REPUBLIK ÖSTERREICH
DATENSCHUTZRAT

A-1010 Wien, Ballhausplatz 1
Tel. ++43-1-531 15/2527
Fax: ++43-1-53109/2702
e-mail: dsrpost@bka.gv.at
DVR: 0000019

GZ BKA-817.230/0001-DSR/2007

An das
Bundesministerium für Inneres
Sektion III-Recht

E-Mail: bmi-III-1@bmi.gv.at

Betrifft: Bundesgesetz, mit dem das Sicherheitspolizeigesetz (SPG), das Grenzkontrollgesetz (Greko) und das Polizeikooperationsgesetz (PolKG) geändert werden
Stellungnahme des Datenschutzrates

Der Datenschutzrat hat in seiner 177. Sitzung am 21. September 2007 beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

I. Allgemeines:

Der vorgelegte Entwurf einer Novelle des SPG verfolgt eine Mehrzahl von Regelungszielen. Zunächst soll dem Erfordernis von im Sinne des § 1 Abs. 2 DSG 2000 ausreichend determinierten Eingriffsermächtigungen zur Datenverwendung Rechnung getragen werden, und zwar vor allem mit Blick auf das Auslaufen der im Verfassungsrang stehenden Übergangsbestimmungen des § 61 Abs. 4 DSG 2000. Zu diesem Zweck soll ein neuer § 53a SPG eingefügt werden sowie § 65 Abs. 6 SPG entsprechend ergänzt werden (vgl. Art. 1 Z 5 und 16 des Gesetzesentwurfes).

Dieser Ansatz ist grundsätzlich zu begrüßen. Gewisse Probleme wirft allerdings der Umstand auf, dass die in § 53a Abs. 2 SPG vorgesehen Ermächtigungen zur Datenspeicherung partiell zu weit greifen und die in Abs. 6 vorgesehenen Löschungsfristen zu wenig restriktiv gestaltet sind. Dies zeigt vor allem ein Vergleich

mit einschlägigen europarechtlichen Vorbildregelungen im Kontext von Europol. Eine Angleichung an dortige Standards würde das Problem weitgehend lösen (Näheres dazu unten in den Detailbemerkungen).

Auch nach der Einführung des § 53a SPG bzw. der Modifikation des § 65 Abs. 6 SPG bleibt allerdings eine Regelungslücke bestehen. Weitgehend ungeregelt sind nämlich weiterhin die Aktivitäten des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung. Hier besteht somit weiterhin Handlungsbedarf.

Ein weiteres Regelungsziel der Novelle besteht darin, den Sicherheitsbehörden eine Möglichkeit zu eröffnen, etwa vermisste bzw. abgängige Personen mittels sogenannter Standortdaten, wie sie in Mobilfunknetzen anfallen, zu suchen.
Wiewohl hier ein grundsätzlich berechtigtes Anliegen zu bestehen scheint, stößt der vorgeschlagene Regelungsansatz auf verfassungsrechtliche Bedenken. Während nämlich eine Standortdatenermittlung bzw. – beauskunftung unter dem Gesichtspunkt der Strafprozessordnung restriktiv geregelt ist und insbesondere eine richterliche Kontrolle bzw. Genehmigung vorgesehen ist, fehlen vergleichbare Kontrollmechanismen im vorgeschlagenen Text völlig.
Unvorgreiflich weiterer angekündigter Gespräche regt der Datenschutzrat an, ob nicht auch im Bereich der Gefahrenabwehr eine – der richterlichen Genehmigung vergleichbare – Genehmigung durch eine Rechtsschutzinstanz (etwa den Rechtsschutzbeauftragten) vorgenommen werden könnte. In dringenden Fällen - wie z.B. bei Gefahr in Verzug - wäre zumindest eine Ex-post-Überprüfung durch eine derartige Rechtsschutzeinrichtung anzustreben.

