REPUBLIK ÖSTERREICH DATENSCHUTZRAT

BALLHAUSPLATZ 2, A-1014 WIEN
GZ ● BKA-817.376/0002-DSR/2011
TELEFON ● (+43 1) 53115/2527
FAX ● (+43 1) 53115/2702
E-MAIL ● DSRPOST@BKA.GV.AT
DVR: 0000019

An das
Bundesministerium für Inneres

Per E-Mail:
bmi-III-7@bmi.gv.at

Betrifft: Entwurf der Bundesministerin für Inneres für ein Bundesgesetz, mit dem das Sicherheitspolizeigesetz, das Polizeikooperationsgesetz und das Bundesgesetz über die Einrichtung und Organisation des Bundesamtes zur Korruptionsprävention und Korruptionsbekämpfung geändert werden

Stellungnahme des Datenschutzrates

Der **Datenschutzrat** hat in seiner 210. Sitzung am 17. Oktober 2011 **einstimmig beschlossen**, zu den im Betreff angeführten Gesetzesentwürfen folgende Stellungnahme abzugeben:

1) Allgemeines:

Der vorliegende Entwurf für eine Novelle des Sicherheitspolizeigesetzes (SPG) enthält im Wesentlichen folgende datenschutzrechtlich relevante Regelungsinhalte:

- Schließung einer angeblichen Regelungslücke für die Datenverarbeitung bei Eignungsprüfungen für Aufnahmewerber in den Exekutivdienst durch seine Ermächtigung im SPG (§ 10 Abs. 2 Z 5a und Abs. 7);

- Neufassung der Rechtsgrundlage für die Datenverarbeitung im Kontext der Aktenverwaltung bzw. des inneren Dienstes der Polizei (§§ 13 und 13a SPG);

- beabsichtigte Stärkung der Terrorismusprävention durch die Ausweitung des Begriffs der sog. „Erweiterten Gefahrenerforschung“ auf das Beobachten von Einzelpersonen (§ 21 Abs. 3 SPG);

- Schaffung einer spezifischen Ermächtigung zur Datenverwendung für Zwecke der Abwehr bestimmter Gefahren für die verfassungsmäßigen Einrichtungen (§§ 53 Abs. 1 Z 7 und 63 Abs. 1a SPG);

- Ausweitung der Befugnis der Exekutive zur Handyortung über den Fall des Vermissten hinaus (§ 53 Abs. 3b SPG);

- Beitrag zum Opferschutz bei Identitätsmissbrauch durch Ermächtigung zur Verarbeitung von Lichtbild und Fingerabdrücken auf Ersuchen des Opfers (§§ 58 Abs. 1 Z 8, § 68 Abs. 1, § 73 Abs. 6, § 74 Abs. 3);

- Verbesserung der Zusammenarbeit der Sicherheitsbehörden mit den Jugendwohlfahrtsträgern in Angelegenheiten der Jugendfürsorge durch Ermöglichung von Direktzugriffe auf bestimmte sensible polizeiliche Daten für die Jugendwohlfahrtsträger (§ 58c Abs. 2 SPG);

- Erweiterung des Kreises staatlicher Organe, die in den Genuss von „Hintergrundinformationen“ kommen (§ 93a SPG).

2) Detailbemerkungen:

Die angesprochenen Änderungen des Sicherheitspolizeigesetzes geben Anlass zu nachstehenden Bemerkungen aus datenschutzrechtlicher bzw. -politischer Sicht.

Zu Art. 1 Z. 1 und 2 des Entwurfs (§ 10 Abs. 2 Z 5a und Abs. 7 SPG)

Inhalt des Änderungsvorschlags ist eine Ermächtigung der Polizeikommanden zur „Mitwirkung“ an Eignungsprüfungen für Bedienstete und Bewerber für Planstellen im Bereich des BMI sowie die entsprechende Ermächtigung zur Datenverwendung.

Das in den Erläuterungen angedeutete Regelungsbedürfnis wird in den Ausführungen der Erläuterungen aber nicht nachvollziehbar gemacht.

Die Prüfung der Eignung zur Aufnahme in den Bundesdienst gehört zu den Angelegenheiten des Dienstrechts. Hierfür sind die Regelungen des Dienstrechts einschlägig. Letztere fallen in die Zuständigkeit des Bundeskanzleramtes (vgl. Anlage zu § 2 Teil 2 A.1 BMG).

