BUNDESKANZLERAMT VERFASSUNGSDIENST

GZ ● BKA-601.598/0002-V/5/2014
ABTEILUNGSMAIL ● V5@BKA.GV.AT
BEARBEITER ● FRAU DR. MARTINA LAIS
FRAU MAG. STEFANIE DÖRNHÖFER[1]
PERS. E-MAIL ● MARTINA.LAIS@BKA.GV.AT
TELEFON ● +43 1 53115-202843
IHR ZEICHEN ●BMI-LR1340/0001-III/1/2014

An das
Bundesministerium für
Inneres

Herrengasse 7
1014 Wien

Antwort bitte unter Anführung der GZ an die Abteilungsmail

Entwurf eines Bundesgesetzes, mit dem das Sicherheitspolizeigesetz geändert wird (SPG-Novelle 2014)
Begutachtung; Stellungnahme

Zu dem mit der do. oz. Note übermittelten Gesetzesentwurf nimmt das Bundeskanzleramt-Verfassungsdienst wie folgt Stellung:

I. Allgemeines

Es wird darauf hingewiesen, dass die Übereinstimmung des im Entwurf vorliegenden Bundesgesetzes mit dem Recht der Europäischen Union vornehmlich vom do. Bundesministerium zu beurteilen ist.

II. Inhaltliche Bemerkungen

Zu Z 4 (§ 22):

Nach den Erläuterungen umfasst der Begriff der „öffentlichen Informations- und Kommunikationstechnologie“ „jegliches Kommunikationsinstrument oder [gemeint wohl: jegliche] Kommunikationsanwendung, inklusive Radio, Fernsehen, Mobiltelefonie, Hardware und Software für Computer und Netzwerke, Satellitensysteme sowie die verschiedenen Dienstleistungen und Anwendungen, die damit verbunden sind“, wobei als Beispiel der „gesamte elektronische Zahlungsverkehr“ genannt wird. Ein solches weites Verständnis erschließt sich nicht

[1] Aus datenschutzrechtlicher Sicht.

aus dem Gesetzesbegriff. Gesetz und Erläuterungen sollten einander angepasst werden.

Nach den Erläuterungen reichen zwar die geltenden sicherheitspolizeilichen Befugnisse zum Schutz der Betreiber kritischer Infrastrukturen aus. Da eine Erweiterung sicherheitspolizeilicher Aufgaben aber eine Ausweitung der bestehenden Befugnisse nach sich zieht und in Anknüpfung an den Schutz kritischer Infrastrukturen die Fälle der Sicherheitsüberprüfung erweitert werden sollen, sollte überprüft werden, ob die vorgeschlagene Ergänzung der Aufgaben des vorbeugenden Schutzes von Rechtsgütern überhaupt erforderlich ist.

Zu Z 10 (§ 55a Abs. 2 Z 3a):

Die vorgeschlagene Sicherheitsüberprüfung im Zusammenhang mit dem Schutz kritischer Infrastrukturen steht, insbesondere wegen des weiten Anwendungsbereiches dieses Begriffes, in einem wertungsmäßigen Spannungsverhältnis zu den übrigen Fällen einer Sicherheitsüberprüfung nach § 55a Abs. 2 SPG. Es sollte daher überprüft werden, ob die Sicherheitsüberprüfung nicht auf einzelne Bereiche kritischer Infrastrukturen eingeschränkt werden kann, zumal eine Sicherheitsüberprüfung voraussetzt, dass der Betroffene Zugang zu „vertraulicher Information“ hat, also zu Information, die unter strafrechtlichem Geheimhaltungsschutz (insb. nach dem 16. Abschnitt des StGB „Landesverrat“) steht und deren Geheimhaltung im öffentlichen Interesse gelegen ist (§ 55 Abs. 3 Z 1 SPG). Sofern dies in einzelnen Bereichen kritischer Infrastrukturen von vornherein ausgeschlossen oder unwahrscheinlich ist, sollten diese Bereiche vom Anwendungsbereich der Sicherheitsüberprüfung von vornherein ausgenommen werden.

