Verein Arbeitskreis Vorratsdaten Österreich (AKVorrat.at),

ZVR: 140062668

Kirchberggasse 7/5

1070 Wien

info@akvorrat.at

Wien, 31. Juli 2015

Betreff: Stellungnahme zur Regierungsvorlage zum PStSG sowie zur SPG Novelle

Für den AKVorrat: Rolf-Dieter Kargl, Christof Tschohl

Der AKVorrat nimmt zu der Regierungsvorlage wie folgt Stellung:

RESÜMEE:

Insgesamt ist zwar zu sehen, dass mit der Regierungsvorlage auf die Kritik im Begutachtungsverfahren reagiert wurde. Wenngleich an manchen Stellen wichtige und begrüßenswerte Änderungen vorgenommen wurden, hat sich substantiell aber im Wesentlichen nicht viel verbessert. Die mangelnde Transparenz und der schwache Rechtsschutz bleiben ebenso wie die zu weit gefassten Befugnisse aufrecht. An manchen Stellen wurden auch Änderungen zum Nachteil des Grundrechtsschutzes vorgenommen. Der AKVorrat wird daher seine juristische und politische Arbeit zum Staatsschutz unbeirrt fortführen.

I. Zusammenfassung

- Im Gegensatz zum Begutachtungsentwurf ist es für die **Position des Direktors** des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung nicht mehr erforderlich, eine 5-jährige Berufserfahrung vorzuweisen. Es genügt ein Abschluss eines Studiums der Rechtswissenschaften. Eine ersatzlose Minderung der praktischen Qualifikationsvoraussetzungen ist hier aber der falsche Ansatz.
- Die **Geschäftsordnung** muss nicht mehr, wie im Begutachtungsentwurf vorgeschlagen, im Einvernehmen mit dem Generaldirektor für öffentliche Sicherheit festgelegt werden. Vor Erlassung und vor jeder Änderung der Geschäftsordnung ist der Generaldirektor für die öffentliche Sicherheit zu befassen. Die praktischen Konsequenzen dieser Änderung werden

wohl nicht allzu groß sein, dennoch sollte insofern auf die Qualifikationsvoraussetzungen des Direktors des BVT besonderes Augenmerk gelegt werden.

- Für das Bestehen der Aufgabe der Prävention „verfassungsgefährdender Angriffe“ im Sinne des § 6 Abs 1 Z 2 PStSG ist nach der Regierungsvorlage nun ein **„begründeter Gefahrenverdacht“** Voraussetzung. Nach dem Begutachtungsentwurf war es noch ausreichend, wenn ein solcher Angriff „wahrscheinlich“ ist. Dies ist zweifellos eine Verbesserung zum Begutachtungsentwurf, die im Rechtsstaat allerdings eine Selbstverständlichkeit sein sollte. Hierzu wäre jedoch zu wünschen, dass es klare Regeln gibt, wo und wie die Begründung für das Vorliegen eines konkreten Gefahrenverdachts schriftlich festzuhalten und vorzulegen ist. Die Begründungspflicht ist nur effektiv, wenn sie auch prozessual abgesichert ist.

- Die **Tatbestände „Sprengung einer Versammlung“ und „Störung einer Versammlung“** gemäß §§ 284 und 285 StGB wurden aus dem Straftatenkatalog des PStSG ersatzlos gestrichen. Auch wurde der Tatbestand des § 274 (Landfriedensbruch) dahingehend beschränkt, dass nur mehr die führende Teilnahme an einer Zusammenrottung von Menschen nach dem PStSG verfolgbar ist. Zwar wurde damit offenbar auf die Kritik insbesondere des AKVorrat reagiert, allerdings ist damit nur „die Spitze des Eisbergs“ gekappt und das grundsätzliche Problem keineswegs beseitigt. Es ist nach wie vor nicht erkennbar, auf Basis welcher Annahmen der Katalog an Straftaten zustande gekommen ist, der in Summe den **zentralen Begriff des „verfassungsgefährdenden Angriffs“** definiert. Außerdem ist für juristische Laien kaum erschließbar, welche strafrechtlichen Tatbestände in welcher Ausprägung verfassungsgefährdende Angriffe sind und damit in die Zuständigkeit des BVT oder der Landesämter fallen. Beispielsweise ist eine gefährliche Drohung, wenn sie „weltanschaulich motiviert“ ist, ein verfassungsgefährdender Angriff und damit in der Zuständigkeit des BVT.

- § 11 Sanktionengesetz 2010 wurde, im Vergleich zum Begutachtungsentwurf, in den Katalog aufgenommen. Dabei geht es um die **Durchführung völkerrechtlich verpflichtender Sanktionsmaßnahmen** der Vereinten Nationen oder der Europäischen Union. Ein Verfassungsgefährdender Angriff im Sinne des PStSG ist eine getätigte Transaktion oder ein Rechtsgeschäft mit einem den Betrag von € 100.000,-, übersteigenden Wert, nachdem gegen den Betroffenen ein Bescheid oder Sanktionsmaßnahmen erlassen wurden. Diese Bestimmung soll der Terrorismusbekämpfung dienen.

- Desweiteren ist, im Vergleich zum Begutachtungsentwurf, die **erweiterte Gefahrenerforschung** auch **aufgrund von Informationen** von Sicherheitsorganisationen, sowie von **Organen der Europäischen Union oder Vereinten Nationen** möglich. Es wird der Kreis der informationsgebenden Organisationen erweitert. Dadurch wird dem BVT ein größerer Pool an Informationen für ihre Handlungen zu Teil.

- Das Bundesamt und die Landesämter haben die **Verhältnismäßigkeit** in § 9 zu beachten. Damit soll sichergestellt werden, dass die Grundrechte beim Verarbeiten und Übermitteln von personenbezogenen Daten gewahrt werden. Auch sollen die Geheimhaltungsinteressen der Betroffenen bei sensiblen Daten gewahrt werden. Wenngleich diese Klarstellung begrüßt wird, ändert dies substantiell aber nichts, weil aufgrund von § 5 PStSG das Sicherheitspolizeigesetz (SPG) subsidiär Geltung hat und § 29 SPG auch ohne ausdrückliche Wiedergabe anwendbar wäre. Das gleiche gilt für die Vorkehrungen zum Schutz der Geheimhaltungsinteressen, weil sich diese Pflicht unmittelbar aus dem verfassungsgesetzlich verankerten Datenschutzgrundrecht des § 1 DSG ergibt. Insofern ist erstaunlich, dass mit dem neu eingefügten § 9 Abs. 1 PStSG eine (durchaus sinnvolle) Redundanz zur

Normenklarheit in Kauf genommen wird, während bei der zentralen Zweckbestimmung des § 6 PStSG durch verschachtelte Verweise die Norm praktisch unverständlich für alle ist, die nicht den gesamten Straftatenkatalog des StGB im Kopf abrufbar haben.

- **Auskünfte zu Standortdaten** und der eindeutigen **Mobil-Teilnehmerkennung (IMSI)** gemäß § 11 Abs. 1 Z 5 werden ausdrücklich ausgedehnt auf die Überwachung einer „Gruppierung", von Betroffenen im Sinne des § 6 Abs. 1 Z 2 PStSG (= Gefährder) sowie deren Kontakt oder Begleitpersonen. Bemerkenswert ist, dass die ursprüngliche Befugnis in § 53 Abs. 3b SPG nach der Argumentation des Innenministeriums nur geschaffen wurde, um vermisste Wanderer oder Schifahrer zu finden sowie suizidgefährdete Menschen rechtzeitig aufzufinden. Die Aufspürung mutmaßlicher Täter ist bisher nach der Strafprozessordnung (StPO) nur aufgrund eines Gerichtsbeschlusses zulässig. Offenbar wird also die bisherige Rechtfertigung ohne weitere Erklärung dazu aufgegeben und der Polizei sowie den Staatsschutzorganen damit selbst das Instrument in die Hand gelegt, Menschen aktuell und historisch zu lokalisieren und allenfalls Bewegungsprofile daraus zu erstellen.

- **Eingriffe in das Telekommunikationsgeheimnis** durch Auskünfte über Verkehrsdaten, Zugangsdaten und Stammdaten zu elektronischer Kommunikation sowie Auskünfte zu „Diensten der Informationsgesellschaft" (Forum, Website, etc) sind in der geänderten Fassung des § 11 Abs. 1 Z 5 und 7 ebenfalls ausdrücklich auf „Gruppierungen" und Betroffene im Sinne des § 6 Abs. 1 Z 2 PStSG (= Gefährder) ausgedehnt. Damit werden die Möglichkeiten zur Überwachung des Kommunikationsverhaltens noch diffuser. So können die Behörden die Reichweite der Ermittlungsmaßnahmen flexibel steuern, in dem der Kreis der Verdächtigen enger oder weiter definiert wird. Ob ein Eingriff in die verfassungsrechtlich geschützte Privatsphäre eines Betroffenen (Verdächtigen) auch im Einzelfall verhältnismäßig ist, wird nicht mehr überprüft, wenn die Genehmigung des Rechtsschutzbeauftragten insgesamt bezüglich der Gruppierung vorliegt, welcher das Individuum zugeordnet wird. Daran anschließend dehnt Ziffer 5 die Überwachungsbefugnis zu Internetzugangsdaten (IP-Adressen und Anschlussteilnehmer) ausdrücklich auf „Kontakt- und Begleitpersonen" aus, womit der Kreis der Betroffenen gerade im Falle der Beobachtung einer gefährlichen „Gruppierung" in der Praxis stark anwachsen wird.

- Während die Befugnis zur Führung der sehr umfassenden **Datenanwendung** nach dem Begutachtungsentwurf zulässig war zur „Bewertung der Wahrscheinlichkeit eines Angriffs" lautet die Anknüpfung nunmehr **„zur Bewertung von wahrscheinlichen Gefährdungen**". Diese Formulierung erscheint zwar enger als die ursprüngliche, löst aber das eigentliche Problem nicht. Es bestehen weiterhin keine objektivierten Kriterien, woraus die Wahrscheinlichkeit für eine Gefährdung ergibt und wo die Grenze zu ziehen ist. Ein konkreter Verdacht ist an dieser Stelle jedenfalls nicht gefordert.