Diese dienstrechtlichen Regelungen – etwa das Ausschreibungsgesetz und das Beamten-Dienstrechtsgesetz – regeln ua. die Anforderungen an die körperliche und geistige Eignung von Aufnahmewerbern (Stichwort „Eignungsprüfung“). Bei der Aufnahme von neuen Bewerbern haben die Dienststellen des BMI insofern die genannten dienstrechtlichen Bestimmungen zu vollziehen. Einer spezifischen Ermächtigung zur „Mitwirkung“ – wie in § 10 Abs. 2 Z 5a neu SPG vorgesehen bedürfte es insofern gar nicht.

Eine eigenständige Ermächtigung zur Datenermittlung und -verarbeitung, wie sie in § 10 Abs. 7 neu SPG vorgesehen werden soll, ist wiederum verfehlt, da auch die Erstellung, Durchführung und Auswertung von Tests uä. im Dienstrecht (va Ausschreibungsgesetz) geregelt ist.

Die Erläuterungen können auch nicht erklären, warum es **derzeit** für die gesundheitliche und psychologische Eignungsprüfung bei der Aufnahme in die exekutivdienstliche Ausbildung keine gesetzliche Grundlage gibt (und weshalb einschlägige Tests derzeit somit generell datenschutzrechtlich unzulässig wären).

Die in den Erläuterungen zitierte Entscheidung der Datenschutzkommission hat eine gesundheitliche Untersuchung und die damit verbundene Ermittlung von Gesundheitsdaten als zulässig angesehen. Dabei war eine Vorschrift des Niederösterreichischen Vertragsbedienstetengesetzes relevant, die von der Datenschutzkommission als **ausreichende** gesetzliche Grundlage für eine Gesundheitsuntersuchung durch einen von der Dienstbehörde beauftragten Arzt angesehen wurde. Aus den Erläuterungen geht daher nicht hervor, warum die entsprechenden Regelungen des **Dienstrechts des Bundes** derzeit nicht ausreichend sind, um grundsätzlich als Grundlage für Untersuchungen von Bewerbern herangezogen zu werden.

Schließlich ist noch auf Folgendes hinzuweisen: Bei den personenbezogenen Daten, die im Rahmen einer (gesundheitlichen oder geistigen) Eignungsprüfung typischerweise erhoben werden können, handelt es sich um höchst sensible Daten. Bei einer Ermächtigung zur Verarbeitung solcher Daten sollte vor diesem Hintergrund daher **schon im jeweiligen dienstrechtlichen Gesetz** (nicht erst im Verordnungsweg) genau festgelegt werden, **welche Daten** anhand **welcher Untersuchungsmethoden** von welcher Stelle ermittelt werden dürfen, dass diese Daten für keine anderen Zwecke verwendet werden dürfen, in welchem Umfang Untersuchungsergebnisse wem bekannt gegeben werden dürfen und schließlich wann und inwiefern sie in der Folge zu anonymisieren oder zu vernichten sind. Das Ausschreibungsgesetz sieht etwa für die darin geregelten Eignungstests eine Pflicht zur Anonymisierung vor (§ 42 leg.cit.).

Zu Art. 1 Z 4 des Entwurfs (§ 13a SPG)

Inhalt des Änderungsvorschlags ist eine neue gesetzliche Grundlage für die Aktenverwaltung durch die Sicherheitsbehörden.

Nach derzeitiger Rechtslage ist bei der gesetzlichen Grundlage für Aktenverwaltung der Sicherheitsbehörden (§ 13a Abs. 2 SPG) aus Gründen des Datenschutzes eine ausdrückliche Schranke mit folgendem Wortlaut eingezogen:

„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“

Diese gesetzliche Schranke hat der Verfassungsgerichthof in seinem Erkenntnis vom 16.12.2009, B 298/09 (VfSlg. 18.963/2009) als Voraussetzung für die Verhältnismäßigkeit der Speicherung von personenbezogenen Daten in der kriminalpolizeilichen Aktenverwaltung angesehen.

Mit der Entfernung dieser Schranke droht die Speicherung in Aktendokumentationssystemen insofern verfassungsrechtlich unzulässig zu werden.

Die vorgeschlagene Entfernung dieser Schranke wird in den Erläuterungen nicht ausreichend begründet:

Die vorgesehene Trennung zwischen „kriminalpolizeilichen Daten“ und „sonstigem Aktenbestand“ ist keine Maßnahme, die eine Beschränkung der Zugänglichkeit bzw. automatisierten Durchsuchbarkeit der elektronischen Akten etwa anhand des Namens Betroffener verhindert. Entgegen den Erläuterungen kann diese Trennung allein daher kein „Regulativ zur Wahrung der Verhältnismäßigkeit“ bilden.

Was die Erläuterungen mit dem Begriff einer „geclearten“ Datenanwendung meinen, ist im Übrigen nicht ersichtlich.