Zu Z 12 (§ 56 Abs. 1 Z 3a):

Die im Entwurf vorgesehene „Übermittlung vorhandener Beweismittel“ ist zu weit gefasst und würde dem Wortlaut nach etwa auch Kommunikationsdaten oder DNA-Daten beinhalten. Eine Einschränkung auf konkrete Beweismittel, etwa auf die in den Erläuterungen genannten Lichtbilder und Vernehmungsprotokolle, wäre in diesem Zusammenhang jedenfalls einer pauschalen Formulierung vorzuziehen. Dabei ist zu berücksichtigen, dass diese Beweismittel auch Daten weiterer Betroffener enthalten können (zB Nennung von Namen im Vernehmungsprotokoll). Zudem ist sicherzustellen, dass die Übermittlung von Daten in jedem Einzelfall auf ihre Erforderlichkeit und Verhältnismäßigkeit hin geprüft wird; im Falle einer

rechtskräftigen Verurteilung würde etwa die Mitteilung über den Ausgang des Strafverfahrens ausreichen, womit eine Übermittlung von Beweismitteln nicht mehr erforderlich wäre.

Zu Z 15 (§ 65 Abs. 1 und 5):

Es ist darauf hinzuweisen, dass der Verfassungsgerichtshof in seinem Prüfungsbeschluss vom 1. Oktober 2013, B 1156/2013 (Gesetzesprüfungsverfahren G 90/2013), hinsichtlich § 65 Abs. 1 das Bedenken formuliert hat, dass „der Verdacht der Begehung jedweder Straftat – selbst einer Verwaltungsstraftat sowie gerichtlich strafbarer Fahrlässigkeitsdelikte oder gerichtlich strafbarer Vorsatzdelikte mit geringem Unwertgehalt („Bagatelldelikte“) – Anlass für eine erkennungsdienstliche Behandlung geben“ kann. Mit der vorgeschlagenen Formulierung wird dieses Bedenken zwar im Hinblick auf Verwaltungsstraftaten und Fahrlässigkeitsdelikte entkräftet, nicht jedoch im Hinblick auf Bagatelldelikte.

Hinzu kommt, dass bei der Prognoseentscheidung dem Wortlaut nach („oder“) ausschließlich auf die Art der Tat abgestellt werden kann, dh. dass die Gefahrenprognose – unabhängig von der Ausführung der Tat und der Persönlichkeitsstruktur des Betroffenen – ausschließlich auf zB statistische Zahlen zur Rückfallswahrscheinlichkeit bei bestimmten Delikten gestützt werden kann. Die Bestimmung läuft damit letztlich darauf hinaus, dass eine erkennungsdienstliche Behandlung bei Personen, die der Begehung eines bestimmten Deliktes mit hoher Rückfallswahrscheinlichkeit verdächtig sind, in jedem Fall als erforderlich anzusehen sein wird, was dem Grundsatz der Verhältnismäßigkeit widerspricht.

Zu Z 16 (§ 67 Abs. 1):

Im Hinblick auf die vom Verfassungsgerichtshof in seinem Erkenntnis vom 12. März 2013, G 76/2013, angesprochene „besondere Sensibilität eines DNA-Profiles …, dessen künftige Verwendbarkeit bzw. Aussagekraft heute noch gar nicht absehbar ist …, sowie die Möglichkeit einer zweckentfremdeten Nutzbarmachung“ wäre anstelle einer Differenzierung nach der Strafdrohung eine Differenzierung nach Deliktstypen zu bevorzugen. Soweit in den Erläuterungen darauf hingewiesen wird, dass die Abgrenzung jener des Europäischen Haftbefehles sowie jener für den Zugriff auf DNA-Daten im Rahmen des Prümer Datenverbundes entspricht, ist zu bemerken, dass die Verhältnismäßigkeit der Übermittlung vorhandener (zulässigerweise ermittelter) DNA-Daten unter anderen Gesichtspunkten zu beurteilen ist als deren Ermittlung.

