BM.I REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
SEKTION III-RECHT

GZ.: BMI-LR1420/0011-III/1/a/2008 Wien, am 21. Mai 2008

An das

Präsidium des
Nationalrates

Parlament
1017 W I E N

Rita Ranftl
BMI - III/1 (Abteilung III/1)
Herrengasse 7, 1014 Wien
Tel.: +43 (01) 531262046
Pers. E-Mail: Rita.Ranftl@bmi.gv.at
Org.-E-Mail: BMI-III-1@bmi.gv.at
WWW.BMI.GV.AT
DVR: 0000051
Antwortschreiben bitte unter Anführung der GZ an die Org.-E-Mail-Adresse.

Betreff: Legistik und Recht; Fremdlegistik; BG-BKA
Entwurf eines Bundesgesetzes, mit dem das Bundesgesetz über den Schutz personenbezogener Daten geändert wird (DSG-Novelle 2008),
Stellungnahme des Bundesministeriums für Inneres

In der Anlage wird zu dem im Betreff bezeichneten Entwurf die Stellungnahme des Bundesministeriums für Inneres übermittelt.

Beilage

Für den Bundesminister:

Mag. Sabine Halbauer

elektronisch gefertigt

BM.I REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
SEKTION III-RECHT

GZ.: BMI-LR1420/0011-III/1/a/2008 Wien, am 21. Mai 2008

An das

Bundeskanzleramt-Verfassungsdienst

Ballhausplatz 2
1014 W I E N

Zu Zl. BKA-810.026/0002-V/2/2008

Rita Ranftl
BMI - III/1 (Abteilung III/1)
Herrengasse 7, 1014 Wien
Tel.: +43 (01) 531262046
Pers. E-Mail: Rita.Ranftl@bmi.gv.at
Org.-E-Mail: BMI-III-1@bmi.gv.at
WWW.BMI.GV.AT
DVR: 0000051
Antwortschreiben bitte unter Anführung der GZ an die Org.-E-Mail-Adresse.

Betreff: Legistik und Recht; Fremdlegistik; BG-BKA
Entwurf eines Bundesgesetzes, mit dem das Bundesgesetz über den Schutz personenbezogener Daten geändert wird (DSG-Novelle 2008);
Stellungnahme des Bundesministeriums für Inneres

Aus der Sicht des Bundesministeriums für Inneres ergeben sich zu dem im Betreff bezeichneten Entwurf folgende Bemerkungen:

Allgemein

Vorab darf auf die bereits unter der Zl. LR1420/0014 vom 18. April 2008 übermittelte Stellungnahme des Bundesministeriums für Inneres verwiesen werden. Ergänzend dazu ergeben sich aus der Sicht des Bundesministeriums für Inneres zu dem im Betreff bezeichneten Entwurf folgende Bemerkungen:

Redaktionell wird vorweg bemerkt, dass im Vorblatt unter dem Titel Besonderheiten des Normsetzungsverfahrens, es wohl richtig „Anwesenheit“ statt „Abwesenheit“ heißen müsste.
In der Textgegenüberstellung zu § 19 Abs. 1 Z 3a wird auf § 18 Abs. 2 Z 1 bis 4 verwiesen. Die vorgeschlagene Fassung enthält keinen Abs. 2 in § 18.

Zu Z 10 (§ 1)

Mit der vorgeschlagenen Fassung, soll das Grundrecht auf Datenschutz, eine Beschränkung auf personenbezogene Daten natürlicher Personen erfahren. Wie den Erläuterungen entnommen werden kann, soll nur schwerlich argumentiert werden können, dass Daten welche juristische Personen betreffen, einer der natürlichen Person vergleichbaren Schutzwürdigkeit unterliegen. Offenbar soll damit ein - wie mit dem DSG (1978) konzipierter - umfassender

Datenschutz aufgegeben werden, welcher ursprünglich als Fortführung der Grundsätze des „Jedermannrechtes“ des Art. 8 der Europäischen Menschenrechtskonvention eingerichtet wurde, erweitert in Richtung auf ein grundsätzliches Informationsrecht des Betroffenen über seine verarbeiteten Daten. Eine Klarstellung hinsichtlich des Anwendungsbereiches des Art. 8 der Europäischen Menschenrechtskonvention selbst erfolgt damit aber nicht.