Regelungstechnisch geht es im gegebenen Kontext darum, die Schranken der Auswählbarkeit von Daten so zu umschreiben, dass ein fairer **Ausgleich** erreicht wird zwischen

- dem legitimen Bedürfnis nach Dokumentation und Auffindbarkeit von Akten im Anlassfall einerseits

- und dem Schutz des Einzelnen vor illegitimer Durchsuchung des gesamten Aktenbestands mit seinem Namen oder anderen Suchkriterien (Extrembeispiel: automatisierte Durchsuchung des gesamten Aktenbestands mittels einer – auch den Akteninhalt erfassenden Volltextsuche nach Namen oder anderer personenbezogener Kriterien).

Darüber hinaus muss die Regelung dem Prinzip folgen, dass Daten, die keine sicherheitspolizeiliche Relevanz für den Zweck der Verarbeitung mehr haben, gelöscht werden. Gegenüber der geltenden Rechtslage sollte keine Verschlechterung aus Sicht der Betroffenen herbeigeführt werden.

Dieser Ausgleich müsste im Gesetzestext selbst seinen Niederschlag finden. Die vorgeschlagene gesetzliche Regelung trägt nach Ansicht des Datenschutzrates diesem gebotenen Ausgleich nicht Rechnung.

Der Datenschutzrat regt daher an, das Spannungsverhältnis zwischen der Zugriffsmöglichkeit der Behörde zu dem relativ großen Spielraum der Abfragemöglichkeiten (Name und weiteres Datum) zu überprüfen, und fordert diesbezüglich geeignete Regelungen.

Zu Art. 1 Z 6 des Entwurfs (§ 21 Abs. 3 SPG neu)

Der Vorschlag zielt auf eine Ausdehnung der „erweiterten Gefahrenerforschung“ auf Einzelpersonen ab.

Die Ausweitung der sicherheitspolizeilichen Aufgabe der „erweiterten Gefahrenerforschung“ auf Einzelpersonen wirft Fragen aus demokratiepolitischer Sicht und Fragen hinsichtlich der Wahrung der Grundsätze eines liberalen Rechtsstaats auf.

Die vorgeschlagene Regelung würde insbesondere die im Sicherheitspolizeigesetz vorgesehenen Eingriffsmaßnahmen der verdeckten Ermittlung gegen Einzelpersonen richten, die in der einen oder anderen Weise „auffällig“ geworden sind. Es ist aber fraglich, ob die beabsichtigten Instrumente überhaupt eingesetzt werden können, ohne dass regelmäßig auch Personen von Eingriffsmaßnahmen betroffen sind, die sich zwar „auffällig“ verhalten haben, sich aber nicht (!) kriminell betätigen.

Wesentliche Voraussetzung für die Anwendung der „erweiterten Gefahrenerforschung“ auf Einzelpersonen soll sein, ob mit einer schweren Gefahr für die öffentliche Sicherheit „zu rechnen“ ist. Dieses relativ unbestimmte Kriterium wirft schwierige Auslegungsfragen auf. So stellt sich die Frage, ab welcher Schwelle von Verdachtsmomenten in der Praxis das Vorliegen dieses Kriteriums bejaht werden kann. **Bei grundrechtskonformer Auslegung dieser Regelung wird man dieses Kriterium zweifelsfrei dann bejahen können, wenn eine Person schon so weit aktiv geworden ist, dass sie der Straftat schon so nahe ist, dass das Stadium der versuchten Straftat bereits erreicht ist.**

Nach der strafrechtlichen Definition des Versuchs (§ 15 StGB) liegt der Versuch einer Straftat dann vor, wenn der Täter eine der Ausführung unmittelbar vorangehende Handlungen mit einem auf die Vollendung gerichteten Vorsatz setzt. Diese relativ

weite Definition des Versuchs im strafrechtlichen Sinn bewirkt aber, dass die Situationen, die durch die Einbeziehung von Einzelpersonen in die „erweiterte Gefahrenerforschung“ erfasst werden, ohnehin bereits in den Bereich normaler kriminalpolizeilicher Ermittlungen reichen und daher unter das Regime der Strafprozessordnung fallen!

Umgekehrt birgt die vorgeschlagene Regelung bei zu großzügiger Auslegung die Gefahr in sich, dass die Rechtsschutzgarantien der Strafprozessordnung (Richtervorbehalt, Staatsanwaltschaftsvorbehalt, etc) durch den Einsatz von Mitteln der Sicherheitspolizei unterlaufen werden.