- Die Beschränkung des Einsatzes von **Kennzeichenerkennungsgeräten** zum automatisierten Abgleich mit KFZ-Kennzeichen für Daten von Betroffene wurde, im Vergleich zum Begutachtungsentwurf, aufgehoben. Stattdessen ist dies jetzt für Gruppierungen, Betroffene, Begleit –und Kontaktpersonen, Informanten und Auskunftspersonen möglich. Auch hier wurden die Befugnisse ausgedehnt, was bedenklich im Hinblick auf die schon vorher mangelnde Verhältnismäßigkeit erscheint.

- Im Begutachtungsentwurf hatten das Bundesamt und die Landesämter die **Daten, wenn sie sechs Monate unverändert geblieben sind, zu prüfen, sie richtigzustellen oder zu löschen**. Nach der Regierungsvorlage müssen die genannten Ämter diese **Daten jährlich prüfen**. Durch die Verdopplung der Prüfungsintervalle werden die Daten länger, gewissermaßen zumindest teilweise auf Vorrat gespeichert. Dies wurde schon im Zuge der Aufhebung der

Vorratsdatenspeicherung durch den österreichischen Verfassungsgerichtshof als verfassungswidrig angesehen.

- Dem **Rechtsschutzbeauftragen** obliegt die **Ermächtigung für Aufgaben zur erweiterten Gefahrenerforschung** und für den **vorbeugenden Schutz vor verfassungsgefährdenden Angriffen**. Diese darf jetzt für höchstens sechs Monate erteilt werden. Neu ist allerdings, dass Verlängerungen zulässig sind. Im Begutachtungsentwurf war nur eine einzige Verlängerung zulässig. Zu bedenken sei hier, ob durch die **zulässige wiederholte Verlängerung** der Zeitraum in der Praxis ausufern könnte.

- Dem **Rechtsschutzbeauftragen** kann nach der Regierungsvorlage im Gegensatz zum Begutachtungsentwurf die Akteneinsicht nur dann verweigert werden, wenn es sich um Auskünfte über die Identität von Personen nach Maßgabe des § 162 StPO handelt. Diese Bestimmung regelt die anonyme Aussage von Zeugen, wenn zu befürchten ist, dass der Zeuge sich oder einen Dritten durch die Bekanntgabe des Namens und anderer Angaben zur Person (Geburtsort, Beruf, Wohnort,…) einer ernsten Gefahr für Leben, Gesundheit, körperliche Unversehrtheit oder Freiheit aussetzen würde. Diese Neuregelung stellt eine Besserung dar, die übrigens nach der Regierungsvorlage nunmehr auch in § 91d SPG nachvollzogen wird. Dennoch ist fragwürdig, warum auch dem Rechtsschutzbeauftragten die Identität „gefährdeten" Zeugen verborgen bleiben soll. Im Vergleich zu einem Gerichtsverfahren bestehen im Kontrollverfahren durch den Rechtsschutzbeauftragten nämlich keine Öffentlichkeit und auch keine Akteneinsicht der Beschuldigten. Sieht man den Rechtsschutzbeauftragten grundsätzlich als vertrauenswürdig, ist der Schutzzweck der Beschränkten Akteneinsicht nicht erkennbar.

- Trotz der begrüßenswerten Änderung, dass die ursprünglich vorgeschlagene, weitgehende Beschränkung der Akteneinsicht nunmehr stark eingeschränkt ist, ist die **Kritik am schwachen Rechtsschutzsystem weiterhin aufrecht zu erhalten**. Um Wiederholungen zu vermeiden wird grundsätzlich auf die Stellungnahme des AKVorrat im Begutachtungsverfahren 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 Innenministerium. An dieser Stelle sei angemerkt, dass beim kürzlich vor der Sommerpause verabschiedeten „Bankenpaket" im Zusammenhang mit **Eingriffen in das Bankgeheimnis neben einer begleitenden Kontrolle durch einen (beim BMF neu geschaffenen) Rechtsschutzbeauftragten eine vollwertige gerichtliche 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.

- Die **Vertrauenspersonenevidenz** wurde, im Vergleich zum Begutachtungsentwurf, gestrichen. Allerdings wurden gleichzeitig die Vertrauenspersonen im Sicherheitspolizeigesetz geregelt. Die Bestimmungen zur Vertrauenspersonenevidenz sind auch für den Aufgabenbereich des Staatsschutzes im (bestehenden) § 54b SPG zu finden. Dort ist schon jetzt ausdrücklich normiert, dass solche Vertrauenspersonen den Sicherheitsbehörden Informationen „gegen Zusage einer Belohnung preisgeben". Trotz der auf den ersten Blick wesentlichen Streichung im PStSG bleibt die schon in der Stellungname zum Begutachtungsentwurf artikulierte Kritik am bezahlten Spitzelwesen unverändert aufrecht.

- Der **offene Einsatz von Bild- und Tonaufzeichnungsgeräten** zur Dokumentation von Amtshandlungen besteht grundsätzlich unverändert, allerdings ist nunmehr „vor Beginn der Aufzeichnung (ist) der Einsatz auf solche Weise anzukündigen, dass er dem Betroffenen bekannt wird“. Somit können die Betroffenen nicht mehr ohne ihr Wissen gefilmt werden. Ergänzt wurde außerdem, dass das Material nur zur Verfolgung von strafbaren Handlungen, die sich während der Amtshandlung ereignet haben, sowie zur Kontrolle der Rechtmäßigkeit der Amtshandlung ausgewertet werden dürfen. Schließlich wurde die Pflicht zur „Protokollierung jedes Zugriffs und Verschlüsselung der Daten“ ergänzt. Insgesamt ist damit der Grundrechtseingriff wohl auf ein verhältnismäßiges Maß reduziert.
- Das PStSG sollt erst mit 01. Juli 2016 in Kraft treten und nicht, wie im Begutachtungsentwurf vorgesehen, am 19. Jänner 2016. Durch den Einsatz des AK Vorrat wurde also zumindest ein halbes Jahr Zeit für weitere Diskussionen im parlamentarischen Prozess „gewonnen“.

II. Zu den einzelnen Bestimmungen

Nachfolgend werden die einzelnen Bestimmungen gemäß der Regierungsvorlage (Ministerratsvortrag) wiedergegeben, wobei die Änderungen gegenüber dem Begutachtungsentwurf kenntlich gemacht sind. Zu jeder Bestimmung erfolgt eine kurze Beschreibung, welche Änderungen inwiefern von substantieller Bedeutung sind.

§ 1: Anwendungsbereich; Polizeilicher Staatsschutz

(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, weltanschaulich 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. ~~Hiezu~~

(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 als Organisationseinheit der

~~Landespolizeidirektion~~Landespolizeidirektionen in jedem Bundesland ein Landesamt Verfassungsschutz (Landesamt).

~~(3) Das Bundesamt wird bei Vollziehung dieses Bundesgesetzes für den Bundesminister für Inneres, das Landesamt für die Landespolizeidirektion tätig.~~(4) Der Bundesminister für Inneres kann bestimmte Angelegenheiten nach Abs. 2 dem Bundesamt vorbehalten. Diesfalls kann das Bundesamt die Landesämter mit der Durchführung einzelner Maßnahmen beauftragen. Auch kann es anordnen, dass ihm das Landesamt direkt über den Fortgang einer Angelegenheit laufend oder zu bestimmten Zeitpunkten zu berichten hat.

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

Kommentar:

Keine substanziellen Änderungen mit grundrechtlicher Relevanz. Im Vergleich zwischen Begutachtungsentwurf und Regierungsvorlage wurden die Absätze 4 und 5 eingefügt. Dabei wurde der Delegationszusammenhang von Absatz 3 in den neuen Absatz 5 transferiert. Substantiell neu ist die ausdrückliche Koordinierungskompetenz des BVT.

§ 2: Organisation

(1) Dem Bundesamt steht ein Direktor vor. ~~Dem~~Der Direktor ~~kommt~~nimmt die Funktion als Informationssicherheitsbeauftragter für den Wirkungsbereich des ~~Informationssicherheitsbeauftragten~~Bundesministeriums für Inneres nach ~~dem Informationssicherheitsgesetz zu~~§ 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 ~~und mindestens fünf Jahre in einem Beruf tätig gewesen ist, in dem der Abschluss des Studiums der Rechtswissenschaften Berufsvoraussetzung ist~~.

(3) Sonstige Bedienstete des Bundesamtes und der Landesämter 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 ~~den~~ Bediensteten in Leitungsfunktionen nicht bereits um Organe des öffentlichen Sicherheitsdienstes handelt, ~~kann der Generaldirektor für die öffentliche Sicherheit~~können sie nach

erfolgreicher Absolvierung der Ausbildung (Abs. 3) zur Ausübung ~~von~~unmittelbarer Befehls- und Zwangsgewalt ~~ermächtigen~~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 ~~Sicherheitspolizeigesetz - SPG, BGBl. Nr. 566/1991~~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:

Im Gegensatz zum Begutachtungsentwurf ist es für die Position des Direktors nicht mehr erforderlich, eine 5-jährige Berufserfahrung in einem Juristischen Beruf vorzuweisen. Es genügt ein Abschluss eines Studiums der Rechtswissenschaften. Diese Änderung ist bemerkenswert, da die Position des Direktors mit einer hohen Verantwortung einher geht und, wie auch in § 3 ersichtlich, gestärkt wird. Verständlich ist wohl, dass Praxiserfahrung in einem Beruf, für den das Studium der Rechtswissenschaften eine Voraussetzung ist, möglicherweise nicht die optimale Bedingung für dieses Amt wäre, weil in den meisten Berufen im Bereich der inneren Sicherheit ein juristisches Studium zumindest keine formale Voraussetzung ist, anders als etwa bei Rechtsanwälten, Notaren oder Richtern. Eine ersatzlose Streichung der praktischen Qualifikationsvoraussetzungen ist hier aber der falsche Ansatz.