Ein weiteres Anliegen des Entwurfes ist es, eine zentrale Analysedatei betreffend Gewaltdelikte, insbesondere sexuell motivierte Straftaten, einzurichten (vgl. Art. 1 Z 13 des Gesetzesentwurfes). Der Datenschutzrat regt daher an, analog zum Rechtsakt des Rates vom 3. November 1998 über die Durchführungsbestimmungen für die von Europol geführten Analysedateien zu Analysezwecken (Amtsblatt Nr. C vom 30. Jänner 1999 Seite 1 f) eine entsprechende Vorabüberprüfung der Analysedateien durch eine Rechtsschutzinstanz – etwa den Rechtsschutzbeauftragten – vorzusehen.

Ein weiterer Punkt der vorliegenden Novelle zielt darauf ab, erkennungsdienstliche Daten, die für einen Zweck ermittelt worden sind, auch für andere Zwecke weiter zu verarbeiten, ohne den Vorgang der physischen Gewinnung wiederholen zu müssen (vgl. Art. 1 Z 18 des Entwurfs).

Eine derartige „Rationalisierung“ im Umgang mit erkennungsdienstlichen Daten erscheint auf den ersten Blick zwar plausibel, wirft aber das gravierende Problem des Verlustes von Transparenz für die Betroffenen auf. Entsprechende ergänzende Regelungen erscheinen daher geboten (Näheres dazu unten in den Detailbemerkungen).
Ein wesentlicher Gesichtspunkt der Novelle ist schließlich in der vorgesehenen Ermächtigung von Organen des öffentlichen Sicherheitsdienstes zum direkten Datenzugriff auf internationale bzw. ausländische Datenanwendungen zu sehen (Art. 3 Z 1 des Entwurfs). Dazu ist zu bemerken, dass dieser Ansatz im offenkundigen Widerspruch zu anderen bestehenden Regelungen über die internationale Amtshilfe steht. Diese ist prinzipiell zentral organisiert und läuft über den Bundesminister für Inneres und nicht „im direkten Verkehr“ zwischen Organen des Sicherheitsdienstes. Der Hintergrund der Zentralorganisation ist insbesondere darin zu sehen, dass nicht unkontrolliert Daten zweifelhafter Qualität zwischen nachgeordneten Dienststellen grenzüberschreitend ausgetauscht werden. Vor diesem Hintergrund ist die vorgeschlagene Bestimmung nicht nur aufgrund des offenkundigen normenlogischen Widerspruches zu bestehenden Regelungen, sondern auch vor dem Hintergrund der praktischen Konsequenzen für den Datenschutz Betroffener kritisch zu hinterfragen.

II. Zu den einzelnen gesetzlichen Bestimmungen:

Zu Art.1 Z 3 (§ 53 Abs. 3a SPG)

Seitens des Datenschutzrates wurden die näheren Gespräche zu diesem Absatz an eine Expertengruppe mit Vertretern des BKA-VD, dem BMI und dem BMVIT, sowie der DSK und den Betreibern im Mobilfunkbereich, sowie Vertretern der AK und der

WKO delegiert und ersucht, über das Ergebnis möglichst rasch – vor der diesbezüglichen Beschlussfassung im Ministerrat - dem Datenschutzrat zu berichten. Der Datenschutzrat wird nach Anhörung der Expertengruppe eine abschließende Stellungnahme abgeben.
Unvorgreiflich weiterer angekündigter Gespräche regt der Datenschutzrat an, ob nicht auch im Bereich der Gefahrenabwehr eine – der richterlichen Genehmigung vergleichbare – Genehmigung durch eine Rechtsschutzinstanz (etwa den Rechtsschutzbeauftragten) vorgenommen werden könnte. In dringenden Fällen - wie z.B. bei Gefahr in Verzug - wäre zumindest eine Ex-post-Überprüfung durch eine derartige Rechtsschutzeinrichtung anzustreben.

Zu Art. 1 Z 5 (§ 53a SPG):

Der Begriff der „ordnungsdienstlichen Anlässe“ sollte zumindest in den Erläuterungen inhaltlich dargelegt werden, da nicht erkennbar ist, zu welcher der den Sicherheitsbehörden zukommenden Aufgabe dieser Begriff zuordenbar ist.