Zu Art. 1 Z 11 und Z 22 des Entwurfs (§ 53 Abs. 1 Z 7 SPG neu und § 63 Abs. 1a SPG neu)

Der vorgeschlagene § 53 Abs. 1 Z 7 SPG bewirkt die Schaffung einer 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*“.

Den Erläuterungen zufolge soll diese Vorschrift dazu dienen, dass Sicherheitsbehörden mithilfe von Informationen, die ihnen zur Verfügung gestellt werden, eine „Analyse und Bewertung zur Feststellung einer Gefährdung der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit“ vornehmen. Die den Sicherheitsbehörden von außen zugekommenen Daten sollen insofern verarbeitet werden „als sie **mit Informationen aus offenen Quellen und vorhandenem Organisationswissen abgeglichen sowie strukturiert analysiert** und bewertet werden dürfen“. Diese Analyse hat den Erläuterungen zufolge „umgehend nach Ermittlung“ (Empfang) der empfangenen Daten zu erfolgen.

Die im Zusammenhang damit vorgeschlagene Löschungsverpflichtung besagt, dass die Daten zu löschen sind, sobald die erfolgte Analyse eine Gefährdung „ausschließt“ (§ 63 Abs. 1a erster Satz SPG neu). Nach dem zweiten Satz des vorgeschlagenen § 63 Abs. 1a ist eine solche Gefährdung „jedenfalls dann auszuschließen“, wenn

binnen eines Jahres ab Beginn der Analyse keine weiteren Anhaltspunkte für deren Bestehen ermittelt werden können“.

Zu der vorgeschlagenen Regelung ist anzumerken, dass eine Gefährdung nie gänzlich „ausgeschlossen“ werden kann. **Eine weitere Speicherung personenbezogener Daten allein auf Basis der Annahme, dass eine „Gefährdung nicht ausgeschlossen“ werden kann, wäre mit der Zielrichtung des Grundrechts auf Datenschutz aber nicht vereinbar.**

Auch während der vorgesehenen Jahresfrist sollten daher personenbezogene Daten nur solange gespeichert werden, als eine Gefährdung nicht bloß „nicht ausgeschlossen“, sondern aufgrund besonderer Anhaltspunkte für wahrscheinlich zu halten ist. Die vorgeschlagene Formulierung stellt dies nicht sicher. Eine Speicherung allein aufgrund des negativen Definitionsmerkmals „nicht ausgeschlossen“, wäre daher unverhältnismäßig. Daran ändert auch der Umstand nichts, dass der zweite Satz des vorgeschlagenen § 63 Abs. 1a SPG den Ausschluss einer Gefährdung gesetzlich fingiert, wenn nach Ablauf eines Jahres „nach Beginn der Analyse“ keine zusätzlichen Anhaltspunkte hervorgekommen sind.

Im Übrigen geht auch der zweite Satz der Bestimmung sehr weit. Er lässt die nach dem Grundrecht auf Datenschutz gebotene Löschung beinahe zum Ausnahmefall werden: Dieser Satz führt dazu, dass sämtliche Daten, die der Analyse zugrunde gelegt wurden (also zB sämtliche Daten, die von einer ausländischen Behörde zur Verfügung gestellt wurden) weiter aufbewahrt werden, sobald innerhalb eines Jahres ein zusätzlicher Anhaltspunkt hervorkommt, der für eine vermutete Gefährdung spricht. **Der im Ministerialentwurf vorgeschlagene Wortlaut ist daher geeignet, eine unbegrenzte Speicherung von Daten zu legitimieren, auch wenn nur eine Vermutung einer Gefährdung gegeben war, die durch einen weiteren Anhaltspunkt ergänzt werden konnte.**

Inhaltlich gesehen handelt es sich bei der vorgeschlagenen Datenverwendungsbefugnis um einen Sonderfall der bestehenden Regelung der „Kriminalitätsanalyse“ im Sinne des § 53a Abs. 2 SPG und, da die zulässigen Datenarten in der vorgeschlagenen Regelung nicht näher definiert werden,

womöglich sogar um eine noch eingriffsintensivere Maßnahme als jene der „Kriminalitätsanalyse“.

Die mit der SPG-Novelle 2007 eingeführte Maßnahme der „Kriminalitätsanalyse“ besteht darin, dass personenbezogene Daten strukturiert und anhand vorhandener Daten der Sicherheitsbehörden ausgewertet werden, zum Zweck der Abwehr oder Vorbeugung gefährlicher Angriffe. Dies schließt auch jenen Bereich der Kriminalität ein, der unter die hier angesprochenen Hauptstücke Vierzehn und Fünfzehn des Strafgesetzbuches fällt.