§ 3: Geschäftsordnung des Bundesamtes

Der Direktor des Bundesamtes hat ~~im Einvernehmen mit dem Generaldirektor für die öffentliche Sicherheit~~ 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:

Die Geschäftsordnung muss nicht mehr, wie noch im Begutachtungsentwurf vorgeschlagen, im Einvernehmen mit dem Generaldirektor für öffentliche Sicherheit festgelegt werden. Vor Erlassung und vor jeder Änderung der Geschäftsordnung ist der Generaldirektor für die öffentliche Sicherheit zu befassen. Hierdurch wird die Position des Direktors des Bundesamtes gestärkt, während die Stellung des Generaldirektors für die öffentliche Sicherheit geschwächt wird. Die praktischen Konsequenzen dieser Änderung werden aber nicht allzu groß sein, dennoch sollte insofern auf die Qualifikationsvoraussetzungen des Direktors des BVT besonderes Augenmerk gelegt werden.

§ 4: Bundesamt als Zentralstelle

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 ~~Strafgesetzbuch (StGB), BGBl. Nr. 60/1974~~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 ~~Zentralstellen des Bundesministeriums~~vom Bundesministerium für Inneres genutzten Gebäude;

5. die internationale Zusammenarbeit auf dem Gebiet des Staatsschutzes; davon unberührt bleibt die Zusammenarbeit der Landesämter mit benachbarten regionalen Sicherheitsdienststellen.

Kommentar:

Es kam zu mehreren nicht substanziellen Veränderungen. Beispielhaft sei die Z 1 zu nennen. Hier wurde „(§ 74 Abs. 1 Z 8 Strafgesetzbuch StGB, BGBl. Nr. 60/1974)“ eingefügt.

§ 5: Anwendbarkeit des Sicherheitspolizeigesetzes

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

Kommentar:

Keine Änderungen

§ 6: Erweiterte Gefahrenerforschung und Schutz vor verfassungsgefährdenden Angriffen

(1) Dem Bundesamt und den Landesämtern 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 weltanschaulich oder religiös motivierter Gewalt kommt;

2. der vorbeugende Schutz vor ~~wahrscheinlichen~~ 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 ~~oder ausländischer~~, 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~~, 278c~~ bis 278f oder, soweit es der Verfügungsmacht einer terroristischen Vereinigung unterliegende Vermögensbestandteile betrifft, nach § 165 Abs. 3 StGB strafbaren Handlung;

2. durch die ~~weltanschaulich oder religiös motivierte~~ rechtswidrige Verwirklichung des Tatbestandes einer nach §§ 274 Abs. 2 erster Fall, 279, 280, 282, 283 oder in § 278c StGB genannten strafbaren Handlung, sofern diese weltanschaulich oder religiös motiviert ist;

3. durch die rechtswidrige Verwirklichung des Tatbestandes einer nach ~~§§ 274, 284 und 285 StGB, nach~~ dem vierzehnten ~~bis sechzehnten~~oder fünfzehnten Abschnitt des StGB oder nach dem ~~Verbotsgesetz~~VerbotsG strafbaren Handlung;

4. durch die rechtswidrige Verwirklichung des Tatbestandes einer nach §§ 175, 177a, 177b StGB, §§ 79 bis 82 Außenwirtschaftsgesetz 2011 ~~(~~ AußWG 2011~~),~~ BGBl. I Nr. 112/2011, § 7 Kriegsmaterialgesetz ~~(~~ KMG~~),~~ BGBl. Nr. 540/1977, ~~sowie nach~~ § 11 Sanktionengesetz 2010 - SanktG, BGBl. I Nr. 36/2010, nach §§ 124, 316, 319 ~~und~~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 ~~und~~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).

Kommentar:

Zu § 6 Abs. 1 Z 2:

Der Begriff **„wahrscheinlicher"** verfassungsgefährdender Angriff wurde in Abs 1 Z 2 durch den „begründeten Gefahrenverdacht“ gem § 22 Abs 2 SPG ersetzt. Zwar normiert auch § 22 Abs. 2 SPG gefährlichen Angriffen auf Leben, Gesundheit, Freiheit, Sittlichkeit, Vermögen oder Umwelt vorzubeugen haben, „sofern solche Angriffe wahrscheinlich sind". Allerdings ist die ausdrückliche Voraussetzung, dass ein „begründeter Gefahrenverdacht“ vorliegen muss, dazu jedenfalls eine substantielle Verbesserung. Hierzu wäre jedoch zu wünschen, dass es klare Regeln gibt, wo und wie die Begründung für das Vorliegen eines konkreten Gefahrenverdachts schriftlich festzuhalten und vorzulegen ist. Die Begründungspflicht ist nur effektiv, wenn sie auch prozessual abgesichert ist.

Zu § 6 Abs. 1 Z 3:

Nunmehr soll nach der Regierungsvorlage gemäß Abs 1 Z 3 die erweiterte Gefahrenerforschung auch aufgrund von Informationen von Sicherheitsorganisationen (§ 2 Abs. 2 und 3 Polizeikooperationsgesetz – PolKG, BGBl. I Nr. 104/1997) sowie von Organen der Europäischen Union oder Vereinten Nationen möglich sein. Hier wurde der Kreis der informationsgebenden Organisationen ausgedehnt und internationalisiert. Dies ist grundsätzlich nachvollziehbar, jedoch darf eine Verdachtsmeldung aus dem Ausland nicht dazu führen, dass das nun neu vorgeschlagene Kriterium eines „begründeten“ Verdachts umgangen wird. Daher sollte auch bei solchen Meldungen

von ausländischen Organisationen ein „begründeter“ Verdacht als Voraussetzung für die Aktivierung der Befugnisse sowie eine klare Dokumentationspflicht normiert werden.

Zu § 6 Abs. 2 Z 2:

Die Tatbestände „Sprengung einer Versammlung“ und „Störung einer Versammlung“ gem § 284 und 285 StGB wurden aus dem Tatbestandskatalog des PStSG entfernt. Auch wurde der Tatbestand des § 274 (Landfriedensbruch) dahingehend beschränkt, dass nur mehr die führende Teilnahme an einer Zusammenrottung von Menschen nach dem PStSG verfolgbar ist.

§ 11 Sanktionengesetz 2010 SanktG, BGBl. I Nr. 36/2010 wurde in den Katalog aufgenommen. Das Sanktionengesetz ist die innerstaatliche Rechtsgrundlage zur Umsetzung von Sanktionen, die auf völkerrechtlicher Ebene beschlossen wurden. Dies geschieht nach den Erläuterungen zum SanktG[1] im Wesentlichen durch die Schaffung innerstaatlicher Umsetzungsmaßnahmen zur Durchführung völkerrechtlich verpflichtender Sanktionsmaßnahmen der Vereinten Nationen und/oder der Europäischen Union (unabhängig davon, ob es sich um Maßnahmen der Europäischen Union zur Umsetzung von Sanktionen der Vereinten Nationen oder „autonome“ Sanktionen der Europäischen Union handelt). Im Fokus dieses Gesetzes stehen dabei vor allem die Bekämpfung von Terrorismus und Geldwäsche. § 11 SanktG konkret sanktioniert eine getätigte Transaktion oder ein Rechtsgeschäft mit einem den Betrag von € 100.000,- übersteigendem Wert mit Freiheitsstrafe, nachdem gegen den Betroffenen ein Bescheid oder Sanktionsmaßnahmen erlassen wurden.

Bewertung:

Die Änderungen zu § 6 PStSG zeigen zumindest, dass die im Begutachtungsverfahren von verschiedensten Stellen massiv geäußerte Kritik am Konzept des „verfassungsgefährdenden Angriffs“ nicht völlig ungehört blieb. Positiv ist die neue Voraussetzung eines „begründeten Gefahrenverdachts“, ebenso die Herausnahme der Tatbestände „Sprengung einer Versammlung“ und „Störung einer Versammlung“ gemäß §§ 284 und 285 StGB. Allerdings wurde damit nur „die Spitze des Eisbergs“ gekappt und das grundsätzliche Problem keineswegs beseitigt. Wie bereits in der Stellungnahme zum Begutachtungsentwurf ausgeführt, ist nach wie vor nicht erkennbar, auf Basis

1 Siehe die Gesetzesmaterialien https://www.ris.bka.gv.at/Dokumente/RegV/REGV_COO_2026_100_2_590998/COO_2026_100_2_593510.pdf.

welcher Annahmen der Katalog an Straftaten zustande gekommen ist, der in Summe den zentralen Begriff des „verfassungsgefährdenden Angriffs“ definiert. Außerdem ist für juristische Laien nach wie vor schwer erschließbar, welche strafrechtlichen Tatbestände in welcher Ausprägung verfassungsgefährdende Angriffe sind und damit in die Zuständigkeit des BVT oder der Landesämter fallen.

Besonders schwierig bleiben die Abgrenzungsschwierigkeiten bei der „verschachtelten“ Verweistechnik in § 6 Abs. 2 Z 2 PStSG, der die „in § 278c StGB genannten strafbaren Handlung“ in den Katalog aufnimmt. Damit sind unter anderem Delikte wie Körperverletzung, gefährliche Drohung oder Datenbeschädigung als „verfassungsgefährdender Angriff“ zu qualifizieren, sofern sie religiös oder weltanschaulich motiviert sind. Nach so einer Rechtslage müsste die Polizei erkennen können, wann etwa eine gefährliche Drohung weltanschaulich motiviert ist, weil in diesem Falle der Staatsschutz zuständige wäre. Durch die unveränderte Formulierung der „in § 278c StGB genannten strafbaren Handlungen“ werden nämlich die dort aufgezählten Straftatbestände unabhängig davon erfasst, ob die Straftat in einem terroristischen Zusammenhang begangen wird, wie § 278c StGB für sich genommen ansonsten voraussetzt. Welchen Unterschied diese Formulierung macht, können Menschen ohne spezifische juristische Ausbildung kaum erkennen. Die Adressaten der Norm sind aber nicht nur die Beamte, die zu deren Vollzug berufen sind, sondern auch alle Personen, in deren Grundrechte durch die Norm potentiell eingegriffen wird.