Abs. 2 regelt in allgemeiner Form die Zulässigkeit von Analysedateien. Welche Analysedateien im konkreten Fall auf Grund dieser Bestimmung angelegt werden, geht aus dieser Regelung nicht hervor. Diesbezüglich ist für die Betroffenen keinerlei Transparenz gegeben. Es wird daher angeregt, analog zum Rechtsakt des Rates vom 3. November 1998 über die Durchführungsbestimmungen für die von Europol geführten Analysedateien zu Analysezwecken (Amtsblatt Nr. C vom 30. Jänner 1999 Seite 1 f) eine entsprechende Vorabüberprüfung der Analysedateien durch eine Rechtsschutzinstanz – etwa den Rechtsschutzbeauftragten – vorzusehen. Dieser Rechtsakt präzisiert die Vorgaben des Art. 10 Europolübereinkommens, welches wiederum als Vorbildregelung für den § 53a SPG gesehen werden kann.

Zu Abs. 2 Z 4 des § 53a SPG ist festzuhalten, dass die hier genannte Kontakt- oder Begleitpersonen nicht automatisch selbst kriminelle Handlungen begeht. Auch hinsichtlich eines zunächst „Verdächtigen“ (Abs. 2 Z 1) kann sich auf Grund weiterer Ermittlungen herausstellen, dass er in weiterer Folge als nicht mehr verdächtig gilt Zeigt sich, dass ein zunächst Verdächtigter oder eine Kontakt- oder Begleitperson

selbst nicht deliktisch handelt bzw. für den weiteren Verlauf von Ermittlungen nicht notwendigerweise im Visier der Behörden bleiben muss, sind Daten unverzüglich zu löschen. Dieser Ansatz kommt in der jetzigen Textierung nicht ausreichend zum Tragen. Es sollte daher eine Präzisierung bzw. einschränkendere Formulierung, die sich am Vorbild des Art. 6 Abs. 3 des oben zitierten Rechtsaktes für die von Europol geführten Analysedateien orientieren sollte, erfolgen.

Hinsichtlich der in § 53a Abs. 2 SPG vorgesehenen Speicherfrist von max. 5 Jahren ist anzumerken, dass diese Frist wiederum unverhältnismäßig lang erscheint. Demgegenüber sieht Art. 7 Abs. 3 des oben zitierten Rechtsaktes des Rates vom 3. November 1998 eine max. Speicherdauer von insgesamt drei Jahren vor. Diese beginnt mit dem Tag neu zu laufen, an dem ein Ereignis eintritt, das zur Speicherung von Daten zu der betreffenden Person führt […]. Eine entsprechende Anpassung an den zitierten Rechtsakt scheint geboten.

Zu Art. 1 Z 8 (§ 55a Abs. 4 SPG)

Hier darf angemerkt werden, dass ein Abstellen auf „Anhaltspunkte“, wonach ein Mensch nicht mehr vertrauenswürdig „sein könnte“ einen sehr großen Ermessensspielraum einzuräumen scheint.

Zu Art. 1 Z 13 (§ 58 d SPG)

Bei näherer Betrachtung der Funktionalitäten dieser neuen Datei zeigt sich, dass der Schwerpunkt ihrer Anwendung auf der erleichterten Aufklärung einschlägiger Straftaten liegt. Insofern erschiene es rechtssystematisch geboten, diese Datei in der Strafprozessordnung zu regeln. Dies würde auch eine entsprechende Klarstellung hinsichtlich der Kontrolle durch die Staatsanwaltschaft mit sich bringen.

Hinsichtlich der in dieser Datei gespeicherten Opferdaten ist anzumerken, dass die Notwendigkeit der Speicherung der genauen Wohnanschrift entbehrlich scheint (insbesondere etwa auch das Herunterbrechen auf Türbezeichnungen) und

jedenfalls zu keiner Anonymisierung der Opfer führt, was aber angesichts der bis zu 20 jährigen Speicherdauer dieser Daten wünschenswert wäre.