In diesem Zusammenhang wird darauf hingewiesen, dass die juristische Person nur Rechtsträger, das Zurechnungsobjekt eines Unternehmens ist. Unternehmen sind nicht juristische Personen, sie werden vielmehr von physischen oder juristischen Personen betrieben. Weiters ist die „Ultra-vires-Lehre“ im österreichischen Privatrecht nicht herrschend und hat den Nachteil, dass die Einschränkung der Rechtsfähigkeit der juristischen Person Dritten nicht leicht erkennbar ist, was den „Geschäftsverkehr“ erheblich belasten kann.
Ob tatsächlich mit den Regelungen des Immaterialgüterrechts in diesem Zusammenhang das Auslangen gefunden werden kann, darf bezweifelt werden, ebenso ob damit Einsparungen erzielt werden könne.
Hinsichtlich des Anwendungsbereiches einfacher Materiengesetze wären die jeweils enthaltenen statischen Verweisungen auf die Bestimmungen des Datenschutzgesetzes 2000, BGBl. I Nr. 165/1999, zu überprüfen.

Zu Z 16 (§ 4 Abs. 1 Z 4):
Um den Begriff des Auftraggebers klar zu definieren und missverständliche Interpretationen zu vermeiden, wird die beispielhafte Aufzählung von Auftraggebereigenschaften wie Handhabung der Benutzerverwaltung, Lösch- und Sperrkompetenz von Daten und Benutzern, inhaltliche Ausgestaltung einer Datenanwendung, Festlegung und Änderung des Datenflusses, Definition des Ziel und Zweckes einer Datenanwendung zwecks Klarstellung des Begriffes zumindest in den Erläuterungen angeregt.

Zu Z 21 und 24 (§ 4 Abs. 1 Z 10 und Abs. 2):
Die Entflechtung der Begriffsbestimmungen von der Art der Datenverwendung, insbesondere die Loslösung des „Ermittlungsbegriffs“ von der Verwendung der Daten in einer Datenanwendung führt zu eine massiven Erweiterung des Anwendungsbereichs des DSG, die Auswirkungen auch auf das Sicherheitspolizeirecht hat. Diese Änderung der Systematik, mit der die Anwendbarkeit der §§ 6 und 7 Abs. 2 und 3 iVm 8 und des 6. Abschnitts auch für Datenverwendungen außerhalb von (manuellen) Dateien oder Datenanwendungen normiert wird, mithin unabhängig von jeglicher Strukturiertheit und sogar unabhängig von jeglichem Erfassungsvorgang, wird abgelehnt. Darüber hinaus widerspricht diese Änderung völlig der bisherigen Systematik des Gesetzes, was sich darin zeigt, dass in den - hinkünftig für alle

ermittelten personenbezogenen Daten unabhängig von ihrer weiteren Verarbeitung geltenden - §§ 6 (vor allem Abs. 2 und 3) und 7 Abs. 2 das Vorhandensein einer Datenanwendungen ausdrücklich vorausgesetzt wird, wodurch die Verweise ins Leere gehen bzw. unverständlich sind.

Der vorletzte Satz der § 4 Abs. 2 lautet: „*Wo im 6. Abschnitt von Datenanwendungen die Rede ist, gelten die Bestimmungen sinngemäß für alle Daten.*“

Den Erläuterungen dazu ist zu entnehmen: „*Die übrigen materiellrechtlichen Abschnitte gelten in Ausgestaltung des Grundrechtes zum Großteil für Datenanwendungen und Dateien, zum Teil auch nur für Datenanwendungen.*“

Soweit aber in der vorgeschlagenen Fassung der Definition „Auftraggeber“ (§ 4 Abs. 1 Z 4) nunmehr auf das Verwenden von Daten (Z 8) abgestellt wird und damit die Bezugnahme auf „*jede andere Art der Handhabung von Daten einer Datenanwendung*“ entfällt, wird die Kognitionsbefugnis der Datenschutzkommission nicht bloß auf Dateien, sondern tatsächlich auf jede Art der Verwendung von Daten (z.B. auf „reine Papierakten“) erweitert, ohne dass dazu den Erläuterungen eine Begründung zu entnehmen wäre.