Im Urteil zur Aufhebung der Vorratsdatenspeicherung ist der Verfassungsgerichtshof eben diesem Argument gefolgt, weil der Individualantrag ansonsten unzulässig gewesen wäre. Daher muss die Norm nicht nur für speziell geschulte Beamte sondern auch für juristisch durchschnittlich verständige Menschen im Wesentlichen verständlich sein. Diese auch vom Europäischen Gerichtshof für Menschenrechte in ständiger Rechtsprechung geforderte Normenklarheit besteht auch in der Regierungsvorlage weiterhin nicht. Die Gestaltung des „verfassungsgefährdenden Angriffs“ nach § 6 PStSG in der Fassung der Regierungsvorlage begegnet weiterhin nicht der Forderung nach einer faktenbasierten Sicherheitspolitik, solange der Gesetzgeber nicht zu erklären vermag, aufgrund welcher Entwicklung welche der neu vorgeschlagenen Befugnisse notwendig geworden sind.

Darüber hinaus wurden in § 6 einige rein formale Änderungen ohne substantielle Bedeutung vorgeschlagen, die hier nicht näher kommentiert werden.

§ 7: Polizeilich staatsschutzrelevante Beratung

~~(1)~~ Dem Bundesamt und den Landesämtern obliegt 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.

~~(2) Darüber hinaus obliegt es dem Bundesamt und den Landesämtern, Vorhaben, die der Vorbeugung verfassungsgefährdender Angriffe dienen, zu fördern.~~

Kommentar:

Gegenüber dem Begutachtungsentwurf wurde der gesamte ursprünglich vorgeschlagene Absatz 2 entfernt, der lautete: „(2) Darüber hinaus obliegt es dem Bundesamt und den Landesämtern, Vorhaben, die der Vorbeugung verfassungsgefährdender Angriffe dienen, zu fördern." Die Erläuterungen zur Regierungsvorlage enthalten allerdings noch immer die Ausführungen zu dieser ursprünglich vorgeschlagenen, sehr dehnbaren Bestimmung: „Vorhaben, die von Schulen sowie anderen öffentlichen oder privaten Einrichtungen im Bereich der Prävention vor verfassungsgefährdenden Angriffen unternommen werden, sollen vom Bundesamt und den Landesämtern im Rahmen ihrer personellen und finanziellen Möglichkeiten gefördert werden können. Daraus ist allerdings kein Rechtsanspruch auf Förderung ableitbar." Die gestrichene Bestimmung sowie die verbliebene Erläuterung dazu lassen völlig unklar, welche Art von „Vorhaben" hier gefördert werden sollen. Da aus der Regierungsvorlage auch nicht ersichtlich ist, mit welcher Begründung der ursprüngliche Normentext dazu gestrichen wurde, ist schwer einzuschätzen, ob auch die Absicht dahinter ersatzlos fallen gelassen oder eine solche Kompetenz nur anders begründet werden soll. Eine Klarstellung dazu im parlamentarischen Ausschuss wäre wünschenswert.

§ 8: Information verfassungsmäßiger Einrichtungen

(1) Dem Bundesamt und den Landesämtern obliegen zur Information verfassungsmäßiger Einrichtungen die Analyse und Beurteilung von staatsschutzrelevanten Bedrohungslagen, die sich auch aus verfassungsgefährdenden Entwicklungen im Ausland ergeben können, sofern nicht der Vollziehungsbereich des Bundesministers für Landesverteidigung und Sport betroffen ist.

(2) Der Bundesminister für Inneres hat über staatsschutzrelevante Bedrohungen den Bundespräsidenten, die Präsidenten des Nationalrates, den Vorsitzenden und die stellvertretenden Vorsitzenden des Bundesrates sowie die anderen Mitglieder der Bundesregierung zu unterrichten,

~~soweit dies~~die für die Wahrnehmung der gesetzlichen Aufgaben in deren Zuständigkeitsbereich ~~oder~~von Bedeutung sind. Ebenso hat der Bundesminister für Inneres die Genannten über Umstände zu unterrichten, die für die Wahrung des Ansehens des Bundespräsidenten, des Nationalrates, des Bundesrates oder der Bundesregierung von Bedeutung ~~ist~~sind.

(3) Der Landespolizeidirektor hat über staatsschutzrelevante Bedrohungen den Landeshauptmann und die Präsidenten des Landtages zu unterrichten, ~~soweit dies~~die für die Wahrnehmung der gesetzlichen Aufgaben in deren Zuständigkeitsbereich ~~oder~~ von Bedeutung sind. Ebenso hat der Landespolizeidirektor die Genannten über Umstände zu unterrichten, die für die Wahrung des Ansehens des ~~Landeshauptmannes,~~Landtages oder der Landesregierung ~~oder des Landtages~~ von Bedeutung ~~ist~~sind.

Kommentar:

Keine substanziellen Änderungen. Für letztlich rein formale Änderungen beispielhaft sei die Streichung des Landeshauptmannes in Z 3 genannt. Diese Änderung hat letztlich keine substantielle Auswirkung, da der Landeshauptmann ein Teil der Landesregierung ist, deren Ansehen zu wahren Aufgabe des Staatsschutzes ist, und damit auch ohne ausdrückliche Aufzählung erfasst ist.

Verwenden personenbezogener Daten auf dem Gebiet des polizeilichen Staatsschutzes

§ 9: Allgemeines

(1) Das Bundesamt und die Landesämter 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.

(2) Personenbezogene Daten dürfen vom Bundesamt und den Landesämtern gemäß diesem Hauptstück nur verwendet werden, soweit dies zur Erfüllung der ihnen übertragenen Aufgaben erforderlich ist. Ermächtigungen nach anderen Bundesgesetzen bleiben unberührt.

Kommentar:

Neu eingefügt wurde hier Z 1. Das Bundesamt und die Landesämter haben die Verhältnismäßigkeit zu beachten. Damit soll sichergestellt werden, dass die Grundrechte beim Verarbeiten und Übermitteln von personenbezogenen Daten gewahrt werden. Auch sollen die Geheimhaltungsinteressen der Betroffenen bei sensiblen Daten gewahrt werden.

Es ist begrüßenswert, dass der zentrale rechtsstaatliche Grundsatz der Verhältnismäßigkeit auch im PStSG ausdrücklich verankert wird, ebenso das Erfordernis, angemessene Vorkehrungen zur Wahrung der Geheimhaltungsinteressen der Betroffenen zu treffen. Dies ist nützlich für die Klarheit, weil die Rechtsanwender beim Vollzug des PStSG diese wichtigen Grundsätze sofort erkennen können, ohne in anderen Rechtsvorschriften wie dem Datenschutzgesetz oder dem Sicherheitspolizeigesetz nachsehen zu müssen. Substantiell ändert dies aber nichts, weil aufgrund von § 5 PStSG das SPG subsidiär Geltung hat und § 29 SPG auch ohne ausdrückliche Wiedergabe anwendbar wäre. Das gleiche gilt für die Vorkehrungen zum Schutz der Geheimhaltungsinteressen, weil sich diese Pflicht unmittelbar aus dem verfassungsgesetzlich verankerten Datenschutzgrundrecht des § 1 DSG ergibt.

Insofern ist erstaunlich, dass mit dem neu eingefügten § 9 Abs. 1 PStSG eine (durchaus sinnvolle) Redundanz zur Normenklarheit in Kauf genommen wird, während bei der zentralen Zweckbestimmung des § 6 PStSG durch verschachtelte Verweise die Norm praktisch unverständlich für alle ist, die nicht den gesamten Straftatenkatalog des StGB im Kopf abrufbar haben.

§10: Ermittlungsdienst für Zwecke des polizeilichen Staatsschutzes

(1) Das Bundesamt und die Landesämter dürfen personenbezogene Daten ermitteln und weiterverarbeiten für

1. *die erweiterte Gefahrenerforschung (§ 6 Abs. 1 Z 1~~);~~),*
2. *den vorbeugenden Schutz vor ~~wahrscheinlichen~~ verfassungsgefährdenden Angriffen (§ 6 Abs. 1 Z 2~~);~~),*
3. *den Schutz vor verfassungsgefährdenden Angriffen aufgrund von Informationen von Dienststellen inländischer Behörden ~~oder ausländischer~~, 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) Das Bundesamt und die Landesämter 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 Strafprozessordnung (- StPO), BGBl. Nr. 631/1975, ist davon nicht umfasst. Bestehende Übermittlungsverbote bleiben unberührt.

(3) Das Bundesamt und die Landesämter 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) Das Bundesamt und die Landesämter 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 § 12 11 sind das Bundesamt und die Landesämter 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:

In Anlehnung an § 6 wurde in Abs 1 der Begriff „wahrscheinlich“ bei verfassungsgefährdenden Angriffen gestrichen. Desweiteren wurde der Kreis der informationsgebenden Organisationen erweitert. Außerdem wurde in Absatz 1 am Ende eine ausdrückliche gesetzliche Befugnis zur Verarbeitung „sensibler Daten“ ergänzt, damit auch „Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder

philosophische Überzeugung, Gesundheit oder ihr Sexualleben“ (§ 4 Z 2 DSG) verarbeitet werden dürfen, soweit „diese für die Erfüllung der Aufgabe unbedingt erforderlich sind“. Damit soll die Verarbeitung sensibler Daten auf Basis einer besonderen gesetzlichen Ermächtigung im Sinne des § 9 Z 3 DSG gerechtfertigt sein.

In Abs 2 wurde ergänzt, dass nur solche Daten weiterverarbeitet werden dürfen, welche durch das Bundesamt oder die Landesämter „rechtmäßig“ verarbeitet werden. Hier wird interessant sein, ob diese Einschränkung als Verwertungsverbot für rechtswidrig erlangtes, datenmäßig erfasstes Beweismaterial verstanden wird.

