Arbeitskreis Vorratsdaten Österreich (AKVorrat.at)

ZVR: 140062668

Kirchberggasse 7/5

1070 Wien, Österreich

info@akvorrat.at

Wien, 09. März 2016

Betreff: Stellungnahme des Arbeitskreis Vorratsdaten zum am 27.01.2016 beschlossenen Polizeilichen Staatsschutzgesetz – PStSG und Änderungen im SPG und TKG 2003 (BGBl. I 5/2016 und BGBl. 6/2016)

Für den AKVorrat:

Ing. Dr.iur. Christof Tschohl, RA Mag. iur. Ewald Scheucher, Mag.iur. Alexander Czadilek, Rolf-Dieter Kargl, LL.M

I. Einleitung – Grundsatzkritik

- Der Gesetzesvorschlag zum Polizeilichen Staatsschutzgesetz wurde am 27. Jänner 2016 mit den Stimmen der Regierungsparteien (SPÖ und ÖVP) in der 111. Sitzung des Österreichischen Nationalrates in dritter Lesung angenommen. Die vorliegende Stellungnahme bezieht sich auf den beschlossenen Gesetzestext, wobei die Änderungen des letzten Abänderungsantrages sichtbar gemacht worden sind.
- Trotz bis zuletzt anhaltender und berechtigter Kritik aus der Zivilgesellschaft wurden gegenüber dem letzten Abänderungsantrag vom November 2015 nur einige, wenn auch zum Teil begrüßenswerte Nachschärfungen am Gesetzestext vorgenommen. Festzuhalten ist aber, dass sich seit dem ersten Entwurf aus dem Frühjahr 2015 substantiell nicht allzu viel verbessert hat. Das Gesetz enthält nach wie vor viele unbestimmte Gesetzesbegriffe und dynamische Verweisungen sowie einen Deliktskatalog (zur Definition des verfassungsgefährdenden Angriffs) der einerseits zu weit gefasst ist, andererseits dem Normadressaten gegenüber große Bedenken im Hinblick auf Verständlichkeit und Transparenz aufwirft. Im Zusammenspiel mit den weiten Ermittlungsbefugnissen und den damit verbundenen massiven Grundrechtseingriffen sowie dem zu schwach ausgestalteten Rechtsschutzsystem ist insgesamt sohin von einem Gesetz zu sprechen, das mit der österreichischen Verfassung nicht in Einklang zu bringen ist. Hervorzuheben sind in diesem Zusammenhang insbesondere die Bestimmungen betreffend die Vertrauenspersonen, die Ermittlung von Verkehrs,- Zugangs- und Standortdaten sowie die unklaren und unzureichenden Regelungen über Höchstspeicherfristen und fehlende Informationspflichten.
- Auch wenn jetzt zur Genehmigung von zwei Ermittlungsmaßnahmen eine Mehrheitsentscheidung eines Rechtsschutzsenates (bei der verdeckten Ermittlung und bei der Einholung von Auskünften über Verkehrs,- Zugangs- und Standortdaten) notwendig ist, ist die **Kritik am schwachen Rechtsschutzsystem weiterhin aufrecht zu halten**. Um Wiederholungen zu vermeiden, wird grundsätzlich auf die bereits ergangenen Stellungnahmen des AKVorrat zu den diversen Entwürfen verwiesen. Ausdrücklich wird festgehalten, dass diese Kritik sich gegen die Struktur des Rechtsschutzes richtet und nicht gegen die Person des derzeitigen Amtsinhabers als Rechtsschutzbeauftragter beim Bundesministerium für Inneres. An dieser Stelle sei abermals angemerkt, dass beim 2015 verabschiedeten „Bankenpaket“ im Zusammenhang mit **Eingriffen in das Bankgeheimnis neben einer begleitenden Kontrolle durch einen (beim BMF neu geschaffenen) Rechtsschutzbeauftragten eine vollwertige richterliche Kontrolle durch das Bundesfinanzgericht geschaffen wurde**. Dies gilt auch für Auskünfte über Zugangsdaten (IP-

Adresse und Teilnehmer) im Rahmen von Finanzstrafverfahren, also einer Befugnis, die auch im SPG und im PStSG – allerdings dort ohne richterliche Kontrolle – verankert ist. Die dort offenbar gewonnenen Einsichten sollte der Gesetzgeber auch auf schwerwiegende Grundrechtseingriffe durch Sicherheitsbehörden anwenden. Denkbar wäre die Einrichtung eines besonderen Senates beim Bundesverwaltungsgericht.

- Insgesamt ist zu sehen, dass mit dem nun im Plenum beschlossenen Gesetzestext auf die Kritik der Zivilgesellschaft und diversen Stakeholdern nicht oder nur marginal reagiert wurde. Es hat den Anschein, dass man durch diverse Nachschärfungen bei einzelnen Bestimmungen medial Kapital schlagen und so kritische Stimmen verstummen lassen wollte, sich aber in der Sache eines echten und wirksamen Grundrechtsschutzes nicht angenommen hat.

- Bedenklich ist, dass die traurigen und zu verurteilenden Terroranschläge von Paris im November 2015 von Vertretern der Regierungsparteien zum Anlass genommen wurden, die Notwendigkeit dieses, unseres Erachtens verfassungswidrigen, weil nicht verhältnismäßigen und überschießenden Gesetzes, zu propagieren. An dieser Stelle sei auf das Zitat des Präsidenten des österreichischen Verfassungsgerichtshofes, Dr. Gerhart Holzinger, verwiesen, der nach den erwähnten Anschlägen gesagt hat:

„So verständlich und notwendig es sein mag, dass in dieser Situation einmal mehr geprüft wird, ob die Instrumente ausreichen, die den Sicherheitsbehörden in unserer rechtsstaatlichen Demokratie zur Verfügung stehen um dieser immanenten terroristischen Bedrohung zu begegnen, so sehr braucht es gerade in Situationen wie der gegenwärtigen, einen kühlen Kopf.“

II. Zu den einzelnen Bestimmungen:

Der AKVorrat nimmt wie folgt Stellung zum:

II.A. Bundesgesetz, mit dem das Bundesgesetz über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz – PStSG) erlassen und das Sicherheitspolizeigesetz geändert werden (BGBl. I 5/2016)

Der Nationalrat hat beschlossen:

Artikel 1

Bundesgesetz über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz - PStSG)

1. Hauptstück

Allgemeines

Anwendungsbereich; Polizeilicher Staatsschutz

§ 1. (1) Dieses Bundesgesetz regelt den polizeilichen Staatsschutz. Dieser erfolgt in Ausübung der Sicherheitspolizei.

(2) Der polizeiliche Staatsschutz dient dem Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit sowie von Vertretern ausländischer Staaten, internationaler Organisationen und anderer Völkerrechtssubjekte nach Maßgabe völkerrechtlicher Verpflichtungen, kritischer Infrastruktur und der Bevölkerung vor terroristisch, ideologisch oder religiös motivierter Kriminalität, vor Gefährdungen durch Spionage, durch nachrichtendienstliche Tätigkeit und durch Proliferation sowie der Wahrnehmung zentraler Funktionen der internationalen Zusammenarbeit in diesen Bereichen.

(3) Für die Wahrnehmung der in Abs. 2 genannten Angelegenheiten bestehen als Organisationseinheit der Generaldirektion für die öffentliche Sicherheit das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (Bundesamt) und in jedem Bundesland eine für Verfassungsschutz zuständige Organisationseinheit der Landespolizeidirektion.

(4) Der Bundesminister für Inneres kann bestimmte Angelegenheiten nach Abs. 2 dem Bundesamt vorbehalten. Diesfalls kann das Bundesamt die für Verfassungsschutz zuständige Organisationseinheit der Landespolizeidirektion mit der Durchführung einzelner Maßnahmen beauftragen. Auch kann das Bundesamt anordnen, dass ihm direkt über den Fortgang einer Angelegenheit laufend oder zu bestimmten Zeitpunkten zu berichten ist.

(5) Das Bundesamt wird bei Vollziehung dieses Bundesgesetzes für den Bundesminister für Inneres, die für Verfassungsschutz zuständige Organisationseinheit für die jeweilige Landespolizeidirektion tätig.

Kommentar:

keine Änderungen

Organisation

§ 2. (1) Dem Bundesamt steht ein Direktor vor. Der Direktor nimmt die Funktion als Informationssicherheitsbeauftragter für den Wirkungsbereich des Bundesministeriums für Inneres nach § 7 des Informationssicherheitsgesetzes - InfoSiG, BGBl. I Nr. 23/2002, wahr.

(2) Zum Direktor kann nur ernannt werden, wer ein abgeschlossenes Studium der Rechtswissenschaften und besondere Kenntnisse auf dem Gebiet des polizeilichen Staatsschutzes aufweist.

(3) Sonstige Bedienstete der Organisationseinheiten gemäß § 1 Abs. 3 haben innerhalb von zwei Jahren nach Dienstbeginn eine spezielle Ausbildung für Verfassungsschutz und Terrorismusbekämpfung zu absolvieren, deren näherer Inhalt durch Verordnung des Bundesministers für Inneres festzusetzen ist.

(4) Sofern es sich bei Bediensteten in Leitungsfunktionen nicht bereits um Organe des öffentlichen Sicherheitsdienstes handelt, können sie nach erfolgreicher Absolvierung der Ausbildung (Abs. 3) zur Ausübung unmittelbarer Befehls- und Zwangsgewalt ermächtigt werden. Diesfalls gelten sie als Organe des öffentlichen Sicherheitsdienstes nach § 5 Abs. 2 Sicherheitspolizeigesetz - SPG, BGBl. Nr. 566/1991.

(5) Vor Beginn der Tätigkeit muss sich jeder Bedienstete einer Sicherheitsüberprüfung (§ 55 SPG) für den Zugang zu geheimer Information unterziehen. Strebt der Bedienstete eine Leitungsfunktion an, muss er sich einer Sicherheitsüberprüfung für den Zugang zu streng geheimer Information unterziehen. Die Sicherheitsüberprüfungen sind nach drei Jahren zu wiederholen. Bei Vorliegen von Anhaltspunkten, wonach ein Bediensteter nicht mehr vertrauenswürdig sein könnte, ist die Sicherheitsüberprüfung vor Ablauf dieser Frist zu wiederholen.

Kommentar:

keine Änderungen

Geschäftsordnung des Bundesamtes

§ 3. Der Direktor des Bundesamtes hat festzulegen, wem die Genehmigung von Entscheidungen für den Bundesminister für Inneres im Rahmen der Geschäftseinteilung zukommt, in welchen Fällen ihm die Genehmigung vorbehalten ist und wem diese im Fall der Verhinderung obliegt (Geschäftsordnung). Vor Erlassung und vor jeder Änderung der Geschäftsordnung ist der Generaldirektor für die öffentliche Sicherheit zu befassen.

Kommentar:

keine Änderungen

Bundesamt als Zentralstelle

§ 4. Das Bundesamt erfüllt für den Bundesminister für Inneres folgende zentrale Funktionen:

1. Operative Koordinierungsstelle für Meldungen über jede Form von Angriffen auf Computersysteme (§ 74 Abs. 1 Z 8 Strafgesetzbuch - StGB, BGBl. Nr. 60/1974) von verfassungsmäßigen Einrichtungen (§ 22 Abs. 1 Z 2 SPG) sowie kritischen Infrastrukturen (§ 22 Abs. 1 Z 6 SPG) nach den §§ 118a, 119, 119a, 126a, 126b und 126c StGB;
2. Meldestelle für jede Form der Betätigung im nationalsozialistischen Sinn nach dem Verbotsgesetz – VerbotsG, StGBl. Nr. 13/1945 (Meldestelle NS-Wiederbetätigung);
3. die Durchführung von Sicherheitsüberprüfungen (§ 55 SPG);
4. die Organisation der Gebäudesicherheit der vom Bundesministerium für Inneres genutzten Gebäude;
5. die internationale Zusammenarbeit auf dem Gebiet des Staatsschutzes; davon unberührt bleibt die Zusammenarbeit der für Verfassungsschutz zuständigen Organisationseinheiten der Landespolizeidirektionen mit benachbarten regionalen Sicherheitsdienststellen.

Kommentar:

keine Änderungen

Anwendbarkeit des Sicherheitspolizeigesetzes

§ 5. Soweit in diesem Bundesgesetz nicht Besonderes bestimmt ist, gilt das Sicherheitspolizeigesetz.

