REPUBLIK ÖSTERREICH
DATENSCHUTZKOMMISSION

A-1010 Wien, Hohenstaufengasse 3
Tel. ++43-1-531 15/2525
Fax: ++43-1-531 15/2690
e-mail: dsk@dsk.gv.at
DVR: 0000027

GZ: DSK-K054.153/0004-DSK/2011

Begutachtung
Sicherheitspolizeigesetz et al

Bundesministerium für Inneres
Abteilung III/1

Herrengasse 7
1014 Wien

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

Betrifft: GZ BMI-LR1340/0005-III/1/2011 – Bundesgesetz, mit dem das Sicherheitspolizeigesetz, das Polizeikooperationsgesetz und das Bundesgesetz über die Einrichtung und Organisation des Bundesamtes zur Korruptionsprävention und Korruptionsbekämpfung geändert werden

Die Datenschutzkommission gibt zum gegenständlichen Entwurf, der ihr per E-Mail am 20. September 2011 übermittelt wurde, nachfolgende Stellungnahme ab:

I. Zu Z 1 und 2: § 10 Abs. 2 Z 5a und § 10 Abs. 7 SPG neu:

Die Datenschutzkommission begrüßt grundsätzlich eine gesetzliche Regelung zur Verwendungen von (sensiblen) personenbezogenen Daten. Allerdings ist die Prüfung der Eignung von Personen zur Aufnahme in den Bundesdienst eine Angelegenheit des Dienstrechts, die in die Zuständigkeit des Bundeskanzleramtes fällt (vgl. Anlage zu § 2 Teil 2 A.1 BMG).

Dennoch sei zur Regelung Folgendes angemerkt:

Bei personenbezogenen Daten, die im Rahmen einer (geistigen und/oder gesundheitlichen) Eignungsprüfung typischerweise verarbeitet werden, handelt es sich idR um sensible Daten (§ 4 Z 2 DSG 2000). ISd § 1 Abs. 2 DSG 2000 sollte daher schon im jeweiligen (dienstrechtlichen) Gesetz genau festgelegt sein, welche (sensiblen) Daten anhand welcher Untersuchungsmethoden von welcher Stelle ermittelt und weiter verarbeitet bzw. an wen übermittelt werden dürfen. Auch sollte festgelegt sein, dass diese Daten für andere Zwecke

als die Eignungsprüfung nicht verwendet werden dürfen. Auch sei hier auf die Regelung des Ausschreibungsgesetzes hingewiesen, die für Eignungstests in § 42 eine Pflicht zur Anonymisierung vorsieht.

Inhaltlich ist in § 10 Abs. 7 SPG neu vorgesehen, dass in den Fällen des Abs. 2 Z 5a (Feststellung der geistigen und körperlichen Eignung von Organen des öffentlichen Sicherheitsdienstes und Aufnahmewerbern in den Exekutivdienst) auch sensible Daten (§ 4 Z 2 DSG 2000) ermittelt und verarbeitet werden dürfen. Nur den Erläuterungen ist zu entnehmen, dass dies nur zulässig ist, „soweit sie zur Beurteilung der Eignung für den Exekutivdienst erforderlich sind."

Die Datenschutzkommission schlägt vor, diesen Passus als Einschränkung im Sinn eines verhältnismäßigen Eingriffs in das Grundrecht auf Datenschutz (§ 1 DSG 2000) direkt in den Gesetzestext aufzunehmen.

II. Zu Z 3 und 4: Entfall des § 13 Abs. 2; § 13a SPG neu:

Der Entwurf sieht vor, dass § 13 Abs. 2 SPG komplett entfällt und dafür ein neuer § 13a eingeführt wird. § 13 Abs. 2 enthielt zwei datenschutzrechtlich wesentliche, dem Gebote der Verhältnismäßigkeit eines Eingriffs in Grundrecht auf Datenschutz (§ 1 DSG 2000) erforderliche, Schranken für Kanzleiordnungen des Inneren Dienstes.