Zu Art. 1 Z 14 (§ 65 Abs. 1 SPG)

Es ist nicht ersichtlich, warum der nunmehr vorgeschlagene Wortlaut zu einer anderen Judikatur des Verwaltungsgerichtshofs führen sollte. Wird das Kriterium der „Persönlichkeit des Betroffenen“ herangezogen, ist selbstverständlich auch weiterhin eine einzelfallbezogene Prognose erforderlich.

Zu Art. 1 Z 16 (§ 65 Abs. 6 SPG)

In der 6. Zeile dieses Abs. 6 sollte deutlich gemacht werden, dass es sich bei den erkennungsdienstlichen Daten um die des Verdächtigen handelt.

Zu Art. 1 Z 18 (§ 75 Abs. 1 SPG)

Im Zusammenhang mit der hier angestrebten „Rationalisierung“ im Bezug auf die Verwendung erkennungsdienstlicher Daten ist zu betonen, dass eine solche nicht zu einem Verlust von Transparenz für die Betroffenen führen darf. Werden also beispielsweise von einer Person nach dem Fremdenpolizeigesetz Fingerabdrücke abgenommen und diese sowohl nach Fremdenpolizeigesetz als auch später nach SPG weiterverarbeitet, wäre sicherzustellen, dass der betreffenden Person eine entsprechende Mitteilung über diese Doppelverwendung zugeht. Legistisch wäre dies durch einen entsprechenden Verweis auf § 65 Abs. 5 SPG zu lösen.

Zu Art. 3 Z 1 (§ 7 Abs. 5 PolKG)

Der Entwurf sieht vor, dass künftig die Sicherheitsbehörden ermächtigt sein sollen, Amtshilfe durch das Verwenden von Daten, die von ausländischen Sicherheitsbehörden und Sicherheitsorganisationen in gemeinsam geführten Informationssammlungen verarbeitet werden, unmittelbar in Anspruch zu nehmen.

Der vorgeschlagene Abs. 5 des § 7 PolKG steht einmal in offenkundigem Widerspruch zu § 7 Abs. 1 PolKG. Zufolge Letzterer nehmen nachgeordnete Sicherheitsbehörden Amtshilfe im Wege des Bundesministers für Inneres in Anspruch. Davon abgesehen ist nicht ersichtlich, wie durch eine solche Norm sichergestellt werden soll, dass nicht etwa Exekutivorgane auf unüberprüfte bzw. unzuverlässige ausländische Informationen (etwa aus problematischen Drittstaaten ohne Überprüfungsmöglichkeit der Datenqualität) zurückgreifen. Den berechtigten Anliegen der Datenrichtigkeit, der Datenlöschung bzw. der Auskunft gegenüber Betroffenen kann durch eine solche rudimentäre Bestimmung ebenfalls nicht ausreichend Rechnung getragen werden.

Weiters wird zu dieser Bestimmung eine Überprüfung dahingehend angeregt, ob nicht in bestehenden völkerrechtlichen Verträgen Regelungen derart vorgesehen sind, dass Amtshilfe durch das Verwenden von Daten im Wege einer bestimmten Stelle bzw. Einrichtung in Anspruch zu nehmen ist. Bejahendenfalls würde die geplante Bestimmung in Widerspruch zu den völkerrechtlichen Verträgen stehen, da eine entsprechende Regelung betreffend unmittelbare Datenverwendung durch die Sicherheitsbehörden selbst zwar – innerstaatlich - entgegenstehenden Bestimmungen in Staatsverträgen auf Gesetzesstufe zu derogieren vermag, gegenüber den Vertragsparteien hätte eine Änderung jedoch grundsätzlich in Form der Abänderung des völkerrechtlichen Vertrages zu erfolgen.

1.Oktober 2007
Für den Datenschutzrat
Der Vorsitzende:
WÖGERBAUER

Elektronisch gefertigt