Kommentar:

keine Änderungen

2. Hauptstück
Aufgaben auf dem Gebiet des polizeilichen Staatsschutzes
Erweiterte Gefahrenerforschung und Schutz vor verfassungsgefährdenden Angriffen

§ 6. (1) Den Organisationseinheiten gemäß § 1 Abs. 3 obliegen

1. die erweiterte Gefahrenerforschung; das ist die Beobachtung einer Gruppierung, wenn im Hinblick auf deren bestehende Strukturen und auf zu gewärtigende Entwicklungen in deren Umfeld damit zu rechnen ist, dass es zu mit schwerer Gefahr für die öffentliche Sicherheit verbundener Kriminalität, insbesondere zu ideologisch oder religiös motivierter Gewalt kommt;

2. der vorbeugende Schutz vor verfassungsgefährdenden Angriffen durch eine Person, sofern ein begründeter Gefahrenverdacht für einen solchen Angriff besteht (§ 22 Abs. 2 SPG);
3. der Schutz vor verfassungsgefährdenden Angriffen aufgrund von Informationen von Dienststellen inländischer Behörden, ausländischen Sicherheitsbehörden oder Sicherheitsorganisationen (§ 2 Abs. 2 und 3 Polizeikooperationsgesetz – PolKG, BGBl. I Nr. 104/1997) sowie von Organen der Europäischen Union oder Vereinten Nationen zu Personen, die im Verdacht stehen, im Ausland einen Sachverhalt verwirklicht zu haben, der einem verfassungsgefährdenden Angriff entspricht.

(2) Ein verfassungsgefährdender Angriff ist die Bedrohung von Rechtsgütern

1. durch die rechtswidrige Verwirklichung des Tatbestandes einer nach §§ 278b bis 278f oder, soweit es der Verfügungsmacht einer terroristischen Vereinigung unterliegende Vermögensbestandteile betrifft, nach § 165 Abs. 3 StGB strafbaren Handlung;
2. durch die rechtswidrige Verwirklichung des Tatbestandes einer nach §§ 274 Abs. 2 erster Fall, 279, 280, 283 Abs. 3 oder in § 278c StGB genannten strafbaren Handlung, sofern diese ideologisch oder religiös motiviert ist;
3. durch die rechtswidrige Verwirklichung des Tatbestandes einer nach §§ 242 und 246 StGB, dem fünfzehnten Abschnitt des StGB oder nach dem VerbotsG strafbaren Handlung;
4. durch die rechtswidrige und vorsätzliche Verwirklichung des Tatbestandes einer nach §§ 175, 177a, 177b StGB, §§ 79 bis 82 Außenwirtschaftsgesetz 2011 - AußWG 2011, BGBl. I Nr. 26/2011, § 7 Kriegsmaterialgesetz - KMG, BGBl. Nr. 540/1977, § 11 Sanktionengesetz 2010 - SanktG, BGBl. I Nr. 36/2010, nach §§ 124, 316, 319 oder 320 StGB sowie nach dem sechzehnten Abschnitt des StGB strafbaren Handlung;
5. durch die rechtswidrige Verwirklichung des Tatbestandes einer nach §§ 118a, 119, 119a, 126a, 126b oder 126c StGB strafbaren Handlung gegen verfassungsmäßige Einrichtungen und ihre Handlungsfähigkeit (§ 22 Abs. 1 Z 2 SPG) sowie kritische Infrastrukturen (§ 22 Abs. 1 Z 6 SPG).

Deleted: 282,

Deleted: dem vierzehnten oder

Kommentar:

Grundsatzkritik zum Begriff "Vorbeugender Schutz vor verfassungsgefährdenden Angriffen" gemäß § 6 Abs 1 Z 2:

Eine Definition des Begriffs "vorbeugender Schutz" findet sich im Gesetzestext nicht. Der Wortlaut lässt auf Prävention schließen, also auf Vermeidung einer in der Zukunft liegenden Gefährdung. Die Norm verweist auch auf § 22 SPG, dessen Überschrift "Vorbeugender Schutz von Rechtsgütern" lautet und der auf § 21 SPG folgt, in dem die Abwehr allgemeiner Gefahren und die Beendigung gefährlicher Angriffe normiert ist. Bei dieser Gefahrenabwehr ist die Bedrohung eines Rechtsgutes

von entscheidender Bedeutung. Im Umkehrschluss darf es beim vorbeugenden Schutz somit noch nicht zu einer Bedrohung gekommen sein, denn diese würde ja unter die Gefahrenabwehr fallen. Der Einsatzbereich des vorbeugenden Schutzes endet demnach mit dem Eintritt einer konkret strafbaren Vorbereitungshandlung. Nach dem Gesetzeswortlaut beginnt der Einsatzbereich, wenn ein begründeter Gefahrenverdacht für einen verfassungsgefährdenden Angriff vorliegt, wohingegen im Begutachtungsentwurf noch auf "wahrscheinliche Angriffe" abgestellt wurde. Zwar findet sich dieser Bezug nicht mehr im PStSG, jedoch verweist die Klammer am Ende der Ziffer 2 auf § 22 Abs 2 SPG, wo sich wiederum ein Bezug zur Wahrscheinlichkeit von Angriffen findet. Nach den Materialien[1] ist unter "begründetem Gefahrenverdacht" mehr als die bloße Möglichkeit oder Nichtausschließbarkeit (eines Angriffs), aber weniger als "mit Gewissheit zu erwarten" zu verstehen. Dieser Verdacht muss darauf gerichtet sein, dass der Betroffene einen verfassungsgefährdenden Angriff in absehbarer Zeit begehen werde. Somit beginnt der Anwendungsbereich des vorbeugenden Schutzes mit der Wahrscheinlichkeit der Begehung eines konkreten Angriffs in absehbarer Zeit. Bei genauerer Betrachtung hat sich zwischen dem Ministerialentwurf und dem beschlossenen Gesetzestext also nicht allzu viel verändert. Um die Begründungspflicht prozessual abzusichern, wären klare Regelungen wünschenswert, wo und wie die Begründungen für das Vorliegen eines konkreten Gefahrenverdachts schriftlich zu dokumentieren und vorzulegen sind. Problematisch ist jedenfalls, dass die Befugnisse nach diesem Bundesgesetz bereits weit im Vorfeld einer strafbaren Handlung ausgelöst werden, wobei einige Delikte im Deliktskatalog selbst schon die Strafbarkeit weit in den Vorbereitungsbereich verlagern (zB § 278b Abs 2 StGB). Ein überbordendes Sicherheitsdenken ist ein weiterer Schritt hin zum Überwachungsstaat, in dem sich die rechtsstaatliche Demokratie selbst preisgeben würde.

Zu den Änderungen:

Der Deliktskatalog, der der Definition des "verfassungsgefährdenden Angriffs" zugrunde liegt, wurde im nun beschlossenen Gesetzestext etwas eingeschränkt. Begrüßenswert ist, dass in § 6 Abs 2 Z 2 PStSG einige Meinungsdelikte aus dem Katalog genommen (§ 282 StGB - Aufforderung zu oder Gutheißung einer mit Strafe bedrohten Handlung) bzw Tatbestände eingeschränkt wurden (§ 283 Abs 3 StGB - die Verhetzung stellt nunmehr nur dann einen verfassungsgefährdenden Angriff dar, wenn die Tat qualifiziert gem Abs 3 leg cit bewirkt wird). Weiterhin scharf zu kritisieren ist jedoch, dass es nach wie vor einen Verweis auf die in § 278c StGB ("Terroristische Straftaten") genannten Delikte gibt. Nach dem Gesetzeswortlaut stellen diese Delikte nämlich einen verfassungsgefährdenden Angriff und somit die Grundlage für Ermittlungsbefugnisse dar, wenn sie rechtswidrig verwirklicht wurden und ideologisch oder religiös motiviert sind. Eine ideologische oder

[1] AB 988 BlgNR XXV. GP, 5.

religiöse Motivation einer strafbaren Handlung muss aber nicht zwangsläufig einen terroristischen oder schwer kriminellen Hintergrund haben, die die Verfassungsschützer auf den Plan rufen müssen. An dieser Stelle sei auf die Stellungnahme des AK Vorrat von Mitte Jänner 2016 verwiesen, in der die Empfehlung ausgesprochen wurde, die Definition des verfassungsgefährdenden Angriffs nur auf wirklich demokratie- bzw staatsfeindliche Handlungen zu beschränken, um zu verhindern, dass personenbezogene Daten von Tätern, bei denen solche Zusammenhänge nicht gegeben sind (für deren strafrechtliche Verfolgung das Regime der Strafprozessordnung also völlig ausreichend ist) in der Analysedatenbank des BVT landen.

Aus dem 14. Abschnitt des StGB verbleiben jetzt nur noch der Hochverrat und staatsfeindliche Verbindungen als verfassungsgefährdende Angriffe im Deliktskatalog. Eine substantielle Verbesserung der Regierungsvorlage ist hier die Herausnahme des Tatbestandes der Herabwürdigung des Staates oder seiner Symbole, da selbst die Verwirklichung dieses Delikts nicht die demokratische Grundordnung des Staates gefährdet und eine Verfolgung nach der Strafprozessordnung genügt.

Gemäß § 6 Abs 2 Z 4 PStSG liegt ein verfassungsgefährdender Angriff nun nur mehr dann vor, wenn die genannten Delikte rechtswidrig und vorsätzlich begangen werden. Die Einschränkung auf Delikte, die Vorsatz verlangen, ist nur bezüglich des Außenwirtschaftsgesetzes sowie des Kriegsmaterialiengesetzes relevant, da die anderen aufgezählten Tatbestände ohnehin nur vorsätzlich begangen werden können. Diese Einschränkung ist jedenfalls begrüßenswert, da bei der Begehung von Fahrlässigkeitsdelikten sicher nicht die geforderte demokratiefeindliche kriminelle Energie verwirklicht wird, die die Ermittlungsbefugnisse des BVT und der Organisationseinheiten rechtfertigen würde.

Polizeilich staatsschutzrelevante Beratung

§ 7. Den Organisationseinheiten gemäß § 1 Abs. 3 obliegen zur Vorbeugung verfassungsgefährdender Angriffe, insbesondere auf dem Gebiet der Cybersicherheit, die Förderung der Bereitschaft und Fähigkeit des Einzelnen, sich über eine Bedrohung seiner Rechtsgüter Kenntnis zu verschaffen und Angriffen entsprechend vorzubeugen.

Kommentar:

keine Änderungen

Information verfassungsmäßiger Einrichtungen

§ 8. (1) Die Wahrnehmung der Aufgabenerfüllung nach diesem Bundesgesetz umfasst ferner die Analyse und Beurteilung von staatsschutzrelevanten Bedrohungslagen, die sich auch aus verfassungsgefährdenden Entwicklungen im Ausland ergeben können, zur Information verfassungsmäßiger Einrichtungen, sofern nicht der Vollziehungsbereich des Bundesministers für Landesverteidigung und Sport betroffen ist.

(2) Über staatsschutzrelevante Bedrohungen sind die obersten Organe der Vollziehung (Art. 19 B-VG) sowie die mit der Leitung der gesetzgebenden Körperschaften des Bundes und der Länder betrauten Organe zu unterrichten, soweit diese Information für die Wahrnehmung der gesetzlichen Aufgaben in deren Zuständigkeitsbereich von Bedeutung ist. Ebenso sind die Genannten über Umstände zu unterrichten, die für die Ausübung ihres Amtes von wesentlicher Bedeutung sind.

Kommentar:

keine Änderungen

3. Hauptstück
Verwenden personenbezogener Daten auf dem Gebiet des polizeilichen Staatsschutzes
Allgemeines

§ 9. (1) Die Organisationseinheiten gemäß § 1 Abs. 3 haben beim Verwenden (Verarbeiten und Übermitteln) personenbezogener Daten die Verhältnismäßigkeit (§ 29 SPG) zu beachten. Beim Verwenden sensibler und strafrechtlich relevanter Daten haben sie angemessene Vorkehrungen zur Wahrung der Geheimhaltungsinteressen der Betroffenen zu treffen. Bei Ermittlungen von personenbezogenen Daten nach diesem Bundesgesetz ist ein Eingriff in das von § 157 Abs. 1 Z 2 bis 4 Strafprozessordnung - StPO, BGBl. Nr. 631/1975, geschützte Recht nicht zulässig. § 157 Abs. 2 StPO gilt sinngemäß.

