgabe für die Staatsschutzbehörden stellt, festgehalten werden, jedoch nicht in der Absolutheit wie bislang: Denn mit der sofortigen Löschung ermittelter Daten ist nicht einfach nur ein Informationsverlust verbunden, sondern schlimmstenfalls eine massive Gefährdung der inneren Sicherheit des Staates, dessen Schutz gerade Aufgabe des polizeilichen Staatsschutzes ist.

Daher soll es im Einzelfall zulässig sein, Daten über das Ende der Ermächtigung hinaus zu speichern, auch wenn zu diesem Zeitpunkt keine aktuelle Gefährdungslage vorliegt. Wie die Erfahrungen zeigen, kann von bestimmten Personen, welche bereits in das Blickfeld von Ermittlungen durch den Staatsschutz geraten sind, zu einem späteren Zeitpunkt erneut eine Gefahr ausgehen. So stellt etwa das Abtauchen von unter polizeilicher Beobachtung stehenden Personen und/oder Gruppierungen im In- oder Ausland und deren späteres Wiedererscheinen in gleicher oder auch anderer Konstellation ein typisches Szeneverhalten dar. Durch eine (längere) Verfügbarkeit dieser Daten soll eine rasche Handlungsfähigkeit der Staatsschutzbehörden bei akuten Bedrohungen ermöglicht werden, anstelle bereits vorgelegene Erkenntnisse wiederholt beschaffen zu müssen. Darüber hinaus ist das Erkennen der Gefahr oft überhaupt erst möglich, wenn neue Umstände im Zusammenhang mit Vorinformationen gesehen werden.

Um den Anforderungen an einen modernen polizeilichen Staatsschutz und dem Grundrecht auf Datenschutz Rechnung zu tragen, soll es in jenen Fällen, in denen es Grund zur Annahme gibt, dass eine der ursprünglichen Anlasssituation vergleichbare Lage wieder eintreten, sich also erneut eine Aufgabe nach § 6 Abs. 1 Z 1 oder 2 stellen werde, zulässig sein, die Daten bis zu zwei Jahre nach Ablauf der Zeit, für die die Ermächtigung erteilt wurde, zu speichern. Um die Verhältnismäßigkeit zu wahren, ist neben dieser Höchstfrist eine jährliche Prüfung des weiteren Verarbeitungsbedarfs vorgesehen, um sicherzustellen, dass Daten vor Ablauf der Höchstfrist gelöscht werden, wenn sie im Einzelfall tatsächlich nicht mehr benötigt werden. Sollte nach Ablauf von zwei Jahren eine Weiterverarbeitung aus Sicht der Staatsschutzbehörden erforderlich sein, dann bedarf dies der Ermächtigung des Rechtsschutzbeauftragten, demgegenüber jene Gründe anzugeben sind, die eine Weiterverarbeitung für ein Jahr begründen. Eine Verlängerung der Verarbeitung durch Ermächtigung des Rechtsschutzbeauftragten soll bis zu einer Höchstfrist von sechs Jahren, gerechnet ab dem Ende der erteilten Ermächtigung, zulässig sein.

Zudem muss für den Fall der Information des Betroffenen nach Ende der Ermächtigung gemäß § 16 Abs. 2 sichergestellt sein, dass die Daten für ein allfälliges Beschwerdeverfahren noch vorhanden sind. Dem trägt Abs. 2 Rechnung, indem er als lex specialis zu Abs. 1 das Bundesamt und die Landesämter verpflichtet, die Daten jedenfalls sechs Monate nach ergangener Information des Betroffenen aufzubewahren. Diese Frist verlängert sich um jenen Zeitraum, als die Information an den Betroffenen

nach § 16 Abs. 3 aufgeschoben wird. Und schließlich muss sichergestellt sein, dass die nach diesem Bundesgesetz ermittelten Daten bis zum Ende eines Rechtsschutzverfahrens vorhanden sind.

Zu § 14:

Der besondere Rechtsschutz für die Aufgaben der erweiterten Gefahrenerforschung und des vorbeugenden Schutzes vor verfassungsgefährdenden Angriffen (§ 6 Abs. 1 Z 1 und 2) sowie die Kontrolle der Datenanwendung nach § 12 Abs. 6 iVm § 91c Abs. 2 SPG wird beim Rechtsschutzbeauftragten nach dem SPG angesiedelt, da sich diese Institution seit Jahren als unabhängige Kontrollinstanz bewährt hat und die besonderen Ernennungsvoraussetzungen Gewähr für eine unabhängige Amtsausübung bieten. Um auch gesetzlich Vorsorge zu treffen, dass der Rechtsschutzbeauftragte über die erforderlichen Personal- und Sachressourcen verfügt, wird in § 91a Abs. 1 SPG die derzeitige fixe Anzahl von Stellvertretern (zwei) auf die erforderliche Anzahl von Stellvertretern geändert. Zusätzlich wird in § 91a SPG ausdrücklich klar gestellt, dass der Rechtsschutzbeauftragte und seine Stellvertreter nicht nur bei Besorgung der ihnen nach dem SPG, sondern auch nach dem PStSG zukommenden Aufgaben unabhängig und weisungsfrei sind. Ergänzt wird der kommissarische Rechtsschutz durch eine umfassende Bestimmung zur Informationspflicht von Betroffenen der genannten Aufgaben, deren Erfüllung wiederrum der Kontrolle des Rechtsschutzbeauftragten obliegt. Und schließlich werden umfassende Berichtspflichten an den ständigen Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit (Art. 52a B-VG) verankert.

Wie schon bisher für die Aufgabe der erweiterten Gefahrenerforschung in § 91c Abs. 3 SPG vorgesehen, dürfen Ermittlungshandlungen zur Erfüllung dieser Aufgabe nur nach vorhergehender Ermächtigung des Rechtsschutzbeauftragten begonnen werden, der ein begründetes Ersuchen des Bundes- oder Landesamtes zugrunde liegt. Soll eine Vertrauensperson im Rahmen einer verdeckten Ermittlung tätig werden, so sind im Ersuchen um Ermächtigung zu dieser Ermittlungsmaßnahme die Gründe für ihren Einsatz entsprechend darzulegen. An dem bewährten System – Einholung der Ermächtigung zur Durchführung der Aufgabe sowie zu den jeweils gesondert zu beantragenden besonderen Ermittlungsmaßnahmen - soll somit festgehalten werden. Damit ist sichergestellt, dass keine Ermittlungsmaßnahme zur Erfüllung der Aufgaben nach § 6 Abs. 1 Z 1 und 2 beginnt, ohne dass der Rechtsschutzbeauftragte dazu die Ermächtigung erteilt hat.

Die Ermächtigung des Rechtsschutzbeauftragten wird in Hinkunft jeweils für die Dauer von höchstens sechs Monaten erteilt werden können, wobei eine (auch mehrmalige) Verlängerung für diese Dauer zulässig ist. Dies stellt sicher, dass die Staatsschutzbehörden in periodischen Abständen die Notwendigkeit und Erforderlichkeit der Maßnahme gegenüber dem Rechtsschutzbeauftragten begründen müssen und dieser aufgrund der zwischenzeitig erlangten Erkenntnisse entscheiden kann, ob die Voraussetzungen für eine Verlängerung der Maßnahme vorliegen. Zudem soll die derzeit schon bestehende Praxis des Rechtsschutzbeauftragten, Ermächtigungen zu Ermittlungsmaßnahmen mitunter nur (sachlich oder örtlich) eingeschränkt zu erteilen, auch im Gesetzestext zum Ausdruck kommen.

Zu § 15:

Die Bestimmung regelt die Rechte und Pflichten des Rechtsschutzbeauftragten und entspricht im Wesentlichen § 91d SPG. Eine Anregung aus dem Begutachtungsverfahren aufgreifend soll der sogenannte Quellenschutz gegenüber dem Rechtsschutzbeauftragten mit einer, der Strafprozessordnung nachgebildeten Ausnahme entfallen. Nur in jenem Umfang, in dem § 162 StPO zulässigerweise eine Geheimhaltung der Identität einer Person gegenüber den Strafverfolgungsbehörden vorsieht, soll dies auch gegenüber dem Rechtsschutzbeauftragten zulässig sein.

Zu § 16:

§ 16 verankert eine umfassende Informationspflicht von Betroffenen, deren personenbezogene Daten im Rahmen der Erfüllung der Aufgabe der erweiterten Gefahrenerforschung und des vorbeugenden Schutzes vor verfassungsgefährdenden Angriffen verarbeitet werden, die die bereits derzeit bestehende Regelung über die Informationsverpflichtung bei Verletzung von Rechten Betroffener durch das Verwenden personenbezogener Daten (§ 91d Abs. 3 SPG) ergänzt. Um einerseits dem Grundrecht auf Schutz des Privatlebens und Achtung der Privatsphäre (Art. 8 EMRK) und anderseits überwiegenden öffentlichen Interessen, die sich aus der Notwendigkeit des Schutzes der verfassungsmäßigen Einrichtungen oder der Vorbeugung, Verhinderung und Verfolgung von Straftaten ergeben, Rechnung zu tragen, sieht der Entwurf folgende Regelung vor:

Grundsätzlich soll jeder Betroffene einer Aufgabe nach § 6 Abs. 1 Z 1 und 2 nach Ablauf der Zeit, für die die Ermächtigung erteilt wurde, vom Bundes- oder Landesamt über Grund, Art und Dauer sowie die Rechtsgrundlage der gesetzten Maßnahmen informiert werden. Diese Information eröffnet dem

Betroffenen die Möglichkeit, gegen die gesetzten Maßnahmen Rechtsmittel, etwa nach § 88 SPG, zu ergreifen.