Der Verfassungsgerichtshof hat im oben genannten Erkenntnis ausgesprochen, dass § 67 Abs. 1 erster Satz SPG keine hinreichenden Kriterien enthält, welche die im Einzelfall vorzunehmende Prognoseentscheidung entsprechend determinieren würden. Dieses Defizit wird mit der vorgeschlagenen Änderung nicht behoben; entsprechende Kriterien zur Determinierung der Einzelfallentscheidung sind daher jedenfalls in den Gesetzestext aufzunehmen.

Darüber hinaus stellt sich wie schon bei § 65 Abs. 1 auch hier das Problem, dass bei der Prognoseentscheidung nach dem Wortlaut („oder“) ausschließlich auf die Art der begangenen strafbaren Handlung abgestellt werden kann, was dazu führt, dass bei Personen, die der Begehung eines bestimmten Deliktes mit statistisch hoher Rückfallswahrscheinlichkeit verdächtig sind, eine DNA-Untersuchung in jedem Fall als erforderlich anzusehen sein wird, was – gerade in Anbetracht der besonderen Sensibilität von DNA-Daten – dem Grundsatz der Verhältnismäßigkeit widerspricht.

Zu Z 17 (§ 73):

Wenngleich § 73 Abs. 1 nach dem Erkenntnis des Verfassungsgerichtshofes vom 12. März 2013, G 76/12, bei einer verfassungskonformen Interpretation eine angemessene Abwägung und Gewichtung des Interesses des Betroffenen an der Geheimhaltung bzw. Löschung seiner personenbezogenen Daten und dem Interesse des Staates am Fortbestehen des Eingriffes durch Fortsetzung der Speicherung nach den allgemeinen Grundsätzen über die Verwendung von Daten im Einzelfall erlaubt, wird empfohlen, einen entsprechenden Tatbestand aufzunehmen.

Die im Falle einer Verurteilung anzuwendende Bestimmung der Z 1 (eine Anwendung der Z 4 kommt diesfalls nicht in Betracht) legt eine sehr umfangreiche Maximalspeicherdauer für Daten aus einer erkennungsdienstlichen Behandlung (Vollendung des 80. Lebensjahres und seit der letzten erkennungsdienstlichen Behandlung mindestens fünf Jahre verstrichen) fest. Eine derart lange Speicherung – möglicherweise über 60 Jahre bei Bagatelldelikten – wäre nach den datenschutzrechtlichen Grundsätzen in der Mehrzahl der Fälle unverhältnismäßig; letztlich sieht der Gesetzgeber mit gutem Grund etwa auch für Strafregisterdaten Tilgungsfristen vor. Da in der Praxis eine regelmäßige amtswegige Prüfung sämtlicher Datensätze dahingehend, ob die fortdauernde Speicherung nach den allgemeinen Grundsätzen des Datenschutzes nach wie vor zulässig ist, kaum umsetzbar ist, wird angeregt, in § 73 Abs. 1 (insbesondere auch für den Fall einer gerichtlichen Verurteilung) generell die amtswegige Löschung der Daten aus einer

erkennungsdienstlichen Behandlung nach einem bestimmten Zeitraum (zB fünf Jahre nach der letzten erkennungsdienstlichen Behandlung) anzuordnen und eine weitere Verarbeitung im Einzelfall davon abhängig zu machen, dass dies erforderlich ist, weil auf Grund konkreter Umstände zu erwarten ist, der Betroffene werde gefährliche Angriffe begehen.

Anregung zu § 74:

Wenngleich nach Aufhebung des § 74 Abs. 1 und 2 betreffend die Löschung erkennungsdienstlicher Daten auf Antrag des Betroffenen die allgemeinen Regelungen des Datenschutzgesetzes 2000 Anwendung finden, sollte der Wegfall dieser verfassungswidrigen Bestimmungen nicht dazu führen, dass das SPG gar keine Regelung darüber enthält, unter welchen Voraussetzungen eine Löschung erkennungsdienstlicher Daten auf Antrag des Betroffenen zu erfolgen hat. Insbesondere auch im Hinblick auf erkennungsdienstliche Daten aus einer DNA-Untersuchung wäre eine klare Regelung, in welchen Fällen diese Daten auf Antrag zu löschen sind, jedenfalls erforderlich. Um verfassungsrechtliche Probleme zu vermeiden, sollte diese Regelung – insofern vergleichbar mit § 73 Abs. 1 – nicht abschließend ausgestaltet sein und jedenfalls eine Verhältnismäßigkeitsprüfung im Einzelfall zulassen.