(2) Personenbezogene Daten dürfen von den Organisationseinheiten gemäß § 1 Abs. 3 gemäß diesem Hauptstück nur verwendet werden, soweit dies zur Erfüllung der ihnen übertragenen Aufgaben erforderlich ist. Ermächtigungen nach anderen Bundesgesetzen bleiben unberührt.

Kommentar:

Bei der Ermittlung von personenbezogenen Daten ist ein Eingriff in das von § 157 Abs 1 Z 2 bis 4 StPO geschützte Recht nun nicht mehr zulässig. Diese Änderung ist grundsätzlich begrüßenswert, da das Berufsgeheimnis unter anderem von Fachärzten, Rechtsanwälten und Medienvertretern aufrechterhalten wird. Problematisch erscheint, dass weder genau bestimmt ist, wie die Behörde die Zugehörigkeit von Personen zu den geschützten Berufsgruppen überprüft (zB durch vom BVT geführte Listen, wobei solche wiederum massive datenschutzrechtliche Problem- und

Fragestellungen aufwerfen), noch was passiert, wenn die persönlichen Daten von Angehörigen dieser Berufsgruppen, wenn sie als Kontakt- oder Begleitpersonen in Erscheinung treten, verarbeitet werden. In letzterem Fall wäre jedenfalls das Grundrecht auf Privatleben gemäß Art 8 EMRK und das Grundrecht auf Datenschutz gemäß Art 1 DSG 2000 bzw Art 8 EU-GRC verletzt, da für eine Datenverwendung dann keine gesetzliche Grundlage besteht. An dieser Stelle sei angemerkt, dass alle Änderungen, auf die sich diese Stellungnahme bezieht, den Abgeordneten erst einen Tag vor Beschlussfassung im Plenum vorgelegt wurden und in der Debatte die eben genannten Ungereimtheiten nicht diskutiert wurden. Diese Vorgehensweise erweckt den Anschein, auf die diesbezügliche berechtigte und substantiierte Kritik aus der Zivilgesellschaft (insbesondere des AK Vorrat, des Österreichischen Rechtsanwaltskammertags und des Österreichischen Journalistenverbandes) im Schnellverfahren reagieren zu wollen um die kritischen Stimmen verstummen zu lassen. Dies ist den Regierungsparteien nicht gelungen. Der Gesetzgeber wäre gerade bei Eingriffen in die Grundrechte in sensiblen Bereichen gut beraten, keine undurchdachten Schnellschüsse vorzunehmen, sondern auf Kritik einzugehen und Problembereiche ausführlich in den Ausschüssen und im Plenum ebenso wie mit Vertretern der Zivilgesellschaft zu diskutieren.

Ermittlungsdienst für Zwecke des polizeilichen Staatsschutzes

§ 10. (1) Die Organisationseinheiten gemäß § 1 Abs. 3 dürfen personenbezogene Daten ermitteln und weiterverarbeiten für

1. die erweiterte Gefahrenerforschung (§ 6 Abs. 1 Z 1),
2. den vorbeugenden Schutz vor verfassungsgefährdenden Angriffen (§ 6 Abs. 1 Z 2),
3. den Schutz vor verfassungsgefährdenden Angriffen aufgrund von Informationen von Dienststellen inländischer Behörden, ausländischen Sicherheitsbehörden oder Sicherheitsorganisationen sowie von Organen der Europäischen Union oder Vereinten Nationen (§ 6 Abs. 1 Z 3) und
4. die Information verfassungsmäßiger Einrichtungen (§ 8),

wobei sensible Daten gemäß § 4 Z 2 Datenschutzgesetz 2000 - DSG 2000, BGBl. I Nr. 165/1999, nur insoweit ermittelt und weiterverarbeitet werden dürfen, als diese für die Erfüllung der Aufgabe unbedingt erforderlich sind.

(2) Die Organisationseinheiten gemäß § 1 Abs. 3 dürfen Daten, die sie in Vollziehung von Bundes- oder Landesgesetzen rechtmäßig verarbeitet haben, für die Zwecke des Abs. 1 ermitteln und weiterverarbeiten. Ein automationsunterstützter Datenabgleich im Sinne des § 141 StPO ist davon nicht umfasst. Bestehende Übermittlungsverbote bleiben unberührt.

Deleted: Strafprozessordnung -

Deleted: , BGBl. Nr. 631/1975,

(3) Die Organisationseinheiten gemäß § 1 Abs. 3 sind berechtigt, von den Dienststellen der Gebietskörperschaften, den anderen Körperschaften des öffentlichen Rechtes und den von diesen betriebenen Anstalten Auskünfte zu verlangen, die sie zur Erfüllung ihrer Aufgaben nach Abs. 1 Z 1 und 2 benötigen. Eine Verweigerung der Auskunft ist nur zulässig, soweit

andere öffentliche Interessen überwiegen oder eine über die Amtsverschwiegenheit (Art. 20 Abs. 3 B-VG) hinausgehende sonstige gesetzliche Verpflichtung zur Verschwiegenheit besteht.

(4) Die Organisationseinheiten gemäß § 1 Abs. 3 sind im Einzelfall ermächtigt, für die Erfüllung ihrer Aufgaben nach Abs. 1 Z 1 und 2 personenbezogene Bilddaten zu verwenden, die Rechtsträger des öffentlichen oder privaten Bereichs mittels Einsatz von Bild- und Tonaufzeichnungsgeräten rechtmäßig ermittelt und den Sicherheitsbehörden übermittelt haben, wenn ansonsten die Aufgabenerfüllung gefährdet oder erheblich erschwert wäre. Dabei ist besonders darauf zu achten, dass Eingriffe in die Privatsphäre der Betroffenen die Verhältnismäßigkeit (§ 29 SPG) zum Anlass wahren. Nicht zulässig ist die Verwendung von Daten über nichtöffentliches Verhalten.

(5) Abgesehen von den Fällen der Abs. 2 bis 4 sowie den Ermittlungen nach § 11 sind die Organisationseinheiten gemäß § 1 Abs. 3 für Zwecke des Abs. 1 berechtigt, personenbezogene Daten aus allen anderen verfügbaren Quellen durch Einsatz geeigneter Mittel, insbesondere durch Zugriff etwa auf im Internet öffentlich zugängliche Daten, zu ermitteln und weiterzuverarbeiten. Abs. 2 zweiter Satz gilt.

Kommentar:

keine Änderungen

Besondere Bestimmungen für die Ermittlungen

§ 11. (1) Zur erweiterten Gefahrenerforschung (§ 6 Abs. 1 Z 1) und zum vorbeugenden Schutz vor verfassungsgefährdenden Angriffen (§ 6 Abs. 1 Z 2) ist die Ermittlung personenbezogener Daten nach Maßgabe des § 9 und unter den Voraussetzungen des § 14 zulässig durch

1. Observation (§ 54 Abs. 2 SPG), sofern die Observation ansonsten aussichtslos oder wesentlich erschwert wäre unter Einsatz technischer Mittel (§ 54 Abs. 2a SPG);
2. verdeckte Ermittlung (§ 54 Abs. 3 und 3a SPG), wenn die Erfüllung der Aufgabe durch Einsatz anderer Ermittlungsmaßnahmen aussichtslos wäre;
3. Einsatz von Bild- und Tonaufzeichnungsgeräten (§ 54 Abs. 4 SPG); dieser darf verdeckt erfolgen, wenn die Erfüllung der Aufgabe ansonsten aussichtslos wäre;
4. Einsatz von Kennzeichenerkennungsgeräten (§ 54 Abs. 4b SPG) zum automatisierten Abgleich mit KFZ-Kennzeichen, die nach § 12 Abs. 1 verarbeitet werden;
5. Einholen von Auskünften nach §§ 53 Abs. 3a Z 1 bis 3 und 53 Abs. 3b SPG zu einer Gruppierung nach § 6 Abs. 1 Z 1 oder einem Betroffenen nach § 6 Abs. 1 Z 2 sowie zu deren jeweiligen Kontakt- oder Begleitpersonen (§ 12 Abs. 1 Z 4) von Betreibern öffentlicher Telekommunikationsdienste (§ 92 Abs. 3 Z 1 Telekommunikationsgesetz 2003 - TKG 2003, BGBl. I Nr. 70/2003) und sonstigen Diensteanbietern (§ 3 Z 2 E-Commerce-Gesetz - ECG, BGBl. I Nr. 152/2001), wenn die Erfüllung der Aufgabe durch Einsatz anderer Ermittlungsmaßnahmen aussichtslos wäre;

6. Einholen von Auskünften zu Kontaktdaten, Nummer und Art des Reisedokuments sowie Zahlungsinformationen eines Betroffenen nach § 6 Abs. 1 Z 2, Datum der Buchung, Reiseverlauf, Reisestatus, Flugscheindaten, Zahl und Namen von Mitreisenden im Rahmen einer Buchung von Personenbeförderungsunternehmen zu einer von ihnen erbrachten Leistung;
7. Einholen von Auskünften über Verkehrsdaten (§ 92 Abs. 3 Z 4 TKG 2003), Zugangsdaten (§ 92 Abs. 3 Z 4a TKG 2003) und Standortdaten (§ 92 Abs. 3 Z 6 TKG 2003), die nicht einer Auskunft nach Abs. 1 Z 5 unterliegen, zu einer Gruppierung nach § 6 Abs. 1 Z 1 oder einem Betroffenen nach § 6 Abs. 1 Z 2 von Betreibern öffentlicher Telekommunikationsdienste (§ 92 Abs. 3 Z 1 TKG 2003) und sonstigen Diensteanbietern (§ 3 Z 2 ECG), wenn dies zur Vorbeugung eines verfassungsgefährdenden Angriffs, dessen Verwirklichung mit beträchtlicher Strafe (§ 17 SPG) bedroht ist, erforderlich erscheint und die Erfüllung der Aufgabe durch Einsatz anderer Ermittlungsmaßnahmen aussichtslos wäre. Eine Ermächtigung darf nur für jenen künftigen oder auch vergangenen Zeitraum erteilt werden, der zur Erreichung des Zwecks voraussichtlich erforderlich ist.

Die Ermittlung ist zu beenden, sobald ihre Voraussetzungen wegfallen.

(2) In den Fällen des Abs. 1 Z 5 bis 7 ist die ersuchte Stelle verpflichtet, die Auskünfte zu erteilen. Der Ersatz von Kosten in den Fällen des Abs. 1 Z 5 hinsichtlich § 53 Abs. 3b SPG und des Abs. 1 Z 7 richtet sich nach der Überwachungskostenverordnung - ÜKVO, BGBl. II Nr. 322/2004.

(3) Beim Einholen von Auskünften nach Abs. 1 Z 7 hat das Bundesamt der um Auskunft ersuchten Stelle die Verpflichtung nach Abs. 2 und ihren Umfang sowie die Verpflichtung, mit der Ermächtigung verbundene Tatsachen und Vorgänge gegenüber Dritten geheim zu halten, aufzutragen und die entsprechende Ermächtigung des Rechtsschutzsenats anzuführen.

Deleted: Rechtsschutzbeauftragten

Kommentar:

Gemäß § 11 Abs 1 Z 5 dürfen nun personenbezogene Daten durch Einholen von Auskünften gemäß § 53 Abs 3a und Abs 3b SPG von den "jeweiligen" Kontakt- oder Begleitpersonen von Gruppierungen oder Gefährdern (§ 6 Abs 1 Z 1 und Z 2) ermittelt werden. Durch das Hinzufügen des Wortes "jeweiligen" ändert sich jedoch nicht viel. Es hat den Anschein, dass man wohl gewisse Kontakt- oder Begleitpersonen aus dem Anwendungsbereich ausschließen wollte, jedoch ist festzuhalten, dass diese Einschränkung in der Praxis keinen Unterschied machen wird, denn entweder jemand ist Kontakt- oder Begleitperson einer Gruppierung oder eines Gefährders oder eben nicht, wobei in ersterem Fall die Ermittlungsbefugnisse bestehen (zur Speicherung von personenbezogenen Daten dieser Kontakt- oder Begleitpersonen; siehe Kommentar zu § 12).