Open Source Intelligence (OSINT)

Wie schon nach dem Begutachtungsentwurf sollen gemäß Absatz 5 das Bundesamt und die Landesämter berechtigt sein, für die in Absatz 1 aufgelisteten Zwecke „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“. Ergänzt wurde hierzu der knappe Verweis, dass „Abs. 2 zweiter Satz gilt“. Dies bezieht sich auf den Satz „Ein automationsunterstützter Datenabgleich im Sinne des § 141 Strafprozessordnung StPO, BGBl. Nr. 631/1975, ist davon nicht umfasst.“

Damit wurde eine Rechtsgrundlage geschaffen, um alle, insbesondere im Internet öffentlich verfügbaren Quellen, für Ermittlungen heranziehen und die gewonnenen Daten und Informationen systematisch weiterverarbeiten zu dürfen. Gleichzeitig wird der „automationsunterstützte Datenabgleich im Sinne des § 141 Strafprozessordnung, im politischen Diskurs auch als „Rasterfahndung“ bezeichnet, ausgeschlossen. Wie schon in der Stellungnahme zum Begutachtungsentwurf beschrieben bestehen hier Abgrenzungsschwierigkeiten, weil angesichts der heutigen technischen Möglichkeiten bei weitem nicht hinreichend präzise definiert ist, was genau unter einem „automationsunterstützten Datenabgleich“ zu verstehen ist. Die aus den späten 1990er Jahren stammenden Definitionen erfassen kaum, was die technischen Möglichkeiten zur „Rasterfahndung“ heutzutage bieten. Vereinfacht gesagt kann die Suchmaschine „Google“ heute weit mehr leisten, als alle Ende der 90er Jahre bekannten Instrumente der „Rasterfahndung“.

Unabhängig von einer weiteren automatisierten Verknüpfung ist die Frage zu stellen, wie die Methoden zur Sammlung von personenbezogenen Daten aus allen öffentlich verfügbaren Quellen zur Erfüllung der Aufgaben des Staatsschutzes aussehen sollen. § 10 Abs. 5 PStSG nennt dazu nur den „Einsatz geeigneter Mittel“ ohne weitere Präzisierung oder Schranken. Im einfachsten Fall erfolgt die

Suche „im Internet“ durch Menschen unter Einsatz allgemein verfügbarer Hilfsinstrumente wie Suchmaschinen web 2.0 Anwendungen (zB Youtube, Facebook, Twitter, etc.). Allerdings ist diese Methode tendenziell sehr ressourcen- und zeitaufwändig. Aus diesem Grund hat die technische Entwicklung der letzten Jahre eine große Zahl sogenannter „Open Source Intelligence“ (kurz OSINT) Instrumente hervorgebracht. Dabei handelt es sich um speziell für Ermittlungen im Sicherheitsbereich angefertigte Programme, im Wesentlichen spezialisierte Suchmaschinen, die automatisiert nach bestimmten Filtern, die vom Anwender konkretisiert werden, alle im Internet verfügbaren Quellen absuchen. Auf diese Weise wird die Ermittlungsarbeit, die sonst durch menschliche Intelligenz gesteuert wird, durch komplexe Algorithmen an die Maschine ausgelagert. So kann die Maschine selbständig eine beachtliche Datensammlung erzeugen, die in einem weiteren Schritt von menschlichen Ermittlern auf ihre Relevanz geprüft und genutzt wird. Diese ursprünglich vor allem für Geheimdienste entwickelten Instrumente drängen international immer mehr in den Bereich der polizeilichen Gefahrenabwehr. Es besteht bereits ein großer und ständig wachsender Markt an Anbietern und Produkten für OSINT Tools, darunter auch österreichische Unternehmen. Beispielhaft genannt seien hier Sail Labs Technology, Wien (http://www.arax.at/venture_capital/unternehmen_a_z_/sail_labs/), , Recorded Future, Boston (https://www.recordedfuture.com/blog/), BLAB, Seattle (http://www.blabpredicts.com/), Brandwatch GmbH, Berlin (https://www.brandwatch.com/de/) oder Echosec (https://www.echosec.net/). Außerdem wird an diesem Thema auch mit öffentlichen Mitteln geforscht, wie etwa das von der EU geförderte Forschungsprojekt VIRTUOSO zeigt (http://www.virtuoso.eu/).

Zugleich greift hier zum Teil das bestehende österreichische Datenschutzrecht zu kurz. Das liegt in erster Linie daran, dass das Datenschutzgrundrecht des § 1 DSG das Bestehen schutzwürdiger Geheimhaltungsinteressen ausschließt, „wenn Daten infolge ihrer allgemeinen Verfügbarkeit (…) einem Geheimhaltungsanspruch nicht zugänglich sind“. Damit ist auf eine automatisierte Sammlung öffentlich bereits verfügbarer Daten auf den ersten Blick das Datenschutzrecht nicht einmal anwendbar, weshalb damit zu rechnen ist, dass auch die Datenschutzbehörde keine Vorabkontrollpflicht annehmen würde, wenn es um die Anschaffung eines OSINT Instruments durch das Innenministerium geht. Zu bedenken ist hier, dass die moderne Judikatur des Gerichtshofs der Europäischen Union (EuGH) etwas differenzierter ist. Die Leitentscheidung hierzu ist „Google Spain“[2]. In der Sache stellt er EuGH zum Umfang der Verantwortlichkeit des Suchmaschinenbetreibers fest, dass dieser unter bestimmten Voraussetzungen verpflichtet ist, von der Ergebnisliste, die im

2 Urteil des EuGH (Große Kammer) vom 13. Mai 2014 in der Rechtssache C-131/12, Google Spain SL und Google Inc. gegen Agencia Española de Protección de Datos (AEPD) und Mario Costeja González.

Anschluss an eine anhand des Namens einer Person durchgeführte Suche angezeigt wird, Links zu von Dritten veröffentlichten Internetseiten mit Informationen über diese Person zu entfernen. Eine solche Verpflichtung kann auch bestehen, wenn der betreffende Name oder die betreffenden Informationen auf diesen Internetseiten nicht vorher oder gleichzeitig gelöscht werden, gegebenenfalls auch dann, wenn ihre Veröffentlichung dort als solche rechtmäßig ist.[3] Die Entscheidung macht jedenfalls klar, dass es unionsrechtlich nicht haltbar ist, dass einem Datum von vornherein jede weitere Schutzwürdigkeit abgesprochen wird, sobald es einmal veröffentlicht wurde. In dieser Hinsicht hat auch bereits der Europäische Gerichtshof für Menschenrechte klargestellt, dass Art 8 EMRK (Recht auf Privatleben) auch beinhaltet, sich grundsätzlich auch in der Öffentlichkeit frei von systematischer staatlicher Beobachtung zu bewegen (vgl. zB EGMR 4.5.2000, Rotaru gg Rumänien, BeswNr. 28341/95).

Auch wenn derzeit nach offiziellen Angaben des Innenministeriums keine OSINT Tools im Einsatz sind, ist vor diesem Hintergrund schwer vorstellbar, dass die Staatsschutzorgane in Österreich in den kommenden Jahren vollkommen darauf verzichten wollen, solche Möglichkeiten zu nutzen. Aus diesem Grund fordert der AKVorrat, den „Einsatz geeigneter Mittel“ (Absatz 5) konkreter zu determinieren und Begleitmaßnahmen zu etablieren, um den spezifischen grundrechtlichen Risiken zu begegnen, die mit OSINT einhergehen. Immerhin wird mit solchen Instrumenten ein wichtiger Teil der Ermittlungsarbeit den Algorithmen anvertraut, die von privaten Unternehmen gestaltet und umgesetzt werden. Wer von einer OSINT Maschine nach bestimmten Kriterien als ermittlungsrelevant identifiziert wird, muss nämlich mit weitergehenden Ermittlungen und Grundrechtseingriffen rechnen. Welche Grenzen und Sicherungsmechanismen hier zu beachten sind, sollte durch den demokratisch legitimierten Gesetzgeber vorgezeichnet werden. An dieser Stelle sei auch an die Grenzen erinnert, die § 49 DSG für „Automatisierte Einzelentscheidungen“ aufstellt.

§ 11: Besondere Bestimmungen für die Ermittlungen

(1) Zur erweiterten Gefahrenerforschung (§ 6 Abs. 1 Z 1) und zum vorbeugenden Schutz vor ~~wahrscheinlichen~~ verfassungsgefährdenden Angriffen (§ 6 Abs. 1 Z 2) ist die Ermittlung personenbezogener Daten nach Maßgabe des § 9 und unter den Voraussetzungen des § ~~15~~14 zulässig durch

3 Vgl. die Zusammenfassung in der Presseaussendung des EuGH, http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070de.pdf, zuletzt abgerufen am 14.8.2014.

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 ~~zu Betroffenen~~ nach § ~~11~~12 Abs. 1 ~~Z 1 lit. l~~ verarbeitet werden;~~-~~

5. Einholen von Auskünften nach §§ 53 Abs. 3a Z 1 bis 3 und 53 Abs. 3b SPG zu ~~Betroffenen~~ einer ~~Aufgabe~~Gruppierung nach § 6 Abs. 1 Z 1 ~~und Z~~ oder einem Betroffenen nach § 6 Abs. 1 Z 2 sowie zu deren Kontakt- oder Begleitpersonen (§ ~~11~~12 Abs. 1 Z ~~3~~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 ~~von Beförderungsunternehmen~~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 ~~Betroffenen~~ einer ~~Aufgabe~~Gruppierung nach § 6 Abs. 1 Z 1 ~~und~~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. ~~Im Übrigen ist die~~

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.

Kommentar:

Bei § 11 handelt es sich um den ehemaligen § 12 nach dem Begutachtungsentwurf. Die beiden Paragraphen tauschten ihren Platz.

In Absatz 1 wird neu auf die Maßgabe nach § 9 verwiesen, welche die Beachtung der Verhältnismäßigkeit ausdrücklich vorschreibt. Wie schon zu § 9 kommentiert, ist dieser Hinweis zur Klarstellung begrüßenswert aber substantiell eigentlich redundant.