Zum Einen ist festgelegt, welche Datenarten grundsätzlich in solchen Kanzleiordnungen verarbeitet werden dürfen: „… Zu diesen Zwecken dürfen sie [Anm. die Sicherheitsbehörden] Daten über natürliche und juristische Personen sowie Sachen verwenden, auf die sich der zu protokollierende Vorgang bezieht, wie insbesondere Datum, Zeit und Ort, Fahrzeugdaten, Betreff und Aktenzeichen samt Bearbeitungs- und Ablagevermerken sowie Namen, Rolle des Betroffenen, Geschlecht, frühere Namen, Aliasdaten, Staatsangehörigkeit, Geburtsdatum, Geburtsort, Wohnanschrift und andere zur Erreichbarkeit des Menschen dienende Daten. Soweit es erforderlich ist, dürfen auch sensible Daten (§ 4 Z 2 DSG 2000) sowie Daten im Sinne des § 8 Abs. 4 DSG 2000 verwendet werden. …" Insbesondere der hier zuletzt genannte Satz bietet eine dem verfassungsrechtlichen Gebot der Verhältnismäßigkeit des Eingriffs ins Grundrecht auf Datenschutz erforderliche Schranke für sensible und strafrechtlich relevante Daten.

Zum anderen sieht § 13 Abs. 2 letzter Satz eine Zugriffsbeschränkung auf die in Kanzleiordnungen gespeicherten Daten vor: „… Die Auswählbarkeit von Daten aus der Gesamtmenge der gespeicherten Daten nur nach dem Namen und nach sensiblen Daten darf nicht vorgesehen sein, vielmehr ist für die Auswahl ein auf den protokollierten Sachverhalt bezogenes weiteres Datum anzugeben." Dazu führten die Erläuterungen zur

damaligen RV aus (bezogen auf BGBl I Nr. 2004/151): „… Die gesonderte Auswählbarkeit von sensiblen Daten in Bezug auf eine bestimmte Person aus der Gesamtmenge der Daten ist aber nicht zulässig. Ebenso wenig darf durch bloße Angabe eines Namens ohne zusätzliches Kriterium aus der Gesamtmenge der Daten ausgewählt werden. Sensible Daten dürfen nur in eingeschränktem Maße für die im Gesetz genannten Zwecke (Auffindbarkeit von Akten und der Nachvollziehbarkeit von Amtshandlungen) verwendet werden, etwa Gesundheitsdaten bei der Dokumentation von Einsätzen zur ersten allgemeinen Hilfeleistung (§ 19 SPG) oder Daten zur politischen Meinung eines Menschen im Zusammenhang mit einer entsprechenden gerichtlich strafbaren Handlung nach dem Verbotsgesetz. …“

Dies scheint offenbar nunmehr keine Rolle zu spielen, denn beide Schranken fallen nunmehr. „Der Regelungsgegenstand des § 13 Abs. 2 soll nunmehr in einem neu geschaffenen § 13a unter dem Titel „Dokumentation“ einer gesonderten Regelung unter Berücksichtigung der Judikatur des Verfassungsgerichtshofs zugeführt werden.“ (Erläuterungen)

Dieser § 13a sieht weder Vorgaben in Bezug auf die zulässigerweise zu verarbeitenden Daten vor – damit will man offenbar die Rechtslage an die Wirklichkeit des in Entwicklung befindlichen Systems PAD 2.0 anpassen. Noch sieht § 13a eine Einschränkung für die Zugriffsbefugnis auf die verarbeiteten Daten vor.

§ 13a Abs. 2 führt aus: „Die Akten im Dienste der Strafrechtspflege sind getrennt vom restlichen Aktenbestand zu führen, die Verwendung der kriminalpolizeilichen Daten ist nur nach Maßgabe der Strafprozessordnung 1975, BGBl. Nr. 631/1975, und für sicherheitspolizeiliche Zwecke gemäß § 53 Abs. 2 zulässig. Die Daten sind um Verständigungen zu Einstellungen, Freisprüchen und diversionellen Entscheidungen zu aktualisieren.“ Die Regelung in Satz 1 ist datenschutzrechtlich selbstverständlich und kann nur als Klarstellung gedeutet werden. Einschränkende Regelungen zur Verwendung sicherheitspolizeilicher Daten (als „Pendant“ zu kriminalpolizeilichen Daten) fehlen völlig.