Es stellt sich daher zunächst die Frage, weshalb überhaupt Bedarf nach einer neuen Regelung in diesem Bereich gegeben sein sollte, wenn ohnehin das Instrument der „Kriminalitätsanalyse“ nach § 53a Abs. 2 SPG existiert.

Außerdem ist zu fragen, ob die Neuregelung nicht dazu führt, dass die Kontrollinstrumente ausgehöhlt werden, die derzeit für die Durchführung einer „**Kriminalitätsanalyse**“ gelten. Nach geltendem Recht darf nämlich der Einsatz einer solchen „**Kriminalitätsanalyse**“ nur dann stattfinden, wenn der Rechtsschutzbeauftragten befasst wurde (§ 91c Abs. 2 SPG). Die Verfassungsbestimmung des § 91a Abs. 3 SPG sichert die Befugnisse des Rechtsschutzbeauftragten im Interesse des Datenschutzes ab und erlaubt eine Einschränkung seine Befugnisse nur unter der Voraussetzung einer Zwei-Drittel-Mehrheit.

Da die Einführung einer Analyse nach dem vorgeschlagenen Modell einen Sonderfall der „**Kriminalitätsanalyse**“ darstellt, für die derzeit eine Kontrollbefugnis des Rechtsschutzbeauftragten besteht, wäre auch hier zumindest vorzusehen, dass der Rechtsschutzbeauftragte zu befassen ist. Aufgrund der Eingriffsintensität und der vergleichsweise geringen Dichte der Definition zulässiger Datenarten erscheint es nicht ausreichend, eine bloße Information des Rechtsschutzbeauftragten vorzusehen. Stattdessen erscheint es notwendig, die Maßnahme an seine vorherige Ermächtigung zu binden.

Der Datenschutzrat hält dazu fest, dass die informierten Vertreter des BMI zugesichert haben, dass die Bestimmung novelliert und insbesondere die

vorgeschlagene Löschungsbestimmung klarer gefasst wird und der Rechtsschutzbeauftragte befasst werden muss.

Zu Art. 1 Z 13 und Art. 2 des Entwurfs (§ 53 Abs. 3b SPG):
Die Änderung betrifft die sogenannte „Handyortung“, das heißt die den Sicherheitsbehörden zukommende Befugnis, von Telekom-Betreibern Auskunft über Standortdaten eines Kunden zu verlangen, der in Gefahr ist.

Die vorgeschlagene Änderung besteht darin, die Wortfolge **„von dem gefährdeten Menschen“** zu streichen. Damit soll es den Sicherheitsbehörden - den Erläuterungen zufolge - ermöglicht werden, die Beauskunftung von Standortdaten bzw. die sogenannte „Handyortung“ auch in solchen Fällen durchzuführen, in denen das Endgerät (zB Mobiltelefon) vermutlich nicht von der gefährdeten Person selbst mitgeführt wird, sondern von einem (einer) Begleiter(in) dieser Person. Der Anwendungsbereich der Eingriffsmaßnahme wird also auf nicht gefährdete, unbeteiligte Personen erweitert, von deren Standort man sich Aufschlüsse auf den Aufenthaltsort der gefährdeten Person erhofft.

Der Datenschutzrat regt daher an, dass in der gegenständlichen Regelung zum Ausdruck gebracht wird, dass die Maßnahme nicht gegen Unbeteiligte angewendet werden darf, sondern nur gegen Personen, die die gefährdete Person tatsächlich begleiten.

Darüber hinaus ist auf Folgendes hinzuweisen: Mit der Ausweitung des Anwendungsbereichs der Regelung tritt einer ihrer schon bestehenden Mängel noch schärfer zutage: **Die gebotene Information des Betroffenen und entsprechender Rechtsschutz.**

Nach der Rechtslage in der Fassung der letzten SPG-Novelle (BGBl I 33/2011, In-Kraft-Treten am 1.4.2012) ist nämlich eine verpflichtende Information des Betroffenen (durch die Sicherheitsbehörde) **nur dann** vorgesehen, wenn für die Standortabfrage „die Verwendung von Vorratsdaten erforderlich war“ (§ 53 Abs. 3c SPG). Diese Einschränkung der Informationspflicht ist nicht verständlich, weil das Bedürfnis des Betroffenen, von einem Eingriff in sein Datenschutzgrundrecht **unabhängig davon**

besteht, ob vor der Standortfeststellung auf Vorratsdaten zurückgegriffen werden musste oder ob die Standorterfassung ohne Rückgriff auf Vorratsdaten stattfindet.