Der vorgesehene Aufschub oder das Unterbleiben der Information in Abs. 3 ist vor dem Hintergrund der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte zu sehen, der im Urteil Klass gegen die Bundesrepublik Deutschland vom 6. September 1978 feststellte, dass eine nachträgliche Mitteilung den langfristigen Zweck einer Überwachung in Frage stellen würde und deshalb unter bestimmen Voraussetzungen unterlassen werden dürfe. Er hielt unter anderem Folgendes fest: „*Eine nachträgliche Benachrichtigung jeder Person, die einmal von einer inzwischen aufgehobenen Maßnahme betroffen worden ist, könnte sehr wohl den langfristigen Zweck gefährden, der seinerzeit die Anordnung ausgelöst hat. Wie das BVerfG richtig festgestellt hat, könnte eine solche Bekanntgabe außerdem zur Aufdeckung von Arbeitsweise und Beobachtungsfeldern der Geheimdienste führen und möglicherweise sogar zur Identifizierung ihrer Agenten beitragen. Insoweit der sich aus den angefochtenen Vorschriften ergebende Eingriff nach Artikel 8 Absatz 2 EMRK gerechtfertigt ist […], kann es nach Ansicht des Gerichtshofes mit dieser Bestimmung nicht unvereinbar sein, dass der Betroffene nach Beendigung der Überwachungsmaßnahme nicht unterrichtet wird, da es gerade dieser Umstand ist, welcher die Wirksamkeit des Eingriffs sicherstellt.*“

In diesem Sinn soll es zulässig sein, die Information nach Ende der Ermächtigung solange aufzuschieben, als andernfalls der Zweck der bereits gegen den Betroffenen gesetzten Maßnahmen gefährdet wäre, etwa wenn aufgrund bestimmter Tatsachen angenommen werden kann, dass von ihm zu einem bestimmten Zeitpunkt (etwa bei neuerlicher Einreise ins Bundesgebiet) erneut eine Gefahr ausgehen kann. Ein weiterer Aufschiebegrund kann darin liegen, dass durch die Information des Betroffenen ein anderes Verfahren gefährdet wäre, weil es etwa in engem sachlichen Zusammenhang steht. Die Information des Betroffenen kann unterbleiben, wenn diese unmöglich ist, was etwa bei Abgängigkeit oder unbekannten Aufenthalt des Betroffenen der Fall ist, oder eine Information des Betroffenen aus den Gründen des § 26 Abs. 2 DSG 2000 nicht erfolgen kann. Über die Zulässigkeit des Aufschubs, wozu auch die Dauer des Aufschubs gehört, bzw. des Unterbleibens der Information entscheidet in jedem Einzelfall der Rechtsschutzbeauftragte.

Zu § 17:

Eine umfassende Berichtspflicht ergänzt den Rechtsschutz und gibt über die Tätigkeit der Staatsschutzbehörden Aufschluss:

Dem Anliegen nach verstärkter Transparenz Rechnung tragend soll das Bundesamt einmal jährlich die Öffentlichkeit über die aktuellen Entwicklungen auf dem Gebiet des polizeilichen Staatsschutzes informieren.

Zudem berichtet der Bundesminister für Inneres dem ständigen Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit jedenfalls halbjährlich darüber, welche Aufgaben sich auf Grundlage des PStSG stellen, etwa in Form von Lagebildern, welche Maßnahmen von Seiten der Staatsschutzbehörden gesetzt werden und auf welche Art und Weise die Verständigung Betroffener nach Ende der Ermächtigung erfolgt.

Und schließlich soll der Bericht des Rechtsschutzbeauftragten über seine Tätigkeit und Wahrnehmungen bei Erfüllung der Aufgaben der erweiterten Gefahrenerforschung und des vorbeugenden Schutzes vor verfassungsgefährdenden Angriffen dem ständigen Unterausschuss des Ausschusses für innere Angelegenheiten nach Art. 52a B-VG im Rahmen seines Auskunfts- und Einsichtsrechtes zugänglich gemacht werden.

Zu §§ 18 bis 22:

Es handelt sich um die Inkrafttretensbestimmung, die erforderlichen Übergangsbestimmungen sowie die allgemeinen Schlussbestimmungen.