Wer als "Personenbeförderungsunternehmen" iSd § 11 Abs 1 Z 6 anzusehen und damit zur Auskunftserteilung verpflichtet ist, ist unklar. Laut den Materialien[2] sind dies natürliche oder juristische Personen, die gewerbsmäßig Personentransporte durchführen oder Transportmittel zur Verfügung stellen oder vermitteln. Als Beispiele werden Fluggesellschaften, Reisebüros oder Mietwagenfirmen genannt. Der Wortlaut des Begriffs "Personenbeförderungsunternehmen" deutet auf den Transport von Menschen durch Dritte hin. Das Zur-Verfügung-Stellen oder Vermitteln von Transportmitteln stellt aber keine Beförderung dar, was auch aus dem klaren Wortlaut des § 111 FPG[3] hervorgeht. Eine Diskrepanz zwischen dem Gesetzeswortlaut und den Materialien ist im Hinblick auf die Normenklarheit und Transparenz wenig hilfreich. Überdies wäre nach einer strengen Wortinterpretation beispielsweise die Auskunftseinholung bei einem Reisebüro über Reisedaten eines Betroffenen nach § 6 Abs 1 Z 2 rechtswidrig, da es dafür keine gesetzliche Grundlage gibt, was sicher nicht im Sinne des Gesetzgebers liegt.

Gemäß § 11 Abs 3 muss bei Einholung von Auskünften von Verkehrs,- Zugangs- und Standortdaten gemäß § 11 Abs 1 Z 7 der um Auskunft ersuchten Stelle nun die Ermächtigung des Rechtsschutzsenates (statt der Ermächtigung des Rechtsschutzbeauftragten) vorgelegt werden. Die Ziffer 7 umfasst die Einholung von Auskünften über alle Verkehrs-, Zugangs- und Standortdaten, die nicht unter Ziffer 5 leg cit fallen. Wegen des sehr weiten Anwendungsbereiches dieser Ermächtigung sind besondere Voraussetzungen vorgesehen. Einerseits ist als Aufgabe die Beobachtung einer Gruppierung oder der vorbeugende Schutz vor einem verfassungsgefährdenden Angriff vorgesehen (wobei diesbezüglich wie oben schon ausgeführt ein konkreter Verdacht einer Straftat *nicht* vorliegen muss), andererseits ist eine Strafdrohung von mehr als einem Jahr erforderlich, was sich durch den Verweis auf § 17 SPG in der Klammer ergibt (wobei anzumerken ist, dass fast alle als verfassungsgefährdende Angriffe in Betracht kommende Delikte darunter fallen). Eine Einschränkung auf besonders schwere Straftaten erfolgt hier nicht. Weiters müssen die Auskunftseinholung erforderlich und andere Ermittlungsmaßnahmen aussichtslos sein (eine Annahme der Aussichtslosigkeit ist ausreichend, andere Ermittlungsmaßnahmen müssen nicht vorher erst versucht werden). Gemäß § 14 Abs 2 darf eine Ermächtigung des Rechtsschutzsenates nur für höchstens sechs Monate erteilt werden, wobei jedoch Verlängerungen zulässig sind. Die Eingriffsintensität bei der Erhebung von Verkehrs-, Zugangs- und Standortdaten ist sehr hoch, da sie ein sehr genaues Persönlichkeitsbild bzw Bewegungsprofil eines Menschen zeichnen können. Insbesondere wenn die Daten über einen längeren Zeitraum (mehrere Monate) erhoben werden, kommt es zu einer

[2] AB 988 BlgNR XXV. GP, 8.
[3] § 111 Abs 1 FPG: "Beförderungsunternehmer, die Personen mit einem Luft- oder Wasserfahrzeug oder im Rahmen des internationalen Linienverkehrs mit einem Autobus über die Außengrenze nach Österreich bringen, sind verpflichtet [...]".

umfassenden Durchleuchtung der Person. Die hohe Eingriffsintensität und der breite Anwendungsbereich stehen schwachen Rechtsschutzmechanismen gegenüber. Eine richterliche Genehmigung ist nicht erforderlich und für Betroffene ist es nicht einfach, rechtliche Schritte einzuleiten. Auch wenn das PStSG ihre Verständigung zwar grundsätzlich vorsieht, normiert § 16 eine Reihe von Ausnahmen von der Informationspflicht. Die Einführung eines Rechtsschutzsenates vermag dieses Rechtsschutzdefizit nicht zu kompensieren. Aus den genannten Gründen ist § 11 Abs 1 Z 7 mit den verfassungsgesetzlich gewährleisteten Rechten[4] des Art 8 EMRK und Art 1 DSG 2000 nicht vereinbar.

Datenanwendungen

§ 12. (1) Der Bundesminister für Inneres und die Landespolizeidirektionen dürfen als datenschutzrechtliche Auftraggeber in einem vom Bundesamt betriebenen Informationsverbundsystem zum Zweck der Bewertung von wahrscheinlichen Gefährdungen sowie zum Erkennen von Zusammenhängen und Strukturen mittels operativer oder strategischer Analyse

1. zu einer Gruppierung nach § 6 Abs. 1 Z 1
   a) Namen,
   b) frühere Namen,
   c) Aliasdaten,
   d) Anschrift/Aufenthalt,
   e) Rechtsform/-status,
   f) sachbezogene Daten zu Kommunikations- und Verkehrsmittel einschließlich Registrierungsnummer/Kennzeichen und
   g) Informationen über wirtschaftliche und finanzielle Verhältnisse einschließlich damit im Zusammenhang stehender Daten juristischer Personen,
2. zu Betroffenen nach § 6 Abs. 1 Z 2
   a) Namen,
   b) frühere Namen,
   c) Aliasdaten,
   d) Namen der Eltern,
   e) Geschlecht,
   f) Geburtsdatum und Ort,
   g) Staatsangehörigkeit,
   h) Wohnanschrift/Aufenthalt,

[4] Seit dem Charta-Erkenntnis des VfGH (VerfSlg. 19632) ist darunter auch ua Art 8 EU-GRC zu verstehen.

i) Dokumentendaten,

j) Beruf, Qualifikation und Funktion/Beschäftigung/Lebensverhältnisse,

k) Daten, die für die Einreise- und Aufenthaltsberechtigung maßgeblich sind,

l) sachbezogene Daten zu Kommunikations- und Verkehrsmittel sowie Waffen einschließlich Registrierungsnummer/Kennzeichen,

m) Lichtbild und sonstige zur Personenbeschreibung erforderliche Daten,

n) erkennungsdienstliche Daten und

o) Informationen über wirtschaftliche und finanzielle Verhältnisse einschließlich damit im Zusammenhang stehender Daten juristischer Personen,

3. zu Verdächtigen eines verfassungsgefährdenden Angriffs die Datenarten nach Z 2 a) bis o),

4. zu Kontakt- oder Begleitpersonen, die unmittelbar und nicht nur zufällig mit einer Gruppierung nach Z 1, Betroffenen nach Z 2 oder Verdächtigen nach Z 3 in Verbindung stehen und bei denen ausreichende Gründe für die Annahme bestehen, dass über sie für die Erfüllung der Aufgabe relevante Informationen beschafft werden können, die Datenarten nach Z 2 a) bis m) bis zur möglichst rasch vorzunehmenden Klärung der Beziehung zu diesen Personen,

5. zu Informanten und sonstigen Auskunftspersonen die Datenarten nach Z 2 a) bis j)

sowie tat- und fallbezogene Informationen und Verwaltungsdaten verarbeiten, die gemäß §§ 10 oder 11 oder auf Grundlage des SPG oder der StPO ermittelt wurden. Soweit dies zur Erfüllung des Zwecks (Abs. 1) unbedingt erforderlich ist, dürfen auch sensible Daten im Sinne des § 4 Z 2 DSG 2000 verarbeitet werden.

(2) Die Daten sind vor der Verarbeitung in der Datenanwendung auf ihre Erheblichkeit und Richtigkeit zu prüfen sowie während der Verwendung zu aktualisieren. Erweisen sich Daten als unrichtig, dann sind diese richtigzustellen oder zu löschen, es sei denn, die Weiterverarbeitung von Falschinformationen mit der Kennzeichnung „unrichtig“ ist zur Erfüllung des Zwecks (Abs. 1) erforderlich. Bei Einstellung von Ermittlungen oder Beendigung eines Verfahrens einer Staatsanwaltschaft oder eines Strafgerichtes sind die Daten durch Anmerkung der Einstellung oder Verfahrensbeendigung und des bekannt gewordenen Grundes zu aktualisieren. Eine Aktualisierung oder Richtigstellung von Daten nach Abs. 1 Z 1 lit. a bis d und Z 2 lit. a bis i darf jeder Auftraggeber vornehmen. Hievon ist jener Auftraggeber, der die Daten verarbeitet hat, zu informieren.

(3) Daten sind nach Maßgabe des § 13 zu löschen. Daten zu Verdächtigen gemäß Abs. 1 Z 3 und damit in Zusammenhang stehenden Personen gemäß Abs. 1 Z 5 sind längstens nach fünf Jahren. Personen gemäß Abs. 1 Z 4 längstens nach drei Jahren zu löschen. Daten zu Kontakt- und Begleitpersonen gemäß Abs. 1 Z 4 sind jedenfalls zu löschen, wenn keine Gründe für die Annahme mehr vorliegen, dass über sie für die Erfüllung der Aufgabe relevante Informationen beschafft werden können.

(4) Übermittlungen sind an Sicherheitsbehörden für Zwecke der Sicherheitspolizei und Strafrechtspflege, an Staatsanwaltschaften und ordentliche Gerichte für Zwecke der Strafrechtspflege, an verfassungsmäßige Einrichtungen nach Maßgabe des § 8 und darüber hinaus an Dienststellen inländischer Behörden, soweit dies eine wesentliche Voraussetzung zur Wahrnehmung einer ihr gesetzlich übertragenen Aufgabe ist, an ausländische

Deleted: die
Deleted:
Deleted: und
Deleted: soweit es sich um
Deleted: sowie
Deleted: damit in Zusammenhang stehende
Deleted: und 5 handelt
Deleted: fünf

Sicherheitsbehörden und Sicherheitsorganisationen (§ 2 Abs. 2 und 3 PolKG) sowie Organe der Europäischen Union oder Vereinten Nationen entsprechend den Bestimmungen über die internationale polizeiliche Amtshilfe zulässig.

(5) Jede Abfrage und Übermittlung personenbezogener Daten ist so zu protokollieren, dass eine Zuordnung der Abfrage oder Übermittlung zu einem bestimmten Organwalter möglich ist. Die Protokollaufzeichnungen sind drei Jahre aufzubewahren und danach zu löschen.

(6) Die Kontrolle der Datenanwendung nach Abs. 1 obliegt dem Rechtsschutzbeauftragten nach Maßgabe des § 91c Abs. 2 SPG sowie § 15 Abs. 1.

(7) Darüber hinaus ist das Bundesamt nach Maßgabe des § 54b SPG ermächtigt, personenbezogene Daten von Menschen, die Informationen zur Erfüllung der Aufgabe der erweiterten Gefahrenerforschung (§ 6 Abs. 1 Z 1), des vorbeugenden Schutzes vor verfassungsgefährdenden Angriffen (§ 6 Abs. 1 Z 2), zur Abwehr gefährlicher Angriffe oder krimineller Verbindungen (§ 21 Abs. 1 SPG) weitergeben, zu verarbeiten.

Kommentar:

Gemäß § 12 Abs 1 Z 4 dürfen nunmehr personenbezogene Daten zu Kontakt- oder Begleitpersonen nur verarbeitet werden, wenn diese "unmittelbar" und nicht nur zufällig mit einer Gruppierung nach Z 1, Betroffenen nach Z 2 oder Verdächtigen nach Z 3 in Verbindung stehen. Diese Nachschärfung ist jedenfalls begrüßenswert, da das bloße Tatbestandsmerkmal "nicht nur zufällig" sehr weit auslegbar ist und somit ein sehr unbestimmter Gesetzesbegriff doch etwas eingeschränkt wurde. Damit wird klargestellt, dass es zu einer unmittelbaren Kontaktaufnahme zwischen diesen Personen und denjenigen, die auch im Fokus des Staatsschutzes stehen sollten, kommen muss, um personenbezogene Daten ersterer verarbeiten zu dürfen.