Zu Z 28, 31 und 82 (§ 8 Abs. 3 Z 5, § 9 Z 9 und § 50a Abs. 3 Z 7 sowie § 50a Abs. 5):

Die angeführten Bestimmungen regeln im Wesentlichen die Datenweitergabe zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde bzw. die Übermittlung aufgezeichneter Daten einer Videoüberwachung an die zuständige Behörde oder Gericht zur Verfolgung gerichtlich strafbarer Handlungen oder Abwehr oder Beendigung eines gefährlichen Angriffs. Obwohl die angeführten Bestimmungen alle einen gemeinsamen Regelungszweck verfolgen, wurden die näheren Zulässigkeitsvoraussetzungen in nicht nachvollziehbarer Weise zum Teil völlig unterschiedlich geregelt.

Darüber hinaus sollte jedenfalls berücksichtigt werden, dass, soweit sich jemand an die Öffentlichkeit wendet, um seine Sicht der Dinge darzustellen, es jedenfalls – auch für Behörden - zulässig sein sollte, in dessen sonst bestehenden Geheimhaltungsanspruch soweit einzugreifen, als es notwendig ist, den Sachverhalt aus der Sicht der Gegenseite darzustellen (z.B. Jemand beschwert sich in einem Medium darüber, dass er aus reiner Willkür der Behörde keinen Waffenpass bekommt; diesfalls soll es der Behörde erlaubt sein, die Hintergründe ihrer Entscheidung, nämlich das Vorliegen einschlägiger strafgerichtlicher Verurteilungen, darzulegen).

Es muss demnach in den §§ 8 und 9 klar gestellt werden, dass schutzwürdige Geheimhaltungsinteressen auch dann nicht verletzt sind, wenn die Verwendung der Daten notwendig ist, um eine veröffentlichte Darstellung des Betroffenen zu berichtigen oder zu vervollständigen.

Zu Z 29 (§ 8 Abs. 4):

Grundsätzlich wird die Aufnahme einer solchen Regelung begrüßt. Eine Einschränkung auf die Anzeigeerstattung scheint jedoch zu kurz zu greifen und kann nicht davon abhängig gemacht werden, ob derjenige, der die Daten weitergibt, eine Anzeige erstatten will. Vielmehr sollte nach dem Vorbild der bundesdeutschen Regelung des § 28 Abs. 3 Z 2 dt. Bundesdatenschutzgesetz generell davon gesprochen werden, dass schutzwürdige Geheimhaltungsinteressen nicht verletzt werden, wenn die Datenweitergabe zur Erfüllung einer sicherheitspolizeilichen Aufgabe sowie für die Verfolgung von Straftaten erforderlich ist.

Zu Z 38 (§ 17):

Soweit hinkünftig das Datenverarbeitungsregister, zwecks Vereinfachung und Beschleunigung der Verwaltungsabläufe, in der Form einer Datenbank geführt werden soll und Meldungen nur mehr in automationsunterstützter Form über eine Internetanwendung erstattet werden können, welche eine Identifizierung und Authentifizierung des Auftraggebers mit der Bürgerkarte (§ 2 Z 10 des E-GovG) zur Voraussetzung hat, muss zum gegebenen Zeitpunkt auf die Notwendigkeit weitere Amtsaustattungen (hier: mit „Bürgerkarten“) hingewiesen werden.