Die Beschränkung des Einsatzes von Kennzeichenerkennungsgeräten (§ 54 Abs. 4b SPG) zum automatisierten Abgleich mit KFZ-Kennzeichen (§ 11 Abs 1 Z 4) für Daten von Betroffenen wurde, im Vergleich zum Begutachtungsentwurf, aufgehoben. Stattdessen ist dies jetzt für Gruppierungen, Betroffene, Begleit –und Kontaktpersonen, Informanten und Auskunftspersonen möglich. Die Reichweite dieser Befugnis wurde somit deutlich weiter gesteckt.

Die Befugnis nach § 11 Abs 1 Z 5 für die Auskunft über IP-Adressen und die zugehörigen Anschlussinhaber sowie die aktuelle und historische Standortdatenerfassung erfährt in der neuen Fassung der Regierungsvorlage eine wichtige ausdrückliche Ausdehnung. Die IP-Adressen Auskünfte, das heißt die Zugangsdaten zu einem Internetanschluss, dürfen von den Staatsschutzorganen nicht nur für Ermittlungen gegen bestimmte Personen sondern auch gegen Gruppierungen gefordert werden. Gleichzeitig muss auch der Rechtsschutzbeauftragte die Maßnahme nur abstrakt für 6 Monate im Voraus für die Beobachtung einer gefährlichen „Gruppierung“ genehmigen. Hier können die Behörden also die Reichweite der Ermittlungsmaßnahmen sehr flexibel steuern, in dem der Kreis der Verdächtigen enger oder weiter definiert wird. Ob ein Eingriff in die verfassungsrechtlich geschützte Privatsphäre eines Betroffenen (Verdächtigen) auch im Einzelfall verhältnismäßig ist, wird nicht mehr überprüft, wenn die Genehmigung insgesamt bezüglich der Gruppierung vorliegt, welcher das Individuum zugeordnet wird. Daran anschließend dehnt Ziffer 5 die Überwachungsbefugnis ausdrücklich auf „Kontakt- und Begleitpersonen“ aus, womit der Kreis der Betroffenen gerade im Falle der Beobachtung einer gefährlichen „Gruppierung“ in der Praxis stark anwachsen wird.

In Bezug auf Standortdaten zu einem mobilen Endgerät wird der Kreis der potentiell Betroffenen sowohl im SPG als auch – durch die Änderung mit der Regierungsvorlage ausdrücklich – im PStSG ausgedehnt. Nach der derzeit geltenden Rechtslage dürfen die Sicherheitsbehörden gemäß § 53 Abs. 3b SPG „Auskunft über Standortdaten und die internationale Mobilteilnehmerkennung (IMSI) der von dem gefährdeten oder diesen begleitenden Menschen mitgeführten Endeinrichtung zu verlangen sowie technische Mittel zur Lokalisierung der Endeinrichtung zum Einsatz zu bringen.“ Der letzte Halbsatz ist die abstrakte Ermächtigung zum Einsatz von sog. „IMSI-Catchern“. Nun erfolgt im SPG (siehe unten zu den SPG Änderungen Z 9) die Erweiterung, dass diese Befugnis auch auf den „Gefährder“ ausgedehnt wird. Das PStSG geht noch einen deutlichen Schritt weiter, weil nach dem Wortlaut des § 11 Abs. 1 Z 5 die Auskünfte zu Standortdaten und IMSI zulässig zur Überwachung einer „Gruppierung“, von Betroffenen im Sinne des § 6 Abs. 1 Z 2 PStSG (= Gefährder) sowie deren Kontakt oder Begleitpersonen sind. Diese Ausdehnung ist schon deshalb bemerkenswert, weil seit der Schaffung der ursprünglichen Befugnis in § 53 Abs. 3b SPG durch die SPG Novelle 2007 in der öffentlichen Debatte seitens des Innenministeriums stets prominent argumentiert wurde, dass diese Befugnis eigentlich nur geschaffen wurde, um vermisste Wanderer oder Schifahrer zu finden oder suizidgefährdete Menschen rechtzeitig aufzufinden. Für die Prävention oder Aufklärung von Straftaten wurde stets darauf verwiesen, dass Standortdatenauskünfte nach der Strafprozessordnung (StPO) nur aufgrund eines Gerichtsbeschlusses zulässig sind. Offenbar wird also die bisherige Rechtfertigung ohne weitere Erklärung dazu aufgegeben und der Polizei sowie den Staatsschutzorganen damit selbst das Instrument in die Hand gelegt, Menschen aktuell und historisch zu lokalisieren und allenfalls Bewegungsprofile daraus zu erstellen.

Die Einzige Einschränkung in § 11 im Vergleich zum Begutachtungsentwurf besteht in Ziffer 6 durch die Konkretisierung, welche Datenkategorien von Beförderungsunternehmen zu beauskunften sind.

Auch die Auskünfte über Verbindungs- und Zugangsdaten zur Telekommunikation und zu Diensten der Informationsgesellschaft gemäß § 11 Abs. 1 Z 7, der den Staatsschutzorganen Eingriffe in das Kommunikationsgeheimnis (ohne Richtervorbehalt) erlaubt, wurde ergänzt, sodass diese Befugnisse nicht nur im Hinblick auf verdächtige Einzelpersonen sondern auch auf Gruppierungen besteht. Die Überwachung der Telekommunikation durch Staatsschutzorgane ist bei dieser Rechtslage schwer kontrollierbar – für die Details der Kritik ist auf die Ausführungen soeben zu Z 5 zu verweisen.

Alle Ermittlungsmaßnahmen sind zu beenden, sobald ihre Voraussetzungen wegfallen. Hier liegt der Unterschied darin, dass bisher nur die Ermittlung nach Abs 1 Z 7 ausdrücklich davon betroffen war.

Wie schon der Hinweis auf den Grundsatz der Verhältnismäßigkeit ist auch diese Vorschrift redundant, dennoch wird die Klarstellung begrüßt.

§ 12: Datenanwendungen

§ ~~11~~12. (1) ~~Das~~ Der Bundesminister für Inneres (Bundesamt) und die Landespolizeidirektionen (Landesämter) dürfen als datenschutzrechtliche Auftraggeber in einem vom Bundesamt betriebenen Informationsverbundsystem zum Zweck der Bewertung ~~der Wahrscheinlichkeit einer Gefährdung~~von wahrscheinlichen Gefährdungen sowie zum Erkennen von Zusammenhängen und Strukturen mittels operativer oder strategischer Analyse

1. zu ~~Betroffenen~~ einer ~~Aufgabe~~Gruppierung nach § 6 Abs. 1 Z 1~~ bis 3~~

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,

i) ~~sonstige zur Personenbeschreibung erforderliche Daten,~~

~~j)~~ Dokumentendaten,

~~k~~j) Beruf ~~und,~~ 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

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

2. 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 ~~1~~2 a) bis ~~n~~o),

~~3~~4. zu Kontakt- oder Begleitpersonen, die nicht nur zufällig mit ~~Personen~~einer Gruppierung nach Z 1~~-~~, Betroffenen nach Z 2 oder ~~Z 2~~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 ~~zu diesen Personen~~ beschafft werden können, die Datenarten nach Z ~~1~~2 a) bis ~~l~~m) bis zur möglichst rasch vorzunehmenden Klärung der Beziehung zu diesen Personen, ~~sowie~~

~~4~~5. zu Informanten und sonstigen Auskunftspersonen die Datenarten nach Z ~~1~~2 a) bis j~~),~~)

sowie tat- und fallbezogene Informationen und Verwaltungsdaten verarbeiten~~,~~. Soweit dies zur Erfüllung des Zwecks (Abs. 1) unbedingt erforderlich ist, dürfen auch ~~wenn es sich um besonders schutzwürdige~~sensible Daten im Sinne des § 4 Z 2 ~~Datenschutzgesetz 2000 (~~DSG 2000~~), BGBl. I Nr. 165/1999, handelt.~~

(2) Die Datenanwendung darf als Informationsverbundsystem zwischen dem Bundesamt und den Landes nhang stehend verarbeitet werden. ~~Daten gemetnanwendung , 2 und 4 sind ltionsverbundsystem zwischen dem Bundesamt und den Landes nhang stehender Daten juristi fher Personen,ttlung nach Abs 1 Z 7 davon betroffennach formantentenetroffene, Begleit und Koneicherungen nach derselben Ziffer bestimmt sich die Löschung nach dem Zeitpunkt der letzten~~

~~Speicherung. Übermittlungen sind an Sicherheitsbehörden für Zwecke der Sicherheitspolizei und Strafrechtspflege, an Staatsanwaltschaften und ordentliche Gerichte für Zwecke der Strafrechtspflege, an Dienststellen inländischer Behörden, soweit dies eine wesentliche Voraussetzung zur Wahrnehmung einer ihr gesetzlich übertragenen Aufgabe ist, sowie an ausländische Sicherheitsbehörden entsprechend den Bestimmungen über die internationale polizeiliche Amtshilfe zulässig.~~

(~~3~~2) Die Daten sind vor der Verarbeitung in der Datenanwendung auf ihre Erheblichkeit und Richtigkeit zu prüfen sowie während der ~~Verarbeitung~~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.

(~~4~~3) Daten sind nach Maßgabe des § 13 und soweit es sich um Daten zu Verdächtigen gemäß Abs.1 Z 3 sowie damit in Zusammenhang stehende Personen gemäß Z 4 und 5 handelt längstens nach fünf Jahren zu löschen. Daten zu Kontakt- und Begleitpersonen gemäß 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 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.

(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.

~~*(2) Das Bundesamt darf sonstigen Sicherheitsbehörden über die in der Evidenz verarbeiteten personenbezogenen Daten nur Auskunft erteilen, wenn diese die Daten für die Abwehr gefährlicher Angriffe oder krimineller Verbindungen (§ 21 Abs. 1 SPG) oder zum vorbeugenden Schutz von Leben, Gesundheit oder Freiheit (§ 22 Abs. 2 SPG) der in Abs. 1 genannten Menschen benötigen. Eine Auskunftserteilung an andere Behörden ist unzulässig. Anzeigepflichten nach der StPO bleiben unberührt.*~~

~~*(3) Jede Verwendung der gemäß Abs. 1 verarbeiteten personenbezogenen Daten ist zu protokollieren. Die Daten sind spätestens zehn Jahre nach der letzten Information zu löschen.*~~

Kommentar:

Wie schon zu § 11 beschrieben, haben § 12 und § 11 Platz getauscht. Hier kam es zu Veränderungen der Auflistungen.