Gemäß Abs 1 dürfen tat- und fallbezogene Informationen sowie Verwaltungsdaten nunmehr nur verarbeitet werden, wenn diese gemäß §§ 10 oder 11 bzw auf Grundlage des SPG oder der StPO ermittelt wurden. Hier ist anzumerken, dass diese Einschränkung aufgrund der umfangreichen Ermittlungsbefugnisse nach dem polizeilichen Staatsschutzgesetz nur eine augenscheinliche ist. Insbesondere und nach wie vor zu kritisieren ist, dass die Ermittlung von im Internet öffentlich zugänglicher Daten gemäß § 10 Abs 5 mithilfe von Open Source Intelligence Tools und deren gemeinsame Weiterverarbeitung von Daten aus nicht-öffentlichen Quellen besondere Abgrenzungsschwierigkeiten zur (nach dem PStSG nicht zulässigen) "Rasterfahndung" aufwirft. Überdies ist zu bedenken, dass die Speicherung von (wenn auch öffentlich zugänglichen) personenbezogenen Daten einen Grundrechtseingriff darstellt. Diesbezüglich besteht ein grundrechtliches Determinierungsgebot, dem aber § 10 Abs 5 nicht gerecht wird, da die Ermittlung ohne konkrete Vorgaben und Beschränkungen als zulässig erachtet wird.

Gemäß Abs 3 sind Daten von Kontakt- oder Begleitpersonen nunmehr längstens nach drei (statt wie bisher fünf) Jahren zu löschen. Abschließend kann nicht beurteilt werden, inwiefern die kürzere Speicherfrist angemessen ist, zumal unseres Erachtens in vielen Fällen schon die Datenerhebungsbefugnis nicht verfassungskonform ist.

Besondere Löschungsverpflichtung

§ 13. (1) Soweit sich eine Aufgabe nach § 6 Abs. 1 Z 1 oder 2 gestellt hat, sind die nach diesem Bundesgesetz ermittelten personenbezogenen Daten zu löschen, wenn sich nach Ablauf der Zeit, für die die Ermächtigung dazu erteilt wurde, keine Aufgabe für die Organisationseinheiten gemäß § 1 Abs. 3 stellt. Überdies kann die unverzügliche Löschung unterbleiben, wenn in Hinblick auf die Gruppierung oder den Betroffenen aufgrund bestimmter Tatsachen, insbesondere aufgrund von verfassungsgefährdenden Aktivitäten im Ausland, erwartet werden kann, dass sie neuerlich Anlass zu einer Aufgabe nach § 6 Abs. 1 Z 1 oder 2 geben wird. Die Organisationseinheiten gemäß § 1 Abs. 3 haben diese Daten einmal jährlich daraufhin zu prüfen, ob ihre Weiterverarbeitung erforderlich ist. Wenn sich zwei Jahre nach Ablauf der Zeit, für die die Ermächtigung dazu erteilt wurde, keine Aufgabe für die Organisationseinheiten gemäß § 1 Abs. 3 stellt, bedarf die Weiterverarbeitung für jeweils ein weiteres Jahr der Ermächtigung des Rechtsschutzbeauftragten (§ 15). Nach Ablauf von sechs Jahren sind die Daten jedenfalls zu löschen.

(2) Wird der Betroffene nach Ende der Ermächtigung gemäß § 16 Abs. 2 von den Organisationseinheiten gemäß § 1 Abs. 3 informiert, sind die nach diesem Bundesgesetz ermittelten personenbezogenen Daten unbeschadet von Abs. 1 für sechs Monate aufzubewahren; diese Frist verlängert sich um jenen Zeitraum, als die Information des Betroffenen nach § 16 Abs. 3 aufgeschoben wird. Darüber hinaus sind die Daten nicht vor Abschluss eines Rechtsschutzverfahrens zu löschen. Diesfalls sind die Daten für den Zugriff zu sperren und dürfen nur zum Zweck der Information Betroffener oder in einem Rechtsschutzverfahren verwendet werden.

Kommentar:

zu Abs 1:

§ 14 Abs 2 PStSG idF des Begutachtungsentwurfes vom 31.03.2015 lautet:

"Die unverzügliche Löschung kann jedoch unterbleiben, wenn in Hinblick auf die Person oder Gruppierung aufgrund bestimmter Tatsachen erwartet werden kann, dass sie neuerlich Anlass zu einer Aufgabe nach § 6 Abs. 1 Z 1 oder 2 geben wird."

§ 13 Abs 1 Satz 2 PStSG idFBGBl. I 5/2106 lautet:

"Überdies kann die unverzügliche Löschung unterbleiben, wenn in Hinblick auf die Gruppierung oder den Betroffenen aufgrund bestimmter Tatsachen, insbesondere aufgrund von verfassungsgefährdenden Aktivitäten im Ausland, erwartet werden kann, dass sie neuerlich Anlass zu einer Aufgabe nach § 6 Abs. 1 Z 1 oder 2 geben wird."

Hier handelt es sich offenbar um ein Redaktionsversehen, nachdem der zitierte Satz in dieser Form grammatikalisch und sprachlich keinen Sinn ergibt. Eine unverzügliche Löschung soll nämlich nur dann unterbleiben können, wenn *die Gruppierung* oder *die betroffene Person* neuerlich Anlass zu einer Aufgabe nach § 6 Abs 1 Z 1 oder Z 2 geben wird. Erklärt werden kann dieses Versehen mit einem Blick auf die Fassung des § 14 Abs 2 aus dem Begutachtungsentwurf und dessen Umgestaltung im Laufe des Gesetzgebungsprozesses. Nichtsdestotrotz ist es wichtig, dass bei einem Gesetz, das zahlreiche unbestimmte Gesetzesbegriffe und dynamische Verweisungen sowie einen nicht leicht überschaubaren Deliktskatalog beinhaltet, die Normen auch im Hinblick auf die Transparenz und die Vorhersehbarkeit präzise formuliert sind.

Geregelt werden in § 13 Abs 1 besondere Löschungsverpflichtungen, wobei die Löschung unter bestimmten Voraussetzungen unterbleiben kann. Am Ende des Abs 1 steht, dass nach Ablauf von sechs Jahren "die Daten" jedenfalls zu löschen sind. Nach dem Wortlaut ist unklar, ob sich die Löschungsverpflichtung auf alle nach dem PStSG gespeicherten Daten bezieht oder nur auf diejenigen Daten, die unter Abs 1 fallen. Man könnte nämlich die Wortfolge als "diese Daten" deuten. Die Systematik der Norm spricht für eine restriktive Auslegung. Die Wortfolge findet sich am Ende eines Absatzes, der Speicherdauer und Voraussetzungen für die Speicherung bestimmter Daten regelt, womit es naheliegend wäre, darin keine absolute Speicherdauer für alle nach dem PStSG gespeicherten Daten zu erblicken. Ebenso spricht der letzte Satz des Abs 2 von "die Daten" und bezieht sich eindeutig nur auf den zweiten Absatz. Auch die Materialien sprechen von einer Höchstfrist von sechs Jahren "gerechnet ab dem Ende der erteilten Ermächtigung". Offenbar gibt es also einen Zusammenhang zwischen der Höchstfrist und der erteilten Ermächtigung. Gemäß § 14 Abs 2 ist eine Ermächtigung nur für die Aufgabenerfüllung gemäß § 6 Abs 1 Z 1 und 2, nicht aber für Aufgaben gemäß Z 3[5] vorgesehen. Für Daten, die zur Erfüllung letzterer Aufgabe gespeichert wurden, gilt die Höchstfrist von sechs Jahren somit nicht. Im Übrigen enthält das PStSG für Daten, die aufgrund der Aufgabe gemäß § 6 Abs 1 Z 3 gespeichert wurden, gar keine Regelungen. Zu beachten ist, dass Verdächtige gemäß § 6 Abs 1 Z 3 zwar nicht ausdrücklich in § 12 Abs 1 (Analysedatenbank) genannt sind, sie aber unter Z 3 leg cit zu subsumieren sind und somit diesbezügliche Daten sehr wohl in der Datenbank gespeichert werden können. Zum fehlenden Rechtsschutz dieser Verdächtigen siehe den Kommentar zu § 14.

[5] § 6 Abs 1 Z 3: Schutz vor verfassungsgefährdenden Angriffen aufgrund von Informationen bestimmter Behörden oder Organe zu verdächtigen Personen.

zu Abs 2:

Dass nunmehr technische Safeguards (Zugriffssperre auf Daten) eingerichtet werden und Daten nach Einleitung eines Rechtsschutzverfahrens nur mehr zur Information Betroffener oder in einem Rechtsschutzverfahren verwendet werden dürfen, ist sicherlich begrüßenswert. Durch diese Maßnahme wird auch die Gefahr vermindert, dass Daten nachträglich missbräuchlich verändert werden. Wie die technische Umsetzung dieser Zugriffssperre in der Praxis aussehen wird, wird jedenfalls genau zu beobachten sein.

Zu beachten ist allerdings, dass für die Speicherung dieser Daten keine Höchstfrist besteht, da auch keine Höchstfrist für die Aufschiebung der Information Betroffener vorgesehen ist.

Ganz allgemein besteht aufgrund des verfassungsmäßigen Verhältnismäßigkeitsgrundsatzes eine Löschungsverpflichtung für nicht mehr benötigte Daten, selbst wenn eine allfällige Höchstspeicherfrist noch nicht erreicht ist. Im PStSG ist aber weder die Möglichkeit Betroffener, die Löschung selbst zu beantragen, noch ein Mechanismus vorgesehen, die Speicherung der Daten in regelmäßigen Abständen auf ihre Verhältnismäßigkeit hin zu überprüfen.

4. Hauptstück
Rechtsschutz auf dem Gebiet des polizeilichen Staatsschutzes
Rechtsschutzbeauftragter

§ 14. (1) Dem Rechtsschutzbeauftragten (§ 91a SPG) obliegt der besondere Rechtsschutz bei den Aufgaben nach § 6 Abs. 1 Z 1 und 2 sowie die Kontrolle der Datenanwendung nach § 12 Abs. 6.

(2) Die Organisationseinheiten gemäß § 1 Abs. 3, denen sich eine Aufgabe gemäß § 6 Abs. 1 Z 1 oder 2 stellt, haben vor der Durchführung der Aufgabe die Ermächtigung des Rechtsschutzbeauftragten im Wege des Bundesministers für Inneres einzuholen. Dasselbe gilt, wenn beabsichtigt ist, besondere Ermittlungsmaßnahmen nach § 11 zu setzen oder gemäß § 10 Abs. 4 ermittelte Daten weiterzuverarbeiten. Jede Einholung einer Ermächtigung ist entsprechend zu begründen, insbesondere sind darin die Gründe für den Einsatz einer Vertrauensperson (§ 11 Abs. 1 Z 2 iVm § 54 Abs. 3 und 3a SPG) anzuführen. Eine Ermächtigung darf nur in jenem Umfang und für jenen Zeitraum erteilt werden, der zur Erfüllung der Aufgabe voraussichtlich erforderlich ist, höchstens aber für die Dauer von sechs Monaten; Verlängerungen sind zulässig.

(3) Über die Erteilung der Ermächtigung zu Ermittlungsmaßnahmen gemäß § 11 Abs. 1 Z 2 iVm § 54 Abs. 3 und 3a SPG und § 11 Abs. 1 Z 7 entscheiden der Rechtsschutzbeauftragte und zwei seiner Stellvertreter mit Stimmenmehrheit (Rechtsschutzsenat). Bei Gefahr im Verzug kann der Rechtsschutzbeauftragte die Ermächtigung vorläufig erteilen. In diesem Fall hat er die dem Rechtsschutzsenat angehörenden Stellvertreter unverzüglich zu befassen; wird die Ermächtigung nicht bestätigt, ist die Ermittlungsmaßnahme sogleich zu beenden und die bislang ermittelten Daten sind zu löschen.