Dabei sollten – unbeschadet der Pflicht zur amtswegigen Löschung – jedenfalls folgende Tatbestände erfasst werden: 1) wenn der Verdacht, der für die Verarbeitung der erkennungsdienstlichen Daten maßgeblich ist, nicht bestätigt werden konnte oder wenn die Tat nicht rechtswidrig war, es sei denn, weiteres Verarbeiten wäre deshalb erforderlich, weil auf Grund konkreter Umstände zu befürchten ist, der Betroffene werde gefährliche Angriffe begehen; 2) wenn der Verdacht zu einer rechtskräftigen Verurteilung geführt hat, jedoch auf Grund der konkreten Umstände des Falles nicht zu erwarten ist, dass der Betroffene weitere gefährliche Angriffe begehen werde.

III. Legistische und sprachliche Bemerkungen

Zu Z 3 (§ 16 Abs. 2 Z 4):

Entsprechend Punkt 25 der Legistischen Richtlinien 1990[2] wäre das Wort „oder“ in Z 4 beizubehalten. Die Novellierungsanordnung wäre im Übrigen umzuformulieren (etwa: *In § 16 Abs. 2 werden in Z 5 am Ende das Wort* „oder“ *und folgende Z 6 angefügt:*)

Zu Z 16 (§ 67 Abs. 1):

Im ersten Satz hätte der Beistrich nach dem Wort „begehen“ zu entfallen.

Zum Vorblatt:

Im Allgemeinen Teil der Erläuterungen ist anzugeben, worauf sich die Zuständigkeit des Bundes zur Erlassung der vorgesehenen Neuregelungen gründet (Punkt 94 der Legistischen Richtinien 1979[3]). Die diesbezüglichen Anmerkungen im Vorblatt wären daher in den Allgemeinen Teil der Erläuterungen zu überführen.

Diese Stellungnahme wird im Sinne der Entschließung des Nationalrates vom 6. Juli 1961 auch dem Präsidium des Nationalrates zur Kenntnis gebracht.

20. März 2014
Für den Bundesminister für
Kunst und Kultur, Verfassung und öffentlichen Dienst:
HESSE

Elektronisch gefertigt

[2] http://www.bka.gv.at/Docs/2005/11/28/LegRL1990.doc
[3] http://www.bka.gv.at/2004/4/15/richtlinien1979.doc

Signaturwert	tX1vwE4PO9xmi3FqqEQ5lk6fBIW0v2HJQyFuk0B7K+sgHQ5yUH3ShsNgXp0ouaMzjzJ Ggwr/Hmi96zUtytBdfyZwWNL+xaH7gwrX6elk7+o9ebo5oCfTx82WfrmsYGGXRiz4n+ /4wTi8Q9BzKN9+tbU6dlwyJbmb1Zb9OjgjRoVfqI7sn9Y0w/JdtDdpdeaMd26ANm9np CSS8JuNJ4LqG4GYQILZdMvfytpurrxh7JrU5ufoZhY65HBIkmS8Pq7gWmwtF5epc4Yr 0RXKgW2UqIWZpYZe2dkbXrUr9aqULQkdGYIKgMCqMdXZEBB/W9/jhtEr4dfprH5vsIz IglkstA==	
	Unterzeichner	serialNumber=812559419344,CN=Bundeskanzleramt,C=AT
	Datum/Zeit-UTC	2014-03-20T12:32:28+01:00
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	1026761
	Methode	urn:pdfsigfilter:bka.gv.at:binaer:v1.1.0
Hinweis	Dieses Dokument wurde amtssigniert.	
Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: http://www.bka.gv.at/verifizierung	