Artikel 2

Zu Z 1 (Inhaltsverzeichnis):

Diese Bestimmung dient der Aktualisierung des Inhaltsverzeichnisses.

Zu Z 2, 6, 8, 10, 14 und 23 bis26 (§§ 6 Abs. 1, 21 Abs. 3, 53 Abs. 1, 3 bis 5, 54 Abs. 2 und 4, 63 Abs. 1a und 1b, 91a Abs. 1, 91c Abs. 1 und 3, 91d sowie 93a SPG):

Es handelt sich um Anpassungen, die aufgrund der Schaffung eines Polizeilichen Staatsschutzgesetzes (PStSG) notwendig sind, sowie um die Beseitigung eines Redaktionsversehens.

Zu Z 3 (§ 13a Abs. 3 SPG):

Mit dieser Bestimmung soll eine gesetzliche Grundlage für den offenen Einsatz von Bild- und Tonaufzeichnungsgeräten, etwa von sogenannten „body worn cameras“, zum Zweck der Dokumentation von Amtshandlungen, bei denen die Organe des öffentlichen Sicherheitsdienstes Befehls- und Zwangsgewalt ausüben, geschaffen werden. Um einerseits den schutzwürdigen Geheimhaltungsinteressen des Betroffenen und der Wahrung seines Rechts auf informationelle Selbstbestimmung und anderseits dem Interesse des Staates an der Strafverfolgung, der Kontrolle der Rechtmäßigkeit von Amtshandlungen sowie einer an den technischen Möglichkeiten ausgerichteten Dokumentation Rechnung zu tragen, sieht der Entwurf folgende Vorkehrungen vor:

Der Einsatz von Bild- und Tonaufzeichnungsgeräten zum Zweck der Dokumentation kommt nur bei Amtshandlungen, bei denen Befehls- und Zwangsgewalt ausgeübt wird, in Betracht. Ein dauernder Einsatz im regulären Streifendienst scheidet damit von vornherein aus. Da mit dem Einsatz von Bild- und Tonaufzeichnungsgeräten auch ein präventiver Zweck verbunden ist, indem die Beteiligten wissen, dass ihr Verhalten videodokumentiert wird, ist vor Beginn der Aufzeichnung der Einsatz gegenüber dem Betroffenen anzukündigen.

Mit der Formulierung, wonach der Einsatz von Bild- und Tonaufzeichnungsgeräten gestützt auf § 13a Abs. 3 nur zulässig ist, sofern gesetzlich nicht Besonderes bestimmt ist, soll klargestellt werden, dass bereits bestehende Sonderregelungen, etwa nach § 54 SPG, §§ 97 und 149 StPO oder dem XIII. Abschnitt der StVO von der Regelung des § 13a Abs. 3 unberührt bleiben.

Die Auswertung der Aufzeichnungen ist auf zwei im Entwurf ausdrücklich genannte Zwecke beschränkt: Die Aufzeichnungen dürfen nur zur Verfolgung von strafbaren Handlungen, die sich während der Amtshandlung ereignet haben, und zur Kontrolle der Rechtmäßigkeit der Amtshandlung ausgewertet werden, etwa um nachträglich gegen das Einschreiten der Exekutive vorgebrachten Vorwürfen nachgehen zu können oder um strafrechtliches Verhalten aufzuklären. Zum Zweck der Verfolgung von strafbaren Handlungen ist eine Übermittlung an die Strafverfolgungsbehörden und zur Kontrolle der Rechtmäßigkeit der Amtshandlung etwa an die Verwaltungsgerichte zulässig; die weitere Verwendung und Löschung richtet sich nach den materienspezifischen Regelungen.

Bis zu ihrer Auswertung oder Löschung sind die Aufzeichnungen gemäß den Bestimmungen des § 14 DSG 2000 vor unberechtigter Verwendung zu sichern; insbesondere ist sicherzustellen, dass jeder Zugriff protokolliert wird und die Daten durch Verschlüsselung gesichert verwahrt werden. Mit der Aufbewahrungsfrist von sechs Monaten soll sichergestellt werden, dass einerseits die Aufzeichnungen bei einem allfälligen Rechtsschutzverfahren zu Beweiszwecken noch vorhanden sind und es somit auch nicht im Ermessen der Behörde liegt, diese Aufnahmen unmittelbar nach der Amtshandlung zu löschen, und anderseits nach Ende dieser Frist - mit Ausnahme eines noch andauernden Rechtsschutzverfahrens - eine Löschung dieser Aufnahmen zwingend zu erfolgen hat.