Während die Befugnis zur Führung der sehr umfassenden Datenanwendung nach dem Begutachtungsentwurf zulässig war zur „Bewertung der Wahrscheinlichkeit eines Angriffs“ lautet die Anknüpfung nunmehr „zur Bewertung von wahrscheinlichen Gefährdungen“. Diese Formulierung erscheint zwar enger als die ursprüngliche, löst aber das eigentliche Problem nicht. Es bestehen keine objektivierten Kriterien, woraus sich die Wahrscheinlichkeit für eine Gefährdung ergibt und wo die Grenze zu ziehen ist. Ein konkreter Verdacht ist an dieser Stelle jedenfalls nicht gefordert, obgleich mit den §§ 278a ff StGB Straftatbestände existieren, die ohnehin bereits die Mitgliedschaft zu einer kriminellen oder terroristischen Organisation unter Strafe stellen und damit bei einem konkreten Verdacht die Befugnisse zur Abwehr „gefährlicher Angriffe“ nach dem SPG begründen.

Interessant erscheint die Änderung in der Regierungsvorlage, dass zu Betroffenen nach § 6 Abs 1 Z 3 keine Daten mehr verarbeitet werden dürfen, da diese Bestimmung in der Aufstellung gestrichen wurde. Das Bedeutet also, dass zu Personen, die im Verdacht stehen, im Ausland einen Sachverhalt verwirklicht zu haben, der einem verfassungsgefährdenden Angriff entspricht, keine Daten in der Datenanwendung gemäß § 12 verarbeitet werden dürfen.

§ 13: Besondere Löschungsverpflichtung

(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 das Bundesamt ~~und~~oder die Landesämter stellt. ~~Die~~Überdies kann die unverzügliche Löschung ~~kann jedoch~~ unterbleiben, wenn in Hinblick auf die ~~Person oder~~ 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. Das Bundesamt und die Landesämter haben ~~solche~~diese Daten~~, wenn sie sechs Monate unverändert geblieben sind,~~ einmal jährlich daraufhin zu prüfen, ob ~~sie nicht gemäß Abs. 1 richtig zu stellen oder zu löschen sind~~ihre Weiterverarbeitung erforderlich ist. Wenn sich zwei Jahre nach Ablauf der Zeit, für die die Ermächtigung dazu erteilt wurde, keine Aufgabe für das Bundesamt und die Landesämter 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 vom Bundes- oder Landesamt gemäß § 16 Abs. 2 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.

Kommentar:

Im Begutachtungsentwurf hatten das Bundesamt und die Landesämter die Daten, wenn sie sechs Monate unverändert geblieben sind, zu prüfen, sie richtigzustellen oder zu löschen. Nun müssen die genannten Ämter diese Daten jährlich prüfen. Gerade bei strategisch angelegter weitreichender Überwachung eines Netzwerks („Gruppierung“) werden praktisch häufig auch Daten über Personen anfallen, die sich im Zuge der weiteren Beobachtung als irrelevant für die Ermittlungen erweisen. Je länger der Abstand zur Überprüfung der Relevanz gesetzt wird, wenn in den Ermittlungen selbst wenig Neues herauskommt, desto stärker rückt die nach § 12 sehr weitreichende Datensammlung

auch zu Kontakt- und Begleitpersonen in die Nähe einer Vorratsdatenspeicherung. Daher sollte man sich hier ernsthaft mit den Entscheidungsgründen des Verfassungsgerichtshofs zur Aufhebung der sechsmonatigen Vorratsdatenspeicherung von Telekommunikationsdaten auseinandersetzen.

Neu eingefügt wurde Absatz 2, der eine Speicherung von Daten für weitere sechs Monate anordnet, nachdem ein Betroffener über eine Maßnahme von den Behörden informiert wird. Ohne ergänzende Ausführungen zum Zweck dieser Bestimmung ist schwer nachvollziehbar, ob diese Ausdehnung der Löschungsfrist eher im Sinne des Rechtsschutzes oder eher im Sinne der Ermittlungen vorgeschlagen wurde. Hier wäre eine Klarstellung überhaupt die Voraussetzung zur Beurteilung des Vorschlags.

Vertrauenspersonen

Die die Vertrauenspersonenevidenz (ehemaliger § 13) gestrichen wurde, findet sich nun die besondere Löschungsverpflichtung in § 13. Die Kommentierung zur veränderten Rechtsgrundlage in Bezug auf Vertrauenspersonen erfolgt daher an dieser Stelle.

Im PStSG findet sich ein Hinweis auf Vertrauenspersonen nur noch im Zusammenhang mit Begründungspflichten zu deren Einsatz gegenüber dem Rechtsschutzbeauftragten. Die ausdrücklichen Regelungen finden sich nach der Regierungsvorlage nunmehr in § 54 Abs. 3 und Abs. 3a SPG – die auch für die Staatsschutzorgane maßgeblich sind. Abs. 3 reguliert ausdrücklich die Zulässigkeit von verdeckten Ermittlungen durch Vertrauenspersonen im Auftrag der Polizei. Der schon im Begutachtungsentwurf komplett neu vorgeschlagene § 54 Abs. 3a SPG war ursprünglich auf die Dokumentation und Kontrolle beim Einsatz von verdeckten Ermittlern gerichtet. Gleichzeitig mit der Streichung der Vertrauenspersonenevidenz im PStSG wurde nun in der Fassung der Regierungsvorlage „verdeckte Ermittler“ durch „Vertrauenspersonen“ ersetzt. Die Bestimmungen zur Vertrauenspersonenevidenz sind auch für den Aufgabenbereich des Staatsschutzes im (bestehenden) § 54b SPG zu finden. Dort ist schon jetzt ausdrücklich normiert, dass solche Vertrauenspersonen den Sicherheitsbehörden Informationen gegen Zusage einer Belohnung preisgeben. Trotz der auf den ersten Blick wesentlichen Änderung des PStSG in dieser Hinsicht bleibt die schon in der Stellungname zum Begutachtungsentwurf artikulierte Kritik am bezahlten Spitzelwesen unverändert aufrecht.

§ 14: Rechtsschutzbeauftragter

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

(2) Das Bundesamt und die Landesämter, denen sich eine Aufgabe gemäß § 6 Abs. 1 Z 1 und ~~Z~~ 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 § ~~12~~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 ~~höchstens~~ sechs Monaten ~~erteilt werden; Verlängerung ist~~; Verlängerungen sind zulässig.

Kommentar:

Dem Rechtsschutzbeauftragten obliegt nach der Regierungsvorlage auch die Kontrolle der Datenanwendung nach § 12 Abs 6. Dem Rechtsschutzbeauftragen obliegt die Ermächtigung für Aufgaben nach § 6 Abs 1 Z 1 und Z 2. Diese darf jetzt für höchstens sechs Monate erteilt werden. Neu ist allerdings, dass Verlängerungen zulässig sind. Im Begutachtungsentwurf war nur eine einzige Verlängerung zulässig. Zu bedenken ist hier, ob durch die Zulässigkeit mehrerer Verlängerungen der Zeitraum ausufern könnte.

§ 15: Rechte und Pflichten des Rechtsschutzbeauftragten

(1) Das Bundesamt und die Landesämter haben dem Rechtsschutzbeauftragten bei der Wahrnehmung seiner Aufgaben jederzeit Einblick in alle erforderlichen Unterlagen und Aufzeichnungen zu gewähren, ihm auf Verlangen Abschriften (Ablichtungen) einzelner Aktenstücke unentgeltlich auszufolgen und alle erforderlichen Auskünfte zu erteilen; insofern kann ihm gegenüber Amtsverschwiegenheit nicht geltend gemacht werden. Dies gilt jedoch nicht für Auskünfte ~~und Unterlagen~~ über die Identität von Personen ~~oder über Quellen, deren Bekanntwerden die nationale Sicherheit oder die Sicherheit von Menschen gefährden würde, und für Abschriften (Ablichtungen), wenn das Bekanntwerden der Information die nationale Sicherheit oder die Sicherheit von Menschen gefährden würde~~nach Maßgabe des § 162 StPO.

(2) Dem Rechtsschutzbeauftragten ist jederzeit Gelegenheit zu geben, die Durchführung der in § ~~15~~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 § ~~14 oder den besonderen Löschungsbestimmungen~~13 zu überwachen.

~~(3)~~(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:

Dem Rechtsschutzbeauftragen kann nach der Regierungsvorlage im Gegensatz zum Begutachtungsentwurf die Akteneinsicht nur dann verweigert werden, wenn es sich um Auskünfte über die Identität von Personen nach Maßgabe des § 162 StPO handelt. Diese Bestimmung regelt die anonyme Aussage von Zeugen, wenn zu befürchten ist, dass der Zeuge sich oder einen Dritten durch die Bekanntgabe des Namens und anderer Angaben zur Person (Geburtsort, Beruf, Wohnort,…) einer ernsten Gefahr für Leben, Gesundheit, körperliche Unversehrtheit oder Freiheit aussetzen würde. Diese Neuregelung stellt eine Besserung dar. Dennoch ist fragwürdig, warum auch dem Rechtsschutzbeauftragten die Identität „gefährdeten" Zeugen verborgen bleiben soll. Im Vergleich zu einem Gerichtsverfahren bestehen im Kontrollverfahren durch den Rechtsschutzbeauftragten nämlich keine Öffentlichkeit und auch keine Akteneinsicht der Beschuldigten. Sieht man den Rechtsschutzbeauftragten grundsätzlich als vertrauenswürdig, ist der Schutzzweck der beschränkten Akteneinsicht nicht erkennbar.

Desweiteren kommt dem Rechtsschutzbeauftragten in Verfahren vor der Datenschutzbehörde, den Verwaltungsgerichten sowie den Gerichtshöfen des öffentlichen Rechts, die Stellung einer mitbeteiligten Amtspartei zu. Das bedeutet, er kann als „Amtspartei" Einwendung geltend machen und Beschwerde/Berufung erheben.