Es mag sein, dass es technisch Schwierigkeiten bereitet, zu unterscheiden, ob der Telekommunikationsbetreiber die Auskunft unter Rückgriff auf Vorratsdaten beantworten wird oder unter Rückgriff auf Daten, die er unabhängig von seiner nach dem TKG bestehenden Pflicht zur Speicherung von Vorratsdaten (§ 102a TKG) aufbewahrt. Entscheidend ist, dass die derzeitige **Rechtslage** ausdrücklich an diese Unterscheidung anknüpft (§ 53 Abs. 3c SPG) und dass sie die Informationspflicht nur dann vorsieht, wenn auf Vorratsdaten zurückgegriffen wurde (so ausdrücklich der vierte Satz des § 53 Abs. 3c SPG in der Fassung BGBl I 33/2011). Diese Einschränkung der Informationspflicht sollte bereinigt werden.

Der Datenschutzrat weist ausdrücklich darauf hin, dass nur in jenen Fällen auf Vorratsdaten zurückgegriffen werden darf, in denen die notwendigen Daten nicht mehr als Verrechnungsdaten zur Verfügung stehen. Für diesen Zweck dürfen nur möglichst zeitnahe Daten mit aktuellem Bezug verwendet werden. Diese Maßnahme darf nämlich nur eingesetzt werden, wenn aufgrund „bestimmter Tatsachen anzunehmen ist, dass eine gegenwärtige Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen besteht“.

Im Zusammenhang mit der „Handyortung“ für Zwecke der internationalen polizeilichen Amtshilfe ist auf Folgendes hinzuweisen. Der Entwurf schlägt vor, das Polizeikooperationsgesetz (PolKG) dadurch zu ergänzen, dass in der Vorschrift, die regelt, welche Maßnahmen der Ermittlung von Daten zum Zweck der Leistung von Amtshilfe zulässig sind (§ 5 PolKG) unter anderem auch auf das Instrument der „Handyortung“ verwiesen wird.

Dabei ist aber fraglich, ob die gewählte Regelungstechnik nicht zu einem überschießenden Ergebnis führt: Da die vorgeschlagene Änderung des § 5 PolKG einen pauschalen Verweis auf § 53 Abs. 3a, 3b und 3c aufweisen soll, wird die Neuregelung dazu führen, dass im Rahmen der internationalen Amtshilfe **auch die Standortdaten** an den ersuchenden Staat ermittelt werden könnten, nicht nur die IMSI-Daten. Im Fall der grenzüberschreitenden Zusammenarbeit wird aber nur der

Austausch von IMSI-Daten erforderlich sein – die konkrete Ortung einer konkreten Person zur Hilfeleistung oder Abwehr der „gegenwärtigen Gefahr für das Leben, die Gesundheit oder die Freiheit“ wird sodann ohnehin auf Grundlage des Sicherheitspolizeigesetzes erfolgen müssen, und zwar ohne dass die Standortdaten ihrerseits nochmals Gegenstand der Übermittlung ans Ausland sind. Dasselbe gilt für den umgekehrten Fall eines von Österreich ausgehenden Ersuchens (auch hier wird nur die Übermittlung der IMSI-Nummer an den anderen Staat erforderlich sein).

Zu Art. 1 Z 17 des Entwurfs (§ 57 Abs. 1 SPG neu):

§ 57 SPG ist die Grundlage für alle wesentlichen Datenanwendungen der Sicherheitsbehörden. Die vorgeschlagene Bestimmung soll bewirken, dass die Datenkategorien, die im Rahmen der in § 57 SPG geregelten Datensammlungen erarbeitet werden dürfen, ergänzt werden durch

- die Speicherung eines Lichtbilds der betroffenen Person und
- die Speicherung eines Hinweises auf allfällige bereits vorhandene erkennungsdienstliche Daten (§ 75 Abs. 1 SPG).

Schon die derzeit geltende Regelung bringt den bei der konkreten Anwendung zu beachtenden Verhältnismäßigkeitsgrundsatz nicht zum Ausdruck, sondern deutet angesichts der undifferenzierten Formulierungsweise in die Richtung, dass sämtliche Datenkategorien für jede einzelne der in § 57 Abs. 1 Z 1 bis 12 SPG genannten Anwendungen gespeichert werden dürften, ohne jegliche Rücksichtnahme darauf, ob die einzelne Datenkategorie (zB das Datum „Namen der Eltern“) im Zusammenhang mit dem Zweck der jeweils in Betracht kommenden Datensammlung erforderlich ist. Diese Problematik verschärft sich durch die oben angesprochene Novellierung.