Da die Regelung des § 13a Abs. 3 im organisationsrechtlichen Teil des SPG verankert werden soll, wird ein Verweis auf die Wahrung der Verhältnismäßigkeit iSd § 29 ausdrücklich in die Vorschrift aufgenommen, um sicherzustellen, dass bei jedem Einsatz dieser Geräte die Grundsätze des § 29 beachtet werden.

Zu Z 4 und Z 7 (§§ 20 und 25 SPG):

Es handelt sich um eine terminologische Anpassung, da es sich bei der in § 25 vorgesehenen Beratung nicht um eine Aufgabe der Kriminalpolizei im Dienste der Strafrechtspflege gem. § 18 StPO handelt, sondern um die Vorbeugung und Verhütung von Straftaten im Rahmen der Sicherheitspolizei [vgl. Leitner, in Thanner/Vogl (Hrsg.) SPG^2 § 25 Anm 1]. Das soll auch in der Überschrift zum Ausdruck kommen.

Zu Z 5 (§ 21 Abs. 2a SPG):

Die Tätigkeit von Organen des öffentlichen Sicherheitsdienstes an Bord von Zivilluftfahrzeugen leitete sich bislang aus § 125 LFG iVm § 5 Z 3 Sondereinheiten-Verordnung ab. Gemäß § 125 LFG hat der Pilot alle zur Aufrechterhaltung von Ordnung und Sicherheit an Bord notwendigen Maßnahmen zu treffen. Diese nationale Regelung findet ihre völkerrechtliche Grundlage in Art. 6 des Abkommens über strafbare und bestimmte andere an Bord von Luftfahrzeugen begangene Handlungen (Tokioter Abkommen) vom 14. September 1963, BGBl. Nr. 247/1974. Auf der Diplomatischen Konferenz zur Änderung des Tokioter Abkommens, die vom 26. März bis 4. April 2014 in Montréal/Kanada stattfand, wurde die Verankerung des Begriffs des „in-flight security officer (IFSO)“ im Tokioter Abkommen beschlossen. Die Änderungen befinden sich noch im Ratifikationsprozess, doch wird hinsichtlich der IFSOs lediglich die ohnehin bereits bestehende internationale Staatenpraxis festgeschrieben. Mit dem geänderten Art. 6 Abs. 2 wird

erstmals eine multilaterale völkerrechtliche Regelung für den Einsatz von IFSOs geschaffen. Es bedarf aber auch einer entsprechenden nationalen Regelung. Dass eine solche Regelung notwendig ist, wird aus Punkt 3.2. des Erkenntnisses des VfGH vom 6. März 2001, B 159/00 (VfSlg. 16.109/2001) deutlich. Darin heißt es: „Letztlich brachte die belangte Behörde in ihrem Bescheid auch vor, daß an Bord des Flugzeuges (einer bulgarischen Fluglinie) keine Akte unmittelbarer verwaltungsbehördlicher Befehls- und Zwangsgewalt gesetzt worden wären, weil die Befehlsgewalt an Bord ausschließlich dem Kapitän des Flugzeuges zugekommen sei. Auch mit dieser Erwägung ist die belangte Behörde nicht im Recht: Sie übersieht, daß aus dem Umstand, daß die Rechtsordnung unter bestimmten Voraussetzungen keine Befugnisse zu Befehls- und Zwangsmaßnahmen einräumt, nicht abgeleitet werden kann, daß staatliche Organe, die zumindest in abstracto mit Hoheitsgewalt betraut sind, nicht dennoch - wenn dann auch ex definitione: rechtswidrige - Akte unmittelbarer verwaltungsbehördlicher Befehls- oder Zwangsgewalt gesetzt haben."