Trotz der begrüßenswerten Änderung, dass die ursprünglich vorgeschlagene, weitgehende und geradezu willkürliche Beschränkung der Akteneinsicht nunmehr stark eingeschränkt ist, ist die Kritik am schwachen Rechtsschutzsystem weiterhin aufrecht zu erhalten. Um Wiederholungen zu vermeiden wird grundsätzlich auf die Stellungnahme des AKVorrat im Begutachtungsverfahren 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 Innenministerium. An dieser Stelle sei angemerkt, dass die Regierung offenbar zeitgleich in anderen Zusammenhängen durchaus erkannt hat, dass das Modell des Rechtsschutzbeauftragten alleine bei schwerwiegenden Grundrechtseingriffen keinen hinreichenden Rechtsschutz bietet. Dementsprechend wurde beim kürzlich vor der Sommerpause verabschiedeten „Bankenpaket" im Zusammenhang mit Eingriffen in das Bankgeheimnis neben einer begleitenden Kontrolle durch einen (beim BMF neu geschaffenen) Rechtsschutzbeauftragten eine vollwertige gerichtliche Kontrolle durch das Bundesfinanzgericht geschaffen. 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.

§ 16: Information Betroffener

(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 vom Bundes- oder Landesamt über Grund, Art und Dauer sowie die Rechtsgrundlage der gesetzten Maßnahmen zu informieren. Über die durchgeführte Information ~~Betroffener~~ 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:

Im Gegensatz zum Begutachtungsentwurf nimmt die Regierungsvorlage jene Betroffene vom Informationsanspruch aus, die gemäß § 6 Abs. 1 Z 3 PStSG einen „verfassungsgefährdenden Angriff" im Ausland begehen und entsprechende Informationen dazu aus dem Ausland oder von Internationalen Organisationen bereitgestellt werden. Zu fragen ist, ob dieser Informationsanspruch

deshalb entfällt, weil auch die Datenanwendung nach § 12 PStSG diese Gruppe ausnimmt. Allerdings ist schwer vorstellbar, dass zu dieser Gruppe überhaupt keine personenbezogenen Daten mehr verarbeitet werden dürfen, weil ansonsten die entsprechende Befugnis wohl kaum wahrgenommen werden könnte.

§ 17: Berichte über den polizeilichen Staatsschutz

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

(2) Über die Erfüllung der Aufgaben nach diesem Bundesgesetz sowie über die Information Betroffener nach § ~~17~~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.

(3) Den Bericht des Rechtsschutzbeauftragten gemäß § ~~16~~15 Abs. ~~3~~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 im Rahmen des Auskunfts- und Einsichtsrechtes nach Art. 52a Abs. 2 B-VG zugänglich zu machen.

Kommentar:

Keine substanziellen Veränderungen.

§18: Inkrafttreten

(1) Dieses Bundesgesetz tritt mit 1. ~~Jänner~~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:

Statt mit 1. Jänner 2016 soll das Gesetz erst am 01. Juli 2016 in Kraft treten. Erfreulich ist dabei, dass die auch stark durch den AKVorrat geprägte öffentliche Debatte offenbar bewirkt hat, dass damit zumindest ein halbes Jahr mehr Zeit für sachliche Diskussionen im Zuge des weiteren parlamentarischen Prozesse bleibt.

§ 19: Sprachliche Gleichbehandlung

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 Veränderungen

§ 20: Verweisungen

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

Kommentar:

Keine Veränderungen

§ 21: Übergangsbestimmungen

(1) Vor Inkrafttreten dieses Bundesgesetzes erteilte Ermächtigungen gemäß § 91c Abs. 3 SPG in der Fassung vor Inkrafttreten dieses Bundesgesetzes gelten als Ermächtigungen gemäß § ~~15~~14 Abs. 2 und bleiben bis zum festgesetzten Zeitpunkt, längstens bis zum ~~30. Juni~~31. Dezember 2016, weiterhin gültig; für diese gelten die Löschungsfristen nach § ~~14 Abs. 2~~13.

(2) Personenbezogene Daten, die vor Inkrafttreten dieses Bundesgesetzes vom Bundes- oder Landesamt für die Aufgabe nach § 21 Abs. 3 SPG in der Fassung vor Inkrafttreten dieses Bundesgesetzes rechtmäßig ermittelt wurden, dürfen nach Maßgabe des § ~~11~~12 Abs. 1 und ~~3~~2 in der Datenanwendung gemäß § ~~11~~12 verarbeitet werden.

~~(3~~(3) Lokale Datenanwendungen, die vor Inkrafttreten dieses Bundesgesetzes auf Grundlage des SPG geführt wurden, dürfen 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 des Bundes- oder Landesamtes sind, haben die in § 2 Abs. 3 vorgesehene spezielle Ausbildung für Verfassungsschutz und Terrorismusbekämpfung innerhalb von ~~zwei~~drei Jahren ab dem Tag des Inkrafttretens zu absolvieren.

Kommentar:

Keine substanziellen Veränderungen

§ 22: Vollziehung

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

Kommentar:

Keine Veränderungen

III. Bundesgesetz, mit dem das Sicherheitspolizeigesetz geändert wird:

Vorbemerkung zu den einzelnen Bestimmungen:

An dieser Stelle erfolgt nur die Weitergabe der SPG Änderungen in der Fassung der Regierungsvorlage und unter Kenntlichmachung der Änderungen im Vergleich zum Begutachtungsentwurf. Zu den wichtigsten substantiellen Änderungen im SPG sind die Kommentare im Zusammenhang mit den relevanten Änderungen zum PStSG bzw. in der Zusammenfassung formuliert.

Die Änderungen im Einzelnen:

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 ~~wird~~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 ~~zulässig~~, sofern gesetzlich nicht ~~Besonderes~~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 ~~österreichischer Zivilluftfahrzeuge~~von Zivilluftfahrzeugen, soweit sich ihre Organe auf begründetes Ersuchen des Luftfahrzeughalters oder zur Erfüllung gesetzlicher Aufgaben an Bord befinden und ~~bindendes~~ Völkerrecht dem nicht entgegensteht.“

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

7. ~~Die~~In der Überschrift ~~des~~zu § 25 wird das Wort „Kriminalpolizeiliche“ durch das Wort „Sicherheitspolizeiliche“ ersetzt.

8. In § 53 entfallen in Abs. 1 die Z 2a und 7~~, in Abs. 3~~ 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“ ~~sowie~~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~~“ und es werden folgende Absätze ein- bzw. angefügt:~~“.

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 ~~das~~ der Bundesminister für Inneres (Bundesamt für Verfassungsschutz und Terrorismusbekämpfung) und die Landespolizeidirektionen (Landesämter Verfassungsschutz ~~(§ 1 Abs. 3 Polizeiliches Staatsschutzgesetz - PStSG, BGBl. I Nr. xx/2015) im~~) als datenschutzrechtliche Auftraggeber in einem vom Bundesamt 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.“

~~12~~14. In § 54 entfallen in Abs. 2 die Z 1 sowie in Abs. 4 die Wortfolge „und zur erweiterten Gefahrenerforschung (§ 21 Abs. 3)“.

~~13~~15. § 54 Abs. 3 lautet:

„(3) Das Einholen von Auskünften durch die Sicherheitsbehörde ohne Hinweis gemäß Abs. 1 oder ~~durch andere Personen~~ 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).“

~~14~~16. Nach § 54 Abs. 3 wird folgender Abs. 3a eingefügt:

„(3a) ~~Der verdeckte Ermittler~~Die Vertrauensperson ist von der Sicherheitsbehörde zu führen und regelmäßig zu überwachen. ~~Sein~~Ihr Einsatz und dessen nähere Umstände sowie Auskünfte und Mitteilungen, die durch ~~ihn~~sie erlangt werden, sind zu dokumentieren (§ 13a), sofern ~~sie~~diese für die Aufgabenerfüllung von Bedeutung sein können.“

~~15~~17. In § 54 Abs. 5 wird im ersten Satz vor der Wortfolge „einer Zusammenkunft“ die Wortfolge „oder im Zusammenhang mit“ eingefügt~~, das Wort „Anwesender“ gestrichen~~ und ~~lautet~~ der letzte Satz lautet:

„Die auf diese Weise ermittelten Daten dürfen auch zur Abwehr und Verfolgung gefährlicher Angriffe ~~und~~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, ~~verarbeitet~~verwendet werden.“

~~16~~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.“

~~17~~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).“

~~18~~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 ~~und~~sowie das Zitat „Abs. 1“ durch das Zitat „Abs. 1 und 1a“ ersetzt.

~~19~~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.“

~~20~~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. 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.

~~21~~25. § 91d Abs. 1 letzter Satz lautet:

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

26. 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 ~~und;~~ 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.“.

~~22~~27. 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/2015 treten mit ~~xx. xx 2015~~1. Jänner 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, 91c Abs. 1, 91d Abs. 1, 3 und 4, 96 Abs. 8 sowie das Inhaltsverzeichnis in der Fassung des Bundesgesetzes BGBl. I Nr. XX/2015 treten mit 1. ~~Jänner~~Juli 2016 in Kraft. Gleichzeitig treten die §§ 21 Abs. 3, 63 Abs. 1a und 1b, 91c Abs. 3 und 93a samt Überschrift außer Kraft.“

~~23~~28. Dem § 96 wird folgender Abs. 8 angefügt:

„(8) Daten, die auf Grundlage des § 53a Abs. 1 in der Fassung vor BGBl. I Nr. xx/20xx für den Personen- und Objektschutz ~~im~~bis zum Zeitpunkt des Inkrafttretens des Bundesgesetzes BGBl. I Nr. xx/20xx verarbeitet ~~werden~~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 ~~Informationsverbund~~Informationsverbundsystem geführt werden.“

~~24~~29. Dem § 97 wird folgender Abs. 4 angefügt:

„(4) § 13a Abs. 3 in der Fassung des Bundesgesetzes BGBl. I Nr. XX/2015 tritt mit Ablauf des 31. Dezember ~~2018~~2019 außer Kraft.“