Die Erläuterungen führen hiezu aus: „Auch im Hinblick darauf, dass eine Einschränkung der Auswählbarkeit, wie sie derzeit in § 13 Abs. 2 vorgesehen ist, eine geclearte Datenanwendung verhindert, wird von einer solchen Regelung in § 13a (neu) abgesehen.“ Nachdem der Begriff der „geclearten“ Datenanwendung der Rechtsordnung fremd ist und auch im gegebenen Zusammenhang nicht erklärt wird, ist dieser Satz unverständlich und wird, wenn man aus den genannten Gründen nicht vollständig von einer solchen Regelung absieht, näher auszuführen sein.

Schließlich sei darauf hingewiesen, dass auch der Verfassungsgerichtshof in seiner Judikatur zu § 13 Abs. 2 SPG (vgl. VfGH 16.12.2009, B298/09) die eingeschränkte Zugriffsbefugnis zumindest in Gestalt des § 13 Abs. 2 letzter Satz SPG als verfassungsrechtlich geboten erachtet.

Aus all diesen Gründen sieht die Datenschutzkommission die vorgeschlagene Regelung als nicht mit zulässigen Eingriffen des im Verfassungsrang stehenden Grundrecht auf Datenschutz (vgl. § 1 Abs. 2 DSG 2000) vereinbar und damit als verfassungswidrig an.

III. Zu Z 11 und 22: § 53 Abs. 1 Z 7 und § 63 Abs. 1a SPG neu:

Die vorgeschlagene Regelung des § 53 Abs. 1 Z 7 SPG neu schafft eine Ermächtigung zur Datenverarbeitung „für die Analyse und Bewertung des Bestehens einer Gefährdung der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit durch die Verwirklichung eines Tatbestandes nach dem Vierzehnten und Fünfzehnten Hauptstück des Strafgesetzbuches“.

Hier stellt sich zunächst die Frage, warum die in § 53a Abs. 2 SPG geregelte „Kriminalitätsanalyse“, die im Übrigen wesentliche detaillierter geregelt ist, nicht ausreicht bzw. weshalb überhaupt ein Bedarf nach der vorgeschlagenen Regelung besteht. Es steht zu befürchten, dass mit dieser neuen Regelung die Kriterien und Kontrollinstrumente (vgl. § 91c Abs. 2 SPG) des § 53a Abs. 2 SPG umgangen werden könnten, da § 53 Abs. 1 Z 7 SPG neu nach Ansicht der Datenschutzkommission vom Wortlaut her wesentlich eingriffsintensiver scheint. Es wäre daher in Erläuterungen darzulegen, inwiefern das vorgesehene Instrument neben der bestehenden „Kriminalitätsanalyse“ einen Anwendungsbereich hat und zumindest auch die Kontrollbefugnis des Rechtsschutzbeauftragten nicht nur durch Information, sondern durch seine vorangehende Ermächtigung vorzusehen.

Die vorgesehene, korrespondierende Löschungsverpflichtung in § 63 Abs. 1a SPG neu) besagt, dass Daten zu löschen sind, sobald die erfolgte Analyse eine Gefährdung „ausschließt“. Dies sei „jedenfalls“ dann der Fall, wenn binnen eines Jahres ab Beginn der Analyse keine weiteren Anhaltspunkte für deren Bestehen ermittelt werden können.