Kommentar:

Dass die Erteilung einer Ermächtigung zu bestimmten Ermittlungsmaßnahmen jetzt einem Rechtsschutzsenat (bestehend aus drei Rechtsschutzbeauftragten) und nicht einem einzelnen Rechtsschutzbeauftragten obliegt, ist eine willkommene Verbesserung, die als Reaktion auf die kritischen Stimmen diverser Stakeholder aufzufassen ist. Eine Entscheidungsfindung im Kollegium erhöht sicherlich die Qualität der Entscheidung (konkret genügt einfache Stimmenmehrheit, wobei bei Gefahr im Verzug die Entscheidung eines Rechtsschutzbeauftragten reicht, die Zustimmung der übrigen beiden aber nachzuholen ist). Nicht nachvollziehbar ist allerdings, warum eine Senatsentscheidung nur zur Genehmigung einer verdeckten Ermittlung (§ 11 Abs 1 Z 2) und zur Einholung von Auskünften über Verkehrs-, Zugangs- und Standortdaten (§ 11 Abs 1 Z 7) ergehen soll, für die Genehmigung der übrigen Ermittlungsmaßnahmen, die allesamt ebenso die Verarbeitung personenbezogener Daten und somit die Privatsphäre betreffen und einen Grundrechtseingriff darstellen, aber weiterhin die Entscheidung eines einzelnen Rechtsschutzbeauftragten ausreichen soll.

Nachdem die Aufgabe gemäß § 6 Abs 1 Z 3 gänzlich der Kontrolle des Rechtsschutzbeauftragten entzogen ist, der Betroffene über diese Aufgabe auch nicht informiert werden muss[6] und somit die Speicherung diesbezüglicher Daten völlig schutzlos erfolgt, ist in diesem Zusammenhang der Rechtsschutz ganz sicher nicht ausreichend. Diese Thematik potenziert sich noch, wenn man bedenkt, dass Informationen aus dem Ausland schlicht und einfach falsch sein können und auch im Ausland kein Rechtsschutz besteht. An dieser Stelle sei auch daran erinnert, dass der Rechtsschutzbeauftragte nach dem Wortlaut des § 14 Abs 2 und dessen Verweis auf § 13 die Einhaltung der Pflicht zur Richtigstellung oder Löschung solcher Daten *nicht* überwachen muss.

Die Kritik aus den vorangegangenen Stellungnahmen, insbesondere, dass die Genehmigung der Ermittlungsmaßnahmen nach dem PStSG nicht von einem mit den verfassungsrechtlichen Garantien ausgestatteten Richter erfolgt, bleibt unverändert aufrecht.

Rechte und Pflichten des Rechtsschutzbeauftragten

§ 15. (1) Die Organisationseinheiten gemäß § 1 Abs. 3 haben dem Rechtsschutzbeauftragten bei der Wahrnehmung seiner Aufgaben jederzeit Einblick in alle erforderlichen Unterlagen und Aufzeichnungen sowie in die Datenanwendung nach § 12 Abs. 1 zu gewähren, ihm auf Verlangen Abschriften (Ablichtungen) einzelner Aktenstücke unentgeltlich auszufolgen und alle erforderlichen Auskünfte zu erteilen; insofern kann ihm

Deleted:

[6] Die Information Betroffener gemäß § 16 Abs 1 und 2 ist auf Aufgaben gemäß § 6 Abs 1 Z 1 und 2 beschränkt.

gegenüber Amtsverschwiegenheit nicht geltend gemacht werden. Dies gilt jedoch nicht für Auskünfte über die Identität von Personen nach Maßgabe des § 162 StPO.

(2) Dem Rechtsschutzbeauftragten ist jederzeit Gelegenheit zu geben, die Durchführung der in § 14 Abs. 2 genannten Maßnahmen zu überwachen und alle Räume zu betreten, in denen Aufnahmen oder sonstige Überwachungsergebnisse aufbewahrt werden. Darüber hinaus hat er im Rahmen seiner Aufgabenstellungen die Einhaltung der Pflicht zur Richtigstellung oder Löschung nach § 13 zu überwachen.

(3) In Verfahren über Beschwerden von Betroffenen einer Aufgabe nach § 6 Abs. 1 Z 1 oder 2 vor der Datenschutzbehörde, den Verwaltungsgerichten sowie den Gerichtshöfen des öffentlichen Rechts kommt dem Rechtsschutzbeauftragten die Stellung einer mitbeteiligten Amtspartei zu.

(4) Der Rechtsschutzbeauftragte erstattet dem Bundesminister für Inneres jährlich bis spätestens 31. März des Folgejahres einen Bericht über seine Tätigkeit und Wahrnehmungen im Rahmen seiner Aufgabenerfüllung nach diesem Bundesgesetz.

Kommentar:

Dass der Rechtsschutzbeauftragte jetzt auch Einblick in die Analysedatenbank hat, ist zwar erfreulich, um die Kontrollbefugnisse wirksam ausüben zu können, sollte dies aber ohnehin selbstverständlich sein. Zu kritisieren ist jedoch, dass dem Rechtsschutzbeauftragten die Kontrolle von gem § 12 Abs 7 gespeicherten personenbezogenen Daten von Vertrauenspersonen gänzlich entzogen ist (§ 14 Abs 1 iVm § 12 Abs 6).

Information Betroffener

§ 16. (1) Nimmt der Rechtsschutzbeauftragte wahr, dass durch Verwenden personenbezogener Daten Rechte von Betroffenen einer Aufgabe nach § 6 Abs. 1 Z 1 oder 2 verletzt worden sind, die von dieser Datenverwendung keine Kenntnis haben, so ist er zu deren Information oder, sofern eine solche aus den Gründen des § 26 Abs. 2 DSG 2000 nicht erfolgen kann, zur Erhebung einer Beschwerde an die Datenschutzbehörde nach § 90 SPG verpflichtet. In einem solchen Verfahren vor der Datenschutzbehörde ist auf § 26 Abs. 2 DSG 2000 über die Beschränkung des Auskunftsrechtes Bedacht zu nehmen.

(2) Nach Ablauf der Zeit, für die die Ermächtigung erteilt wurde, ist der Betroffene einer Aufgabe nach § 6 Abs. 1 Z 1 oder 2 von den Organisationseinheiten gemäß § 1 Abs. 3 über Grund, Art und Dauer sowie die Rechtsgrundlage der gesetzten Maßnahmen zu informieren. Über die durchgeführte Information ist der Rechtsschutzbeauftragte in Kenntnis zu setzen.

(3) Die Information kann mit Zustimmung des Rechtsschutzbeauftragten aufgeschoben werden, solange durch sie die Aufgabenerfüllung gefährdet wäre, und unterbleiben, wenn der Betroffene bereits nachweislich Kenntnis erlangt hat, die Information des Betroffenen unmöglich ist oder aus den Gründen des § 26 Abs. 2 DSG 2000 nicht erfolgen kann.

Kommentar:

keine Änderungen

Berichte über den polizeilichen Staatsschutz

§ 17. (1) Das Bundesamt hat unter Einbeziehung der Tätigkeiten der für Verfassungsschutz zuständigen Organisationseinheiten der Landespolizeidirektionen jährlich einen Bericht zu erstellen, mit dem die Öffentlichkeit, unter Einhaltung von gesetzlichen Verschwiegenheitspflichten, über aktuelle und mögliche staatsschutzrelevante Entwicklungen informiert wird.

(2) Der Bundesminister für Inneres hat dem ständigen Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit in dessen Sitzungen über Unterrichtungen gemäß § 8 Abs. 2 erster Satz zu berichten.

(3) Über die Erfüllung der Aufgaben nach diesem Bundesgesetz sowie über die Information Betroffener nach § 16 hat 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 zu berichten.

(4) Den Bericht des Rechtsschutzbeauftragten gemäß § 15 Abs. 4 hat der Bundesminister für Inneres dem ständigen Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit zu übermitteln.

(5) Der Rechtsschutzbeauftragte hat dem ständigen Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit für Auskünfte über wesentliche Entwicklungen zur Verfügung zu stehen; zudem steht es dem Rechtsschutzbeauftragten frei, in solchen Angelegenheiten jederzeit von sich aus an den ständigen Unterausschuss heranzutreten. In einem solchen Fall hat er seine Absicht dem Vorsitzenden des ständigen Unterausschusses mitzuteilen, der für eine umgehende Einberufung sorgt.

Kommentar:

keine Änderungen

5. Hauptstück
Schlussbestimmungen
Inkrafttreten

§ 18. (1) Dieses Bundesgesetz tritt mit 1. Juli 2016 in Kraft.

(2) Verordnungen auf Grund dieses Bundesgesetzes können bereits ab dem auf seine Kundmachung folgenden Tag erlassen werden; sie dürfen jedoch frühestens mit dem Inkrafttreten dieses Bundesgesetzes in Kraft gesetzt werden.

Kommentar:

keine Änderungen

Sprachliche Gleichbehandlung

§ 19. Soweit in diesem Bundesgesetz auf natürliche Personen bezogene Bezeichnungen nur in männlicher Form angeführt sind, beziehen sie sich auf Frauen und Männer in gleicher Weise. Bei der Anwendung der Bezeichnungen auf bestimmte natürliche Personen ist die geschlechtsspezifische Form zu verwenden.

Kommentar:

keine Änderungen

Verweisungen

§ 20. Verweisungen in diesem Bundesgesetz auf andere Bundesgesetze sind als Verweisungen auf die jeweils geltende Fassung zu verstehen.

Kommentar:

keine Änderungen

Übergangsbestimmungen

§ 21. (1) Vor Inkrafttreten dieses Bundesgesetzes erteilte Ermächtigungen gemäß § 91c Abs. 3 SPG in der Fassung vor Inkrafttreten dieses Bundesgesetzes gelten als Ermächtigungen gemäß § 14 Abs. 2 und bleiben bis zum festgesetzten Zeitpunkt, längstens bis zum 31. Dezember 2016, weiterhin gültig; für diese gelten die Löschungsfristen nach § 13.

(2) Personenbezogene Daten, die vor Inkrafttreten dieses Bundesgesetzes von den Organisationseinheiten gemäß § 1 Abs. 3 für die Aufgabe nach § 21 Abs. 3 SPG in der Fassung vor Inkrafttreten dieses Bundesgesetzes rechtmäßig ermittelt wurden, dürfen nach Maßgabe des § 12 Abs. 1 und 2 in der Datenanwendung gemäß § 12 verarbeitet werden.

(3) Lokale Datenanwendungen der Organisationseinheiten gemäß § 1 Abs. 3, die vor Inkrafttreten dieses Bundesgesetzes auf Grundlage des § 53 SPG geführt wurden, dürfen für die Aufgaben nach dem SPG bis zur vollständigen Inbetriebnahme der Datenanwendung nach § 12, längstens bis zum 1. Juli 2017 weitergeführt werden. Darüber hinaus dürfen diese Datenanwendungen ausschließlich für die Zwecke der Übernahme von rechtmäßig verarbeiteten Daten in die Datenanwendung nach § 12 und der Durchführung von Abfragen nach Maßgabe anderer bundesgesetzlicher Regelungen oder unionsrechtlicher Vorschriften bis 1. Juli 2019 weitergeführt werden.

(4) Personen, die im Zeitpunkt des Inkrafttretens dieses Bundesgesetzes bereits Bedienstete der Organisationseinheiten gemäß § 1 Abs. 3 sind, haben die in § 2 Abs. 3 vorgesehene spezielle Ausbildung für Verfassungsschutz und Terrorismusbekämpfung innerhalb von drei Jahren ab dem Tag des Inkrafttretens zu absolvieren.

Kommentar:

Die Änderung betrifft eine Konkretisierung der Handhabung der derzeit bestehenden lokalen Datenanwendungen und deren Überführung in die neue Analysedatenbank.

Vollziehung

§ 22. Mit der Vollziehung dieses Bundesgesetzes ist der Bundesminister für Inneres betraut.

Kommentar:

keine Änderungen

Artikel 2

Änderung des Sicherheitspolizeigesetzes

Das Sicherheitspolizeigesetz (SPG), BGBl. Nr. 566/1991, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 43/2014 und die Kundmachung BGBl. I Nr. 97/2014, wird wie folgt geändert:

1. *Im Inhaltsverzeichnis wird im Eintrag zu § 25 das Wort* „Kriminalpolizeiliche“ *durch das Wort* „Sicherheitspolizeiliche“ *ersetzt und es entfällt der Eintrag* „§ 93a Information verfassungsmäßiger Einrichtungen“.