Zu Z 47(§ 26 Abs. 10):

Der Bundesminister für Inneres übt bei zahlreichen Informationsverbundsystemen (z.B.: Kriminalpolizeilicher Aktenindex (KPA), Sachenfahndung (SF), oder Zentrales Melderegister (ZMR), sowohl die Funktion des Betreibers gemäß § 50 DSG 2000 als auch des Dienstleisters im Sinne des § 4 Z 5 DSG 2000 aus (siehe insb. die ausdrücklichen gesetzlichen Anordnungen in §§ § 22b Abs. 1 Passgesetz oder § 16 Abs. 2 Meldegesetz)

In seiner Funktion als Betreiber hat der Bundesminister für Inneres gemäß § 50 Abs. 1 DSG 2000 jedem Betroffenen auf Antrag binnen zwölf Wochen alle Auskünfte zu geben, die notwendig sind, um den für die Verarbeitung seiner Daten im System verantwortlichen Auftraggeber festzustellen.

In seiner Funktion als Dienstleister hätte der Bundesminister für Inneres - nunmehr gemäß § 26 Abs. 10 DSG 2000 - jedem Betroffenen auf Antrag binnen zwei Wochen Namen und Adresse des tatsächlichen Auftraggebers bekannt zu geben.

Die Frist des § 26 Abs. 10 DSG 2000 wäre sechsmal „kürzer“ als die Frist des § 50 Abs. 1 DSG 2000: Warum für ein- und dieselbe Verpflichtung (hier: Bekanntgabe des jeweiligen Auftraggebers) jeweils unterschiedliche Fristen für die jeweils Verpflichteten (hier: Dienstleister und Betreiber) normiert werden sollen, kann den Erläuterungen nicht entnommen werden. Die Bestimmung des § 26 erscheint in ihren Auswirkungen noch nicht

ausreichend durchdacht und sollte nochmals überarbeitet werden. Welche Frist zur Anwendung gelangt, wenn eine Organisationseinheit sowohl die Funktion des Betreibers als auch des Dienstleisters ausübt, kann dem Entwurf auch nicht entnommen werden.
Durch welche Maßnahmen (z.B. zusätzliches Personal) ein Dienstleister (z.B.: wie das Bundesministerium für Inneres) in die Lage versetzt werden soll, Auskunftsanträge derart rasch (bzw. sechsmal schneller als in seiner Funktion als Betreiber) zu prüfen und auf andere Auftraggeber hinzuweisen, kann den Erläuterungen nicht entnommen werden.
Die kurze zweiwöchige Frist wäre nicht zuletzt deshalb abzulehnen, da für ein- und dasselbe Auskunftsverfahren unterschiedliche Fristen (von zwei, acht und zwölf Wochen) normiert werden, soweit der Auftraggeber, der Auskünfte zu erteilen hat, auch noch Dienstleister und Betreiber ist, und solcherart auch andere Auftraggeber zu benennen hat.

Zu Z 55 (§ 31):

Die Änderung in § 31 Abs. 2 ist insofern nachvollziehbar, als die „negative“ Abgrenzung der Beschwerdelegitimation im Hinblick auf § 32 Abs. 1 vorgenommen wurde. Die Änderung von „Auftraggeber des öffentlichen Bereichs, der nicht als Organe der Gesetzgebung oder Gerichtsbarkeit tätig ist“ in „Organ der Gesetzgebung oder Gerichtsbarkeit“, die in den Erläuterungen mit einem nicht nachvollziehbaren Verweis auf § 1 Abs. 5 begründet wird, ist abzulehnen und befindet sich vor allem im Widerspruch zu § 106 StPO, wonach Einsprüche wegen Rechtsverletzungen auch durch die Kriminalpolizei ausschließlich ans Gericht zu richten sind.

Zu Z 70 (§ 40):

Die Beschränkung der Amtsbeschwerdemöglichkeit und der Verweis auf Spezialregelungen in den Materien wurden schon im Zuge der Begutachtung des DSG 2000 als unzureichend erachtet. Zwischenzeitlich hat sich bei mehreren Anlässen gezeigt, (siehe auch den in den Erläuterungen zitierten Beschluss des Verwaltungsgerichtshofs. Zl. 2006/06/0068), dass ein Anpassungsbedarf besteht, um Streitigkeiten hinsichtlich der Zuständigkeit der DSK im Einzelfall (keine Zuständigkeit des DSK nach § 31 Abs. 2, wenn sich die Beschwerde gegen ein *Organ der Gesetzgebung oder Gerichtsbarkeit* richtet, Äußerung dazu siehe oben) vor einem Höchstgericht klären zu lassen. Die nunmehr vorgenommene „Klarstellung“, dass in Verfahren gemäß § 31 grundsätzlich keine Amtsbeschwerdemöglichkeit besteht, widerspricht darüber hinaus dem System, das sich in anderen Bereichen bei Zuständigkeit der Unabhängigen Verwaltungssenate als zweckmäßig und wirkungsvoll erwiesen hat.