Es wird zwar geboten sein, die Regelung unter Rückgriff auf verfassungsrechtliche Grundsätze anders zu interpretieren, doch sollte bereits der Wortlaut des einfachen Gesetzes klar und deutlich zu erkennen geben, dass die Datenspeicherung dem **Erforderlichkeitsgrundsatz** gehorchen muss. Eine Neuformulierung des Abs. 1 könnte sich an der aktuellen Formulierung des Abs. 2 anlehnen, der die folgende Wendung enthält: „sofern die für die Erreichung des Zwecks der Datenverarbeitung erforderlich ist“, etwa in der Weise, dass der Abs. 1 des § 57 mit den folgenden Worten eingeleitet wird: „Soweit dies jeweils für die Erreichung des Zweckes der Datenanwendung erforderlich ist, dürfen die Sicherheitsbehörden …“.

Zu Art. 1 Z 21 des Entwurfs (§ 58c Abs. 2 SPG neu):

Hier ist anzumerken, dass insbesondere aus dem Argument der Erforderlichkeit (Gefährdungsabklärung), aber auch aus Datensicherheitsgründen eine Übermittlung sensibler Polizeidaten nur an behördliche Einrichtungen der Jugendwohlfahrt verantwortbar erscheint. Da es auch sog. freie Jugendwohlfahrtsträger (va. private Vereine) gibt, denen bestimmte Betreuungsaufgaben übertragen werden, bedarf es der Klarstellung, dass als Adressaten der Informationen iSd § 58c Abs. 2 ausschließlich staatliche Stellen der Jugendwohlfahrt in Betracht kommen (BezVwBH, LReg). Darüber hinaus sind auch offene kompetenzrechtliche Fragen zur Regelung einer Datenübermittlung noch zu klären.

Der Datenschutzrat merkt grundsätzlich an, dass die Daten ausschließlich an behördliche Einrichtungen der Jugendwohlfahrt, nicht jedoch an private Einrichtungen übermittelt werden dürfen.

Zu Art. 1 Z 37 des Entwurfs (§ 91c Abs. 1 SPG)

Es dürfte ein legistisches Versehen sein, dass der Vorschlag bei den Verpflichtungen der Sicherheitsbehörden zur vorherigen Information des Rechtsschutzbeauftragten (§ 91c Abs. 1 SPG) im Fall von Observations- und Ermittlungsmaßnahmen zur erweiterten Gefahrenerforschung, insbesondere des § 54 Abs. 2 SPG (Observation), zwar ausdrücklich auch die Geltung des Absatzes 3 des § 91c SPG vorsieht (Pflicht zur Einholung der Ermächtigung des Rechtsschutzbeauftragten), dass aber im genannten Absatz 3 diese Norm nicht noch einmal genannt wird:

Der Datenschutzrat weist darauf hin, dass von den informierten Vertretern zugesichert wurde, dass legistische Klarheit hergestellt wird. Zu diesem Zweck sollte daher nicht nur im Absatz 1 des § 91c SPG eine Ergänzung durch den Verweis auf den geschaffenen § 54 Abs. 2a SPG erfolgen, sondern auch im Absatz 3.

Zu Art. 1 Z 40 des Entwurfs (§ 93a Abs. 1 SPG)

Die Erläuterungen zu dieser Bestimmung nehmen Bezug auf die sicherheitspolizeiliche Aufgabe des „Schutzes der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit“. Diese Aufgabe ist in § 21 Abs. 1 Z 2

SPG genannt. Mit diesem Hinweis erwecken die Erläuterungen den Eindruck, dass die „Regierungsinformation“ nach § 93a SPG (nunmehr „Information verfassungsmäßiger Einrichtungen“) eine Aufgabe ist, die zu den Aufgaben auf dem Gebiet der „Sicherheitspolizei“ im Sinne des 2. Teils des SPG gehört. Wäre dem so, so müsste gefragt werden, ob und mit welchen Eingriffsbefugnissen diese Aufgabe verbunden ist. Beachtet man die parlamentarischen Materialien zur Regelung der „Regierungsinformation“ nach § 93a SPG, wird aber deutlich, dass es sich ihrem Konzept nach um keine Aufgabe der Sicherheitspolizei handelt (so dass sie auch nicht mit sicherheitspolizeilichen Eingriffsbefugnissen verbunden sein kann). Die Materialien besagen in diesem Zusammenhang Folgendes: *„Die Verpflichtung des Bundesministers für Inneres und der Sicherheitsdirektionen zur Regierungsinformation unter den Gesichtspunkten der Sicherheitsverwaltung soll ermöglichen, daß der in hohem Maße auf Informationsgewinnung angelegte Apparat der Sicherheitsbehörden nicht nur diesen selbst zugute kommt. Bei der Regierungsinformation handelt es sich nicht um eine sicherheitspolizeiliche Aufgabenstellung im eigentlichen Sinne, vielmehr werden hier Sicherheitsbehörden im Interesse der Unterstützung von Regierungsmitgliedern bei der Erfüllung von deren gesetzlichen Aufgaben in die Pflicht genommen. Nach Maßgabe ihres Wissens sollen der Bundesminister für Inneres und die Sicherheitsdirektionen auch verpflichtet sein, Regierungsmitglieder vor Schritten zu bewahren, die dem Ansehen des Staates Schaden zufügen würden. Eine Ermittlung personenbezogener Daten zur Erfüllung der Verpflichtung zur Regierungsinformation ist nur aus offenen Quellen erlaubt; eine Datengewinnung mit den Mitteln einer verdeckten Ermittlung oder einer Observation mithin unzulässig.“*