Nachdem nunmehr der Einsatz von IFSOs einer völkerrechtlichen Klärung zugeführt wurde, soll mit der Regelung des § 21 Abs. 2a gesetzlich verankert werden, dass österreichische Exekutivbeamte, die speziell für den Sicherheitsdienst an Bord ausgebildet und geschult sind (siehe § 5 Z 3 Sondereinheiten-Verordnung), unter den in Abs. 2a genannten Voraussetzungen an Bord eines Flugzeuges zur Ausübung unmittelbarer verwaltungsbehördlicher Befehls- und Zwangsgewalt in dem Ausmaß befugt sind, als es um die Abwehr und Beendigung von gefährlichen Angriffen gegen Leben, Gesundheit, Freiheit oder Eigentum geht. Die Aufgabe bezieht sich primär auf Zivilluftfahrzeuge, die der österreichischen Hoheitsgewalt unterliegen. Ein Zivilluftfahrzeug unterliegt der österreichischen Hoheitsgewalt, wenn es sich in Österreich einschließlich des österreichischen Luftraums befindet oder es sich um ein in Österreich registriertes Flugzeug (§§ 15 f LFG) handelt, das sich in oder über einem fremden Staat oder über der Hohen See „im Flug" befindet. Befindet sich das Flugzeug „im Flug", bedarf es dazu außerhalb des österreichischen Hoheitsgebiets aufgrund völkerrechtlicher Vorgaben des Einvernehmens mit dem verantwortlichen Piloten. Dieses Einvernehmen wird vorausgesetzt, wenn die Organe des öffentlichen Sicherheitsdienstes auf begründetes Ersuchen des Luftfahrzeughalters oder zur Erfüllung gesetzlicher Aufgaben (etwa im Rahmen des vorbeugenden Rechtsschutzes oder einer Abschiebung) an Bord sind. Eine Anregung aus dem Begutachtungsverfahren aufgreifend soll die Einschränkung auf österreichische Zivilluftfahrzeuge entfallen, da bereits durch die im zweiten Satzteil des § 21 Abs. 2a vorgesehenen Beschränkungen (Ersuchen des Luftfahrzeughalters bzw. Erfüllung gesetzlicher Aufgaben und Einhaltung des Völkerrechts) ohnehin sicher gestellt ist, dass den Sicherheitsbehörden nicht die Abwehr und Beendigung von gefährlichen Angriffen weltweit an Bord eines jeden Zivilluftfahrzeugs obliegt.

Zu Z 9 (§ 53 Abs. 3b SPG):

Bislang ist die Standortfeststellung auf gefährdete Personen und Begleitpersonen beschränkt. Im Rahmen der Aufgabe der Gefahrenabwehr soll es aber auch zulässig sein, Standortdaten des Gefährders zu ermitteln, wenn es gilt, eine gegenwärtige Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen abzuwehren. Davon wären Fälle erfasst, in denen etwa eine Person ankündigt, den Flughafen in die Luft zu sprengen oder eine Bombe zu zünden. Dass es sich dabei um eine ureigene Aufgabe der Sicherheitspolizei auf dem Gebiet der Abwehr von Gefahren und nicht der Kriminalpolizei handelt, sollte auch in einer entsprechenden Regelung des SPG zum Ausdruck kommen.

Zu Z 11 bis 13 (§ 53a SPG):

Die Führung einer Datenanwendung für den Personen- und Objektschutz wird aus dem Abs. 1 herausgelöst und in Abs. 1a einer eigenständigen Regelung, in der die für diesen Zweck benötigten Datenarten taxativ aufgezählt werden, zugeführt. Zudem sollen das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung und die Landesämter Verfassungsschutz (§ 1 Abs. 4 PStSG) für bestimmte Zwecke des Staatsschutzes ermächtigt sein, diese Datenanwendung im Informationsverbundsystem zu führen.

Zu Z 15 und 16 (§ 54 Abs. 3 und 3a SPG):

Bislang geht die herrschende Meinung davon aus, dass der Einsatz von Vertrauenspersonen für die verdeckte Ermittlung nach dem geltenden Wortlaut des § 54 Abs. 3 SPG im Unterschied zur StPO nicht zulässig ist [vgl. zuletzt Wiederin, Vertrauenspersonen als verdeckte Ermittler nach dem SPG und als Scheinkäufer nach der StPO?, in Reindl-Krauskopf ua (Hrsg.) Festschrift für Helmut Fuchs, 657; aA Zerbes, WK-StPO § 129 Rz 30]. Mit dieser Änderung soll der Einsatz von Vertrauenspersonen im SPG einer mit der StPO abgestimmten Regelung zugeführt werden, da deren Einsatz vor allem für Ermittlungen bei kriminellen Organisationen oder auf dem Gebiet des polizeilichen Staatsschutzes als notwendig erkannt wird. In diesen Bereichen erweist es sich nämlich in der Praxis aufgrund äußerst konspirativ agierender Personenkreise und vorhandener Sprachbarrieren äußerst schwierig, als verdeckte Ermittler tätige Organe der Sicherheitsbehörden einzuschleusen. Da es verfassungsrechtlich für die

Zulässigkeit der Einbindung privater Personen als Hilfsorgane des Staates geboten ist, dass die staatlichen Behörden, denen das von den Privaten gesetzte Verhalten zugerechnet wird und die es vor den Verwaltungsgerichten zu vertreten haben, dieses Verhalten effektiv zu beeinflussen vermögen, sind entsprechend der Regelung in § 131 StPO in Abs. 3a gewisse Führungs-, Überwachungs- und Dokumentationspflichten vorgesehen. Wie diese Pflichten nach der StPO in der Praxis umgesetzt werden sollen, ist derzeit schon in einem eigenen Erlass des BM.I geregelt (vgl. Zerbes, WK-StPO § 131 Rz 12). Davon umfasst sind etwa die Bindung der Vertrauensperson an die Anweisungen ihres Vertrauenspersonführers und die Dokumentation von Anweisungen, Richtlinien für den Kontakt zwischen Vertrauensperson und Vertrauenspersonführer sowie die sorgfältige Kontrolle der Vertrauensperson. Damit soll der behördliche Einfluss auf in die staatliche Tätigkeit eingebundene Private gewährleistet werden.