Der Ausschluss der Möglichkeit der Anrufung des Verwaltungsgerichtshofes durch Auftraggeber des öffentlichen Bereichs als Beschwerdegegner in Verfahren nach § 31, stellt ein klares rechtsstaatliches Defizit dar.

Art 131 Abs 2 B-VG ermächtigt den einfachen Gesetzgeber, Amtsbeschwerden vorzusehen. Es geht dabei nicht um den Schutz subjektiver Rechte, sondern um die Wahrung der objektiven Rechtmäßigkeit.

Gemäß § 31 Abs 1 besteht keine Zuständigkeit der DSK, wenn sich Auskunftsverlangen auf die Verwendung von Daten für Akte der Gesetzgebung oder der Gerichtsbarkeit beziehen. Die Beantwortung der Frage, ob ein Auftraggeber des öffentlichen Bereichs „als Organ der Gesetzgebung oder der Gerichtsbarkeit tätig ist“, ist nach dem Willen des Gesetzgebers „nach funktionalen Gesichtspunkten vorzunehmen“ (1613 BlgNR, 20.GP, 49). Entscheidend ist also nicht, ob der betreffende Auftraggeber des öffentlichen Bereiches organisatorisch als Organ der Gesetzgebung oder für die Gerichtsbarkeit zu qualifizieren ist; entscheidend ist vielmehr, ob er eine Tätigkeit für die Organe der Gesetzgebung oder für die Gerichtsbarkeit ausübt. Dies ist dann der Fall, wenn die betreffende Tätigkeit einen vorbereitenden Teilakt gesetzgeberischer oder gerichtlicher Tätigkeit darstellt. Ist dies der Fall, dann wird der Auftraggeber des öffentlichen Bereiches „als Organ der Gesetzgebung oder Gerichtsbarkeit tätig“ und wäre eine Zuständigkeit der Datenschutzkommission nicht gegeben.
Obwohl die o.a. Voraussetzungen im Rahmen von Ermittlungstätigkeit vorlagen, ergingen von der DSK an das BM.I negative Bescheide, wobei ho die Auffassung vertreten wird, dass die DSK zu Unrecht ihre Zuständigkeit in Anspruch genommen hat. Eine Beschwerde an den VwGH blieb aber mangels Beschwerdelegitimation erfolglos. Wie dieser in 98/12/0515-5 festgehalten hat, ist eine Amtsbeschwerde des Bundesministers für Inneres zur Gänze mangels Legitimation unzulässig, wenn ein Polizeihandeln im Dienste der Strafjustiz vorliegt, da sich die Möglichkeit einer Amtsbeschwerde nur auf den Datenschutz in Angelegenheiten der Sicherheitsverwaltung (§§ 90 u. 91 SPG) bezieht.
Es ist durchaus denkbar – auch im Lichte der Änderung des DSG 2000 und den Regelungen in der StPO – vertretbare Argumente zu finden, die sicherheitsbehördliches Handeln funktionell entweder als Akt der Gerichtsbarkeit oder als Akt der Verwaltung qualifizieren lassen. Die von der DSK in Anspruch genommene Zuständigkeit führt nach ho Auffassung nicht nur zu einer „Doppelgleisigkeit der Kontrolle“ und würde damit Ermittlungen im Rahmen der Strafrechtspflege – die in der StPO durch den Gesetzgeber wohl abschließend geregelt sind - erheblich beeinträchtigen, sondern auch zu einer de facto Kontrollbefugnis der DSK über die Gerichtsbarkeit führen. Eine solche Doppelgleisigkeit ist ergo auch im Hinblick auf den Grundsatz der Trennung von Gerichtsbarkeit und Verwaltung (Art. 94 B-VG) mehr als

problematisch zu sehen, weil hier die DSK als Verwaltungsbehörde mit Gerichten (zumindest) „konkurriert".