Zu empfehlen ist daher, dies in den Erläuterungen entsprechend klarzustellen.

Zusammenfassende Schlussfolgerungen:

Der Datenschutzrat

- hält die beabsichtigte Erlassung einer Ermächtigung zur Datenverwendung in § 10 SPG für Zwecke der Verwaltung der Aufnahme in den Bundesdienst und der Personalverwaltung für 1. systematisch verfehlt und 2. im inhaltlichen

- lehnt die Beseitigung der Daten-Verwendungsbeschränkung in § 13a Abs. 2 (letzter Satz) SPG ab, fordert eine Regelung der polizeilichen Aktenverwaltung, die einen sachgerechten Ausgleich zwischen dem Akten-Dokumentationszweck einerseits und dem Löschungsrecht des Betroffenen andererseits herstellt (Löschungsfristen, Verwendungsbeschränkungen) und erinnert, dass eine solche Regelung vom Grundsatz geleitet sein muss, dass Daten zu löschen sind, sobald kein legitimer Zweck ihrer Speicherung mehr gegeben ist;

- befürchtet, dass die Ausdehnung der Fälle der „erweiterten Gefahrenerforschung“ dazu führen kann, dass unter dem Titel der vorbeugenden Kriminalitätsbekämpfung staatliche Eingriffsbefugnisse zum Einsatz kommen, ohne dass sie der Strafprozessordnung gleichwertigen Kontrollinstrumenten (Instanz mit gleichen Unabhängigkeitsgarantien wie ein Gericht, Information des Betroffenen) unterstellt sind;

- fordert, dass der Einsatz des Instruments der „Analyse“ nach dem vorgeschlagenen § 53 Abs. 1 Z 7 SPG zumindest unter einen Genehmigungsvorbehalt durch den Rechtsschutzbeauftragten gestellt wird, und dass die einschlägigen Löschungsverpflichtungen (§ 63 Abs. 1a SPG) klarer formuliert werden;

- fordert die Festlegung einer klaren Pflicht zur Information der Betroffenen nach Einsatz einer Standortbestimmung nach § 53 Abs. 3b SPG, uzw. in sämtlichen Fällen (dh. nicht nur im Fall des Rückgriffs auf Vorratsdaten);

- regt im Hinblick auf die Standortbestimmung an, dass geprüft werden soll, ob es ausreichend ist, dass die IMSI-Daten übermittelt werden, und deswegen weitere Änderungen im PolKG erforderlich sind;

- verlangt eine klarere Formulierung der vorgeschlagenen Änderung des § 57 Abs. 1 SPG (neu) im Lichte des Grundsatzes, dass nur im Fall der Erforderlichkeit für den Zweck der jeweiligen Datenanwendung Lichtbilderdaten und/oder Hinweise auf vorhandene erkennungsdienstliche Daten zu speichern sind;

- merkt zu den Adressaten der Informationen iSd § 58c Abs. 2 SPG an, dass die Daten ausschließlich an behördliche Einrichtungen der Jugendwohlfahrt, nicht jedoch an private Einrichtungen übermittelt werden dürfen;

- fordert hinsichtlich der Befugnis zum Einsatz der Mittel nach § 54 Abs. 2a SPG die legistische Klarstellung der Pflicht zur Einbindung des Rechtsschutzbeauftragten auch im Absatz 3 des § 91c SPG;

- fordert die Klarstellung, dass die „Information verfassungsmäßiger Einrichtungen“ ausschließlich mittels offenen Quellen stattfinden darf und keine Aufgabe der Sicherheitspolizei darstellt.

21. Oktober 2011
Für den Datenschutzrat
Der Vorsitzende:
MAIER

Elektronisch gefertigt