§ 1 Abs. 2 DSG 2000 (im Verfassungsrang) sieht vor, dass auch im Falle zulässiger Beschränkungen (des Grundrechts, zB durch ein formelles Gesetz) der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden darf. Die vorgeschlagene Regelung wird zunächst zu dem Ergebnis in der Praxis führen, dass auf Grundlage des § 53 Abs. 1 Z 7 SPG ermittelte Daten jedenfalls ein Jahr (ab Ermittlungszeitpunkt gerechnet) aufbewahrt werden, da eine Gefährdung nie ganz

„ausgeschlossen“ werden kann. Aber auch eine weitere Aufbewahrung – uU für sehr lange Zeiträume – nur auf der Basis, dass eine Gefährdung nicht ausgeschlossen werden kann, ist mit § 1 DSG 2000 nicht in Einklang zu bringen. Das DSG 2000 geht davon aus, dass für die Aufbewahrung von Daten ein konkreter Zweck anzugeben ist (vgl. § 6 Abs. 1 Z 2 und die §§ 7ff DSG 2000), im gegebenen Zusammenhang also für die Gefährdung konkrete Anhaltspunkte bestehen.

Bei der derzeitigen Fassung (insbes. auch des zweiten Satzes des § 63 Abs. 1a SPG neu) ist der Wortlaut geeignet, eine unbegrenzte Speicherung von Daten zu legitimieren, wenn die Behörde zur Auffassung gelangt und argumentiert, dass eine Gefährdung nicht ausgeschlossen werden kann – die bloße Vermutung wäre also ausreichend.

Die Datenschutzkommission schlägt daher vor, die Weiterverwendung der auf Basis des § 53 Abs. 1 Z 7 SPG neu ermittelten Daten an konkrete Anhaltspunkte einer Gefährdung zu knüpfen, andernfalls die Daten zu löschen sind.

IV. Zu Z 12: Änderung in § 53 Abs. 3b SPG:

Diese Regelung scheint durch den Entfall der Worte „von dem gefährdeten Menschen“ zu unbestimmt. Die Erläuterungen erklären zwar nachvollziehbar, warum diese Schranke entfernt wird.

Die Datenschutzkommission schlägt daher vor, im Gesetzestext enumerativ die Personenkreise, deren Standortdaten in diesem Fall ermittelt werden dürfen, aufzuzählen.

Im Übrigen ist auch nicht klar, wie dem Informationsgebot des § 24 DSG 2000 Rechnung getragen und damit die nachfolgende Verfolgung der Betroffenenrechte (§§ 26ff DSG 2000) ermöglicht werden soll. Auch das wäre im Gesetz klarzustellen.

Schließlich sollte auch klargestellt werden, dass im Hinblick auf gespeicherte Vorratsdaten die Ermittlungen von Standortdaten nur im engen zeitlichen Konnex zum zugrundeliegenden Ereignis stattfinden darf.

II. Eine Ausfertigung dieser Stellungnahme wurde dem Präsidium des Nationalrates im Wege elektronischer Post an die Adresse: begutachtungsverfahren@parlament.gv.at übermittelt.

21. Oktober 2011
Für die Datenschutzkommission
Der stellvertretende Vorsitzende:
Hofrat des OGH Hon.Prof. Dr. KURAS

Signaturwert	yl2UPTPxS5Y7ji044SXtJmuyWmh8+NY6o1rbTyLQAKhuW4ae8mi2UmgsoBmvZkXYk68 vjQ84TPua7B3yKZylKVKvqCKudUzFaCvem2XUNEtCZPPBuHc42VqLmdHb3i6cnE+0dW b1UXGrBkJ7LYVdxDnHpWkTdwJ6HH6PcQWcg5bjLTuHZczwHDY3EYHndG2j5+e79urZ0 srGgeEKZIcMsR/2/+r54Mkv/TCN5dGdabrE1ertqT05LI0E7elpRLXnxK4Q1PkIFSwb nAhH7BqBjYyuGmgaKGXFvEOMHzvzXjRM3P74U19EnpDtJ6uXvtn1cCuUFpwwy+LSIKZ BuVhY8g==	
	Unterzeichner	serialNumber=117229306313,CN=Amtssignatur Datenschutzkommission,O=Amtssignatur Datenschutzkommission,C=AT
	Datum/Zeit-UTC	2011-10-21T12:56:33+02:00
	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.	543759
	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	