2. *In § 6 Abs. 1 zweiter Satz werden nach dem Wort* „Bundeskriminalamtes“ *die Wortfolge* „und des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung“ *sowie nach dem Wort* „erfolgt“ *das Wort* „jeweils“ *eingefügt und es wird das Wort* „Organisationseinheit“ *durch das Wort* „Organisationseinheiten“ *ersetzt.*

3. *Dem § 13a wird folgender Abs. 3 angefügt:*

   „(3) Zum Zweck der Dokumentation von Amtshandlungen, bei denen die Organe des öffentlichen Sicherheitsdienstes Befehls- und Zwangsgewalt ausüben, ist der offene Einsatz von Bild- und Tonaufzeichnungsgeräten, sofern gesetzlich nicht anderes bestimmt ist, nach Maßgabe der Bestimmungen dieses Absatzes zulässig. Vor Beginn der Aufzeichnung ist der Einsatz auf solche Weise anzukündigen, dass er dem Betroffenen bekannt wird. Die auf diese Weise ermittelten personenbezogenen Daten dürfen nur zur Verfolgung von strafbaren Handlungen, die sich während der Amtshandlung ereignet haben, sowie zur Kontrolle der Rechtmäßigkeit der Amtshandlung ausgewertet werden. Bis zu ihrer Auswertung und Löschung sind die Aufzeichnungen gemäß den Bestimmungen des § 14 DSG 2000 vor unberechtigter Verwendung, insbesondere durch Protokollierung jedes Zugriffs und Verschlüsselung

der Daten, zu sichern. Sie sind nach sechs Monaten zu löschen; kommt es innerhalb dieser Frist wegen der Amtshandlung zu einem Rechtsschutzverfahren, so sind die Aufzeichnungen erst nach Abschluss dieses Verfahrens zu löschen. Bei jeglichem Einsatz von Bild- und Tonaufzeichnungsgeräten ist besonders darauf zu achten, dass Eingriffe in die Privatsphäre der Betroffenen die Verhältnismäßigkeit (§ 29) zum Anlass wahren."

4. *In § 20 wird das Wort „kriminalpolizeiliche" durch das Wort „sicherheitspolizeiliche" ersetzt.*

5. *Nach § 21 Abs. 2 wird folgender Abs. 2a eingefügt:*

„(2a) Den Sicherheitsbehörden obliegen die Abwehr und Beendigung von gefährlichen Angriffen gegen Leben, Gesundheit, Freiheit oder Eigentum auch an Bord von Zivilluftfahrzeugen, soweit sich ihre Organe auf begründetes Ersuchen des Luftfahrzeughalters oder zur Erfüllung gesetzlicher Aufgaben an Bord befinden und Völkerrecht dem nicht entgegensteht."

6. *Die §§ 21 Abs. 3, 63 Abs. 1a und 1b, 91c Abs. 3 sowie 93a samt Überschrift entfallen.*

7. *In der Überschrift zu § 25 wird das Wort* „Kriminalpolizeiliche" *durch das Wort* „Sicherheitspolizeiliche" *ersetzt.*

8. *In § 53 entfallen in Abs. 1 die Z 2a und 7 und es wird am Ende der Z 6 der Strichpunkt durch einen Punkt ersetzt, in Abs. 3 entfallen der Beistrich nach dem Wort* „Angriffe" *und die Wortfolge* „für die erweiterte Gefahrenerforschung unter den Voraussetzungen nach Abs. 1" *und in Abs. 5 entfällt die Wortfolge* „für die erweiterte Gefahrenerforschung (§ 21 Abs. 3)"*.*

9. *In § 53 Abs. 3b wird nach der Wortfolge* „die internationale Mobilteilnehmerkennung (IMSI) der" *die Wortfolge* „vom Gefährder oder" *eingefügt.*

10. *In § 53 Abs. 4 wird die Wortfolge* „auf allgemein" *durch die Wortfolge* „etwa auf im Internet öffentlich" *ersetzt.*

11. *In § 53a entfällt in Abs. 1 die Wortfolge* „den Personen- und Objektschutz und"*.*

12. *Nach § 53a Abs. 1 wird folgender Abs. 1a eingefügt:*

„(1a) Die Sicherheitsbehörden dürfen für den Personen- und Objektschutz Erreichbarkeits- und Identifikationsdaten über die gefährdete natürliche oder juristische Person, die erforderlichen Sachdaten einschließlich KFZ-Kennzeichen zu den zu schützenden Objekten, Angaben zu Zeit, Ort, Grund und Art des Einschreitens sowie Verwaltungsdaten verarbeiten."

13. *Nach § 53a Abs. 5 wird folgender Abs. 5a eingefügt:*

„(5a) Datenanwendungen nach Abs. 1a zum Schutz von verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit (§ 22 Abs. 1 Z 2), der Vertreter ausländischer Staaten, internationaler Organisationen und anderer Völkerrechtssubjekte (§ 22 Abs. 1 Z 3) sowie von kritischen Infrastrukturen (§ 22 Abs. 1 Z 6) dürfen der Bundesminister für Inneres und die Landespolizeidirektionen als datenschutzrechtliche Auftraggeber in einem vom Bundesamt für Verfassungsschutz und Terrorismusbekämpfung betriebenen Informationsverbundsystem führen. Übermittlungen der gemäß Abs. 1a verarbeiteten Daten sind an Sicherheitsbehörden für Zwecke der Sicherheitspolizei und Strafrechtspflege, an Staatsanwaltschaften und

ordentliche Gerichte für Zwecke der Strafrechtspflege, darüber hinaus an Dienststellen inländischer Behörden, soweit dies eine wesentliche Voraussetzung zur Wahrnehmung einer ihr gesetzlich übertragenen Aufgabe ist, an ausländische Sicherheitsbehörden und Sicherheitsorganisationen (§ 2 Abs. 2 und 3 PolKG) entsprechend den Bestimmungen über die internationale polizeiliche Amtshilfe und im Übrigen nur zulässig, wenn hierfür eine ausdrückliche gesetzliche Ermächtigung besteht."

14. *In § 54 entfallen in Abs. 2 die Z 1 sowie in Abs. 4 die Wortfolge* „und zur erweiterten Gefahrenerforschung (§ 21 Abs. 3)".

15. § 54 Abs. 3 lautet:

„(3) Das Einholen von Auskünften durch die Sicherheitsbehörde ohne Hinweis gemäß Abs. 1 oder im Auftrag der Sicherheitsbehörde durch andere Personen (Vertrauenspersonen), die ihren Auftrag weder offen legen noch erkennen lassen, ist zulässig, wenn sonst die Abwehr gefährlicher Angriffe oder krimineller Verbindungen gefährdet oder erheblich erschwert wäre (verdeckte Ermittlung). Wohnungen und andere vom Hausrecht geschützte Räume dürfen im Rahmen einer verdeckten Ermittlung nur im Einverständnis mit dem Inhaber betreten werden; dieses darf nicht durch Täuschung über eine Zutrittsberechtigung herbeigeführt werden."

16. *Nach § 54 Abs. 3 wird folgender Abs. 3a eingefügt:*

„(3a) Die Vertrauensperson ist von der Sicherheitsbehörde zu führen und regelmäßig zu überwachen. Ihr Einsatz und dessen nähere Umstände sowie Auskünfte und Mitteilungen, die durch sie erlangt werden, sind zu dokumentieren (§ 13a), sofern diese für die Aufgabenerfüllung von Bedeutung sein können. § 54a gilt für verdeckte Ermittlungen durch Vertrauenspersonen nicht."

17. *In § 54 Abs. 5 wird im ersten Satz vor der Wortfolge* „einer Zusammenkunft" *die Wortfolge* „oder im Zusammenhang mit" *eingefügt und der letzte Satz lautet:*

„Die auf diese Weise ermittelten Daten dürfen auch zur Abwehr und Verfolgung gefährlicher Angriffe sowie zur Verfolgung strafbarer Handlungen in Angelegenheiten der Sicherheitsverwaltung, nach Art. III Abs. 1 Z 4 EGVG, § 3 AbzeichenG sowie § 3 Symbole-Gesetz, BGBl. I Nr. 103/2014, die sich im Zusammenhang mit oder während der Zusammenkunft ereignen, verwendet werden."

18. *In § 58b Abs. 2 erster Satz wird das Wort* „Asylverfahren" *durch die Wortfolge* „Verfahren nach § 3 BFA-Verfahrensgesetz – BFA-VG, BGBl. I Nr. 87/2012," *ersetzt.*

19. *§ 59 Abs. 2 lautet:*

„(2) Jede Abfrage und Übermittlung personenbezogener Daten aus der Zentralen Informationssammlung und den übrigen Informationsverbundsystemen ist so zu protokollieren, dass eine Zuordnung der Abfrage oder Übermittlung zu einem bestimmten Organwalter möglich ist. Die Zuordnung zu einem bestimmten Organwalter ist bei automatisierten Abfragen nicht erforderlich. Von der Protokollierung gänzlich ausgenommen sind automatisierte Abfragen gemäß § 54 Abs. 4b, es sei denn, es handelt sich um einen Treffer. Die Protokollaufzeichnungen sind drei Jahre aufzubewahren und danach zu löschen."

20. *Nach § 75 Abs. 1 wird folgender Abs. 1a eingefügt:*

„(1a) Die Sicherheitsbehörden sind ermächtigt, eine nach den Bestimmungen der StPO ermittelte Spur, die einer Person, die im Verdacht steht, eine mit gerichtlicher Strafe

bedrohte vorsätzliche Handlung begangen zu haben, zugehört oder zugehören dürfte, und deren Ermittlung durch erkennungsdienstliche Maßnahmen erfolgen könnte (§ 64 Abs. 2), zum Zweck ihrer Zuordnung zu einer Person in der Zentralen erkennungsdienstlichen Evidenz zu verarbeiten. Zur Spur dürfen auch Verwaltungsdaten verarbeitet werden. Die Daten sind zu löschen, wenn der für die Speicherung maßgebliche Verdacht nicht mehr besteht oder der bezughabende Akt im Dienste der Strafrechtspflege zu löschen ist (§ 13a Abs. 2).“

21. *In § 75 Abs. 2 wird im ersten Satz nach der Wortfolge* „zu benützen“ *die Wortfolge* „und zu vergleichen“ *eingefügt, im zweiten Satz vor dem Wort* „Übermittlungen“ *die Wortfolge* „Abfragen und“ *eingefügt sowie das Zitat* „Abs. 1“ *durch das Zitat* „Abs. 1 und 1a“ *ersetzt.*

22. *Nach § 80 Abs. 1 wird folgender Abs. 1a eingefügt:*

„(1a) Sofern Auskunft über die gemäß § 75 Abs. 1a verarbeiteten Daten begehrt wird, sind die Sicherheitsbehörden ermächtigt, gegen Kostenersatz (Abs. 1 letzter Satz) vom Auskunftswerber Abbildungen oder Papillarlinienabdrücke herzustellen oder seine DNA zu ermitteln, und diese Daten mit den gemäß § 75 Abs. 1a verarbeiteten Daten zu vergleichen. Von der Erteilung der Auskunft ist abzusehen, wenn der Auskunftswerber an der Ermittlung dieser Daten nicht mitgewirkt oder er den Kostenersatz nicht geleistet hat. Die aus Anlass des Auskunftsverlangens ermittelten Daten über den Auskunftswerber sind gesondert zu verwahren und dürfen innerhalb eines Zeitraums von einem Jahr, im Falle der Erhebung einer Beschwerde gemäß § 31 DSG 2000 an die Datenschutzbehörde bis zum rechtskräftigen Abschluss des Verfahrens, nicht vernichtet werden.“

23. *In § 91a Abs. 1 werden das Wort* „zwei“ *durch die Wortfolge* „der erforderlichen Anzahl von“ *und die Wortfolge* „nach dem Sicherheitspolizeigesetz“ *durch die Wortfolge* „auf dem Gebiet der Sicherheitspolizei“ *ersetzt.*

24. *§ 91a Abs. 2 lautet:*

„(2) Der Rechtsschutzbeauftragte und seine Stellvertreter haben gleiche Rechte und Pflichten. Im Bereich des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz – PStSG, BGBl. I Nr. xx/201x) haben sie sich regelmäßig über ihre Wahrnehmungen zu unterrichten und in grundsätzlichen Fragen der Aufgabenerfüllung eine einvernehmliche Vorgangsweise anzustreben. Sie werden vom Bundespräsidenten auf Vorschlag der Bundesregierung nach Anhörung der Präsidenten des Nationalrates sowie der Präsidenten des Verfassungsgerichtshofes und des Verwaltungsgerichtshofes auf die Dauer von fünf Jahren bestellt. Wiederbestellungen sind zulässig. Zumindest bei einem Stellvertreter muss es sich um eine Person handeln, die als Richter oder Staatsanwalt mindestens zehn Jahre tätig war und nicht gemäß § 91b Abs. 1 zweiter Satz ausgeschlossen ist. Der Rechtsschutzbeauftragte hat gemeinsam mit seinen Stellvertretern nähere Regelungen zu ihrem Zusammenwirken, insbesondere über die Vertretung des Rechtsschutzbeauftragten im Verhinderungsfall, die Einberufung von Sitzungen, die Zusammensetzung des Rechtsschutzsenates (§ 14 Abs. 3 PStSG) sowie dessen Entscheidungsfindung in einer Geschäftsordnung zu treffen.“

25. *§ 91b Abs. 3 lautet:*

„(3) Der Bundesminister für Inneres stellt dem Rechtsschutzbeauftragten und seinen Stellvertretern die zur Bewältigung der administrativen Tätigkeit notwendigen Personal- und Sacherfordernisse zur Verfügung, wobei diese den jeweiligen gesetzlichen Aufgaben adäquat anzupassen sind. Zur Gewährung der Unabhängigkeit sind dem Rechtsschutzbeauftragten Büroräumlichkeiten außerhalb des Raumverbundes der Generaldirektion für die öffentliche Sicherheit oder einer ihr nachgeordneten Sicherheitsbehörde zur Verfügung zu stellen. Dem Rechtsschutzbeauftragten und seinen Stellvertretern gebührt für die Erfüllung ihrer Aufgaben eine Entschädigung. Der Bundesminister für Inneres ist ermächtigt, mit Verordnung Pauschalsätze für die Bemessung dieser Entschädigung festzusetzen."