Zu Z 17 (§ 54 Abs. 5 SPG):

Mit der Änderung des § 54 Abs. 5 soll der Einsatz von Bild- und Tonaufzeichnungsgeräten auch im sachlichen, zeitlichen und örtlichen Zusammenhang mit einer Zusammenkunft zahlreicher Menschen, bei der gefährliche Angriffe gegen Leben, Gesundheit oder Eigentum befürchtet werden, gesetzlich verankert werden. Dadurch soll es ermöglicht werden, dass diese Geräte etwa auch bei Aufsplitterungen kleinerer Gruppen im Zusammenhang mit solchen Zusammenkünften zum Zweck der Vorbeugung zum Einsatz gelangen können.

Wie in § 54 Abs. 6 sollen die Bild- und Tonaufzeichnungen, die unter den Voraussetzungen des § 54 Abs. 5 ermittelt wurden, nicht nur für die Zwecke der Verfolgung von gerichtlich strafbaren Handlungen, sondern auch zur Verfolgung von solchen Verwaltungsübertretungen, die sich typischerweise bei Demonstrationen oder Sportgroßveranstaltungen ereignen, verwendet werden dürfen. Wie der Entschließung betreffend Reglementierung pyrotechnischer „Signalstifte“, 61/E, 25. GP vom 10. Dezember 2014, und den diesbezüglichen Ausführungen im Bericht des Ausschusses für innere Angelegenheiten, AB 411 BlgNR 25. GP, zu entnehmen ist, stellen Verwaltungsübertretungen, insbesondere nach dem PyrotechnikG 2010 bei Sportgroßveranstaltungen ein großes Gefahrenpotential dar. Schon alleine daraus ergibt sich die Notwendigkeit der Verwendung von Bild- und Tonaufzeichnungen auch für die Verfolgung von Verwaltungsübertretungen, stellt das bei der Sicherheitsbehörde vorhandene Videomaterial doch oftmals die einzige Möglichkeit zur Ausforschung der Betroffenen dar.

Zu Z 18 (§ 58b Abs. 2 SPG):

Es handelt sich um eine Anpassung an das BFA-VG.

Zu Z 19 (§ 59 Abs. 2 SPG):

Von der Zuordnung der Abfrage oder Übermittlung zu einem bestimmten Organwalter soll abgesehen werden können, wenn es sich um automatisierte Abfragen handelt, da bei solchen Anfragen die gesamte Datenverwendung programmgesteuert erfolgt und nicht aufgrund der Entscheidung eines Organwalters. Solche Abfragen erfolgen etwa gemäß § 16a Abs. 11 MeldeG.

Zu Z 20 (§ 75 Abs. 1a SPG):

Mit § 75 Abs. 1a soll eine ausdrückliche gesetzliche Grundlage im SPG für die Verarbeitung von Spuren, die auf Grundlage der Strafprozessordnung ermittelt worden sind, zum Zweck ihrer Zuordnung zu einer Person geschaffen werden. Davon umfasst sind ausschließlich solche Spuren, die durch erkennungsdienstliche Maßnahmen gem § 64 Abs. 2 ermittelt werden können, also insbesondere Papillarlinienabdrücke, DNA-Profile oder Abbildungen, und die somit eindeutig einer bestimmten Person zuordenbar sind. Für die Verarbeitung in der Zentralen erkennungsdienstlichen Evidenz ist zudem entscheidend, dass im Zeitpunkt der Verarbeitung Grund zur Annahme besteht, dass die Spur einer Person, die im Verdacht steht, eine mit gerichtlicher Strafe bedrohte vorsätzliche Handlung begangen zu haben, zugehört oder zugehören dürfte. Das Ziel der Speicherung ist die Zuordnung der Spur zu einer verdächtigen Person, worunter auch der Nachweis mehrerer Straftaten für den Fall eines Spur-Spur Treffers fällt. Vergleichbar mit den in Abs. 1 von § 75 genannten Identitätsdaten dürfen zur Spur nur Verwaltungsdaten verarbeitet werden, um im Anlassfall („Trefferfall“) eine Zuordnung der Spur zum bezughabenden kriminalpolizeilichen Akt herstellen zu können. Unter Verwaltungsdaten sind interne Bearbeitungsvermerke wie Sachbearbeiter, Aktenzahl oder Dienststelle zu verstehen [vgl. Weiss in Thanner/Vogl (Hrsg.) SPG^2, § 53a Anm 14].