26. *In § 91c Abs. 1 wird im ersten Satz das Zitat* „(§ 54 Abs. 3)" *durch das Zitat* „(§ 54 Abs. 3 und 3a)" *ersetzt, es entfällt der zweite Satz und es wird das Wort* „Kennzeichnerkennungsgeräten" *durch das Wort* „Kennzeichenerkennungsgeräten" *ersetzt.*

27. *§ 91d Abs. 1 letzter Satz lautet:*

„Dies gilt jedoch nicht für Auskünfte über die Identität von Personen nach Maßgabe des § 162 StPO."

28. *In § 91d wird in Abs. 3 der Satz* „In einem solchen Verfahren vor der Datenschutzbehörde ist auf § 26 Abs. 2 DSG 2000 über die Beschränkung des Auskunftsrechtes Bedacht zu nehmen." *angefügt; in Abs. 4 wird der Strichpunkt durch einen Punkt ersetzt und es entfällt die Wortfolge* „insbesondere ist darin auf Ermächtigungen nach § 91c Abs. 3 Bezug zu nehmen.".

29. *Dem § 94 werden folgende Abs. 38 und 39 angefügt:*

„(38) Die §§ 13a Abs. 3, 20, 21 Abs. 2a, die Überschrift des § 25, die §§ 54 Abs. 5, 58b Abs. 2, 59 Abs. 2, 75 Abs. 1a und 2, 80 Abs. 1a sowie der Eintrag im Inhaltsverzeichnis zu § 25 in der Fassung des Bundesgesetzes BGBl. I Nr. XX/201x treten mit 1. März 2016 in Kraft.

(39) Die §§ 6 Abs. 1, 53 Abs. 1, 3, 3b, 4 und 5, 53a Abs. 1, 1a und 5a, 54 Abs. 2, 3, 3a und 4, 91a Abs. 1 und 2, 91b Abs. 3, 91c Abs. 1, 91d Abs. 1, 3 und 4, 96 Abs. 8 und 9 sowie das Inhaltsverzeichnis in der Fassung des Bundesgesetzes BGBl. I Nr. XX/201x treten mit 1. Juli 2016 in Kraft. Gleichzeitig treten die §§ 21 Abs. 3, 63 Abs. 1a und 1b, 91c Abs. 3 und 93a samt Überschrift außer Kraft."

Deleted: 2015

30. *Dem § 96 werden folgende Abs. 8 und 9 angefügt:*

„(8) Daten, die auf Grundlage des § 53a Abs. 1 in der Fassung vor BGBl. I Nr. xx/20xx für den Personen- und Objektschutz bis zum Zeitpunkt des Inkrafttretens des Bundesgesetzes BGBl. I Nr. xx/20xx verarbeitet wurden, dürfen auf Grundlage des § 53a Abs. 1a in der Fassung BGBl. I Nr. xx/20xx weiterverarbeitet sowie unter den Voraussetzungen des § 53a Abs. 5a in der Fassung BGBl. I Nr. xx/20xx auch im Informationsverbundsystem geführt werden.

(9) § 91a Abs. 2 fünfter Satz in der Fassung des Bundesgesetzes BGBl. I Nr. xx/201x kommt bei Neu- oder Wiederbestellung eines Stellvertreters des Rechtsschutzbeauftragten nach Inkrafttreten des Bundesgesetzes BGBl. I Nr. xx/201x zur Anwendung."

Deleted: letzter

31. *Dem § 97 wird folgender Abs. 4 angefügt:*

„(4) § 13a Abs. 3 in der Fassung des Bundesgesetzes BGBl. I Nr. XX/201x tritt mit Ablauf des 31. Dezember 2019 außer Kraft."

Kommentar:

Die Änderungen im SPG sind grundrechtlich eine Verbesserung und somit zu begrüßen. Die Zweifel an der Verfassungskonformität der neuen §§ 53 Abs 3b (IMSI-Catcher) und 54 Abs 3 (Vertrauenspersonen) bleiben unverändert aufrecht.

zu Ziffer 15:

Gemäß § 54 Abs 3 SPG dürfen Wohnungen und andere vom Hausrecht geschützte Räume nunmehr im Rahmen einer verdeckten Ermittlung nur mehr im Einverständnis mit dem Inhaber betreten werden.

zu Ziffer 16:

Gemäß § 54 Abs 3a SPG dürfen über die Identität täuschende Urkunden von Behörden nicht für Vertrauenspersonen (V-Leute) ausgestellt werden. Auch wenn diese Änderung positiv zu beurteilen ist, ändert dies allerdings nichts an der schon in den vorangegangenen Stellungnahmen zum PStSG geäußerten Kritik am Konzept der Vertrauensleute insgesamt.

zu Ziffer 24:

Diese Ergänzung hat organisatorischen Charakter und keine substantiellen grundrechtlichen Auswirkungen. Zur Kritik am Konzept des Rechtsschutzbeauftragten sei an dieser Stelle auf die Einleitung und die vorangegangenen Stellungnahmen verwiesen.

II.B. Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 geändert wird (BGBl. I 6/2016)

[Anmerkung: hier erfolgten seit der letzten Stellungnahme des AK Vorrat vom 11. Jänner 2016 keine Änderungen]

Der Nationalrat hat beschlossen:

Das Telekommunikationsgesetz 2003 (TKG 2003), BGBl. I Nr. 70/2003, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 134/2015, wird wie folgt geändert:

1. *In § 90 Abs. 7 wird nach der Wortfolge* „§ 53 Abs. 3a Z 1 SPG“ *die Wortfolge* „und § 11 Abs. 1 Z 5 Polizeiliches Staatsschutzgesetz – PStSG, BGBl. I Nr. xx/2016“ *eingefügt.*

2. *In § 93 Abs. 3 wird im zweiten Satz die Wortfolge* „Nachrichten und der Auskunft über Daten einer Nachrichtenübermittlung“ *durch die Wortfolge* „Nachrichten, der Auskunft über Daten einer Nachrichtenübermittlung und der Auskunft über Daten nach § 11 Abs. 1 Z 7 PStSG“ *ersetzt.*

3. *In § 94 Abs. 1 lautet der erste Satz:*

„(1) Der Anbieter ist nach Maßgabe der gemäß Abs. 3 und 4 erlassenen Verordnungen verpflichtet, alle Einrichtungen bereitzustellen, die zur Überwachung von Nachrichten und zur Auskunft über Daten einer Nachrichtenübermittlung nach den Bestimmungen der StPO sowie zur Auskunft über Daten nach § 11 Abs. 1 Z 7 PStSG erforderlich sind.“

4. *In § 94 Abs. 2 lautet der erste Satz:*

„(2) Der Anbieter ist verpflichtet, an der Überwachung von Nachrichten und der Auskunft über Daten einer Nachrichtenübermittlung nach den Bestimmungen der StPO sowie an der Auskunft über Daten nach § 11 Abs. 1 Z 7 PStSG im erforderlichen Ausmaß mitzuwirken.“

5. *In § 94 Abs. 4 erster Satz wird die Wortfolge* „StPO sowie des SPG“ *durch die Wortfolge* „StPO, des SPG sowie des PStSG“ *ersetzt.*

6. *In § 99 wird in Abs. 1 zweiter Satz die Wortfolge* „StPO sowie des SPG“ *durch die Wortfolge* „StPO, des SPG sowie des PStSG“ *ersetzt, in Abs. 5 Z 3 nach der Wortfolge* „§ 53 Abs. 3a und 3b SPG“ *die Wortfolge* „sowie § 11 Abs. 1 Z 5 PStSG“ *und in Z 4 nach der Wortfolge* „§ 53 Abs. 3a Z 3 SPG“ *die Wortfolge* „sowie § 11 Abs. 1 Z 5 PStSG“ *eingefügt und am Ende der Z 4 der Punkt durch einen Strichpunkt ersetzt sowie folgende Z 5 angefügt:*

„5. Verkehrsdaten, Zugangsdaten und Standortdaten nach Maßgabe des § 11 Abs. 1 Z 7 PStSG.“

7. Dem § 137 wird folgender Abs. 8 angefügt:

„(8) §§ 90 Abs. 7, 93 Abs. 3, 94 Abs. 1, 2 und 4 sowie 99 Abs. 1 und 5 in der Fassung des Bundesgesetzes BGBl. I Nr. xx/2016 treten mit 1. Juli 2016 in Kraft."

Begründung:

Zu Z 1 bis 6:

Mit der Anpassung der Bestimmungen des Telekommunikationsgesetzes 2003 an das Polizeiliche Staatsschutzgesetz (PStSG) soll sichergestellt werden, dass einerseits die Grundlage für die Erteilung der Auskünfte zu § 11 Abs 1 Z 5 und 7 PStSG auf Seiten der Anbieter gegeben ist und anderseits die Auskunftsverlangen über die – eine sichere Übermittlung gewährleistende – Durchlaufstelle nach § 94 abgewickelt werden können.

Zu Z 7:

Die Bestimmungen des TKG 2003 sollen gleichzeitig mit dem PStSG in Kraft treten.

Kommentar:

Unbeschadet der allgemeinen und besonderen Kritik am PStSG und insbesondere am fehlenden richterlichen Rechtsschutz ist es grundsätzlich wichtig und richtig, dass neue Befugnisse zum Eingriff in das Kommunikationsgeheimnis ausschließlich über den sicheren und (für die Rechtsschutzorgane) nachvollziehbaren Weg der Durchlaufstelle abgewickelt werden. Dass die Befugnisse auch im § 99 Abs 5 TKG aufgezählt werden, ist rechtlich durch die lex spezialis des § 99 Abs 1 TKG geboten, der eine abschließende Aufzählung der Fälle zulässiger Datenverwendung im TKG selbst normiert. Insofern sind die im TKG vorgeschlagenen Änderungen wohl zu begrüßen, was jedoch nichts an der Kritik ändert, dass die Befugnisse selbst angesichts der bestehenden Mittel überschießend erscheinen und die Erläuterungen keine Argumente oder gar Belege dafür liefern, warum die neuen Befugnisse im Vergleich zum Status Quo erforderlich sein sollten.

Schließlich ist auch im Zusammenhang mit der Abwicklung der Auskünfte über die Durchlaufstelle auf ein bestehendes Problem hinzuweisen, nämlich die Zulässigkeit zur kompletten Umgehung der Durchlaufstelle in Fällen von „Gefahr im Verzug". Hier sollte dringend eingeführt werden, dass in solchen Fällen zumindest eine Nachmeldung über die Durchlaufstelle zu erfolgen hat, auch damit die in dieser automatisch erzeugten Statistikwerte nicht verfälscht werden.