Die Voraussetzungen für die Übermittlung von strafprozessual ermittelten Spuren in die Zentrale erkennungsdienstliche Evidenz ergeben sich aus § 76 Abs. 4 StPO idF BGBl. I Nr. 71/2014. Daraus folgt, dass etwa DNA-Spuren nur unter den Voraussetzungen des § 124 Abs. 5 StPO iVm § 67 Abs. 1 erster

Satz SPG, also bei Vorliegen einer mit mindestens einjähriger Freiheitsstrafe bedrohten Vorsatzstraftat, verarbeitet werden dürfen.

Die Daten sind zu löschen, wenn der für die Speicherung maßgebliche Verdacht nicht mehr besteht, wenn sich also herausstellt, dass die Spur von einer nicht im Verdacht stehenden Person hinterlassen wurde. Im Übrigen richtet sich der Zeitpunkt der Löschung nach der Löschungsfrist des bezughabenden kriminalpolizeilichen Aktes.

Zu Z 21 (§ 75 Abs. 2 SPG):

Mit der Änderung des ersten Satzes soll klar zum Ausdruck gebracht werden, dass die Sicherheitsbehörden ermächtigt sind, die von ihnen in der Zentralen erkennungsdienstlichen Evidenz gespeicherten Daten nach Abs. 1 und Abs. 1a miteinander zu vergleichen. Davon umfasst ist auch der aufgrund neuerster technischer Entwicklungen mögliche automationsunterstützte Vergleich von Lichtbildern. Daneben sind Abfragen und Übermittlungen von Daten nach Abs. 1 und Abs. 1a im Dienste der Sicherheitspolizei, der Strafrechtspflege und für andere Aufgaben der Sicherheitsverwaltung zum Zwecke der Wiedererkennung zulässig, jedoch nur insoweit, als die Regelungen in den jeweiligen Materiengesetzen dies zulassen. In diesem Zusammenhang ergeben sich etwa Schranken aus dem Passgesetz 1992: Eine Abfrage in der zentralen Evidenz nach dem PassG mit einem Lichtbild bzw. Papillarlinienabdruck scheidet nach den Bestimmungen der §§ 22a Abs. 3 erster Satz iVm 22b Abs. 4 und § 22b Abs. 1 Passgesetz aus.

Zu Z 22 (§ 80 Abs. 1a SPG):

Mit § 80 Abs. 1a soll das Auskunftsrecht nach § 26 DSG 2000 im Hinblick auf gem. § 75 Abs. 1a verarbeitete Spuren konkretisiert werden. Da es für diese Art von Auskunft notwendig ist, entsprechendes Vergleichsmaterial herzustellen, hängt die Erteilung einer entsprechenden Auskunft von einer den Auskunftswerber treffenden Mitwirkungspflicht sowie der Pflicht zur Tragung des Kostenersatzes, der in der Sicherheitsgebührenverordnung zu verankern wäre, ab. Das unter Mitwirkung des Auskunftswerbers hergestellte Vergleichsmaterial ist bis zu seiner Löschung gesondert zu verwahren und das Ergebnis der Auskunft für ein allfälliges Beschwerdeverfahren zu dokumentieren. Soweit in Abs. 1a keine besondere Regelung getroffen wird, kommt § 26 DSG 2000 zur Anwendung, woraus folgt, dass der Auskunftswerber etwa seine Identität in geeigneter Form nachzuweisen hat.

Zu Z 27 und 28 (§§ 94 Abs. 38 und 39, 96 Abs. 8 SPG):

Es handelt sich um die Inkrafttretensbestimmungen sowie die Übergangsbestimmung für Datenanwendungen nach § 53a Abs. 1 für den Personen- und Objektschutz.

Zu Z 29 (§ 97 Abs. 4 SPG):

Die vorgeschlagene Änderung in § 13a Abs. 3 SPG soll zur Gewinnung von Erfahrungen in diesem Bereich vorläufig nur befristet in Kraft gesetzt werden. Innerhalb eines Zeitraumes von mehr als drei Jahren soll es möglich sein, die notwendigen Erfahrungswerte über die durch Bild- und Tonaufzeichnung unterstützte Dokumentation von Amtshandlungen, bei denen Befehls- und Zwangsgewalt ausgeübt wird, zu gewinnen.