Es wird daher dringend angeregt, zumindest die subsidiäre Möglichkeit einer Amtsbeschwerde – wenn also keine besondere gesetzliche Regelung besteht – für Auftraggeber des öffentlichen Bereichs in § 40 Abs 2 jedenfalls aufzunehmen.

Zu Z 81 (§ 50 Abs. 2a):

Wird ein Informationsverbundsystem auf Grund einer Meldung von zumindest zwei Auftraggebern registriert, so können Auftraggeber, die in der Folge die Teilnahme an dem Informationsverbundsystem anstreben, in Hinkunft nach § 50 Abs. 2a Satz 1 die Meldung im Umfang des § 19 Z 3 bis 8 auf einen Verweis auf den Inhalt der Meldung eines bereits registrierten Auftraggebers beschränken.

Es wird eine Ergänzung dahingehend angeregt, dass ein derartiger Verweis auf den Inhalt der bereits registrierten Meldung eines (bereits registrierten) Auftraggebers dann zulässig ist, wenn der „verweisende" Auftraggeber Datenverwendungen auch in exakt demselben Umfang vornimmt, wie sie in der bereits registrierten Meldung eines anderen Auftraggebers ausgewiesen sind.

Fehlt eine derartige Regelung, könnte z.B. in Hinkunft eine Asylbehörde bei der Meldung ihrer Verarbeitungen für das Informationsverbundsystem „Zentrales Fremdenregister" auf die Meldung einer Fremdenpolizeibehörde verweisen, obgleich diese Fremdenpolizeibehörde andere Daten zu anderen Betroffenenkreise (als die Asylbehörde) verarbeitet.

Zu Z 82 (9a. Abschnitt - Videoüberwachung)

Wie Punkt 7 des Anhanges Videoüberwachung des Datenschutzberichtes 2007 der Datenschutzkommission zu entnehmen ist, bedarf die Videoüberwachung für behördliche (hoheitliche) Zwecke jeweils einer besonderen gesetzlichen Grundlage, und ist die Videoüberwachung für sicherheitspolizeiliche Zwecke im Sicherheitspolizeigesetz abschließend geregelt.

§ 50a Abs. 4 ist daher zu entnehmen, dass Abs. 3 Z 4 bis 7 nicht für Auftraggeber des öffentlichen Bereichs bei Wahrnehmung hoheitlicher Aufgaben gelten.

§ 50a Abs. 3 beschreibt den Erläuterungen zufolge in den Z 4 bis 7 jene Fälle, in denen eine Interessenabwägung zu erfolgen hat, um festzustellen, ob schutzwürdige Geheimhaltungsinteressen eines von Videoüberwachung Betroffenen nicht verletzt werden. In der in der Praxis wohl am häufigsten vorkommenden Fallkonstellation des Eigen- oder Eigentumsschutzes (Z 5) wird begrifflich auf den in § 16 Abs. 1 Z 1 SPG definierten

(wahrscheinlichen) gefährlichen Angriff abgestellt. Aus mehreren Gründen scheint die Anknüpfung an den sicherheitspolizeilichen Begriff des „gefährlichen Angriffes“ und damit an eine mögliche Gefahrenprognose zweifelsfrei nicht als optimale Lösung.
In zeitlicher Hinsicht beginnt der gefährliche Angriff schon vor dem Versuchsstadium (§ 16 Abs. 3 SPG), daraus erscheint es nicht zweckmäßig bereits vorangegangene strafbare Handlungen als Anknüpfungspunkt heranzuziehen. Außerdem fallen die Organisationsdelikte der §§ 278 bis 278b StGB nicht unter den Begriff gefährlicher Angriff, ebenso wenig wie Privatanklagedelikte - etwa die im Zusammenhang mit Videoüberwachung durchaus zu bedenkende Auskundschaftung eines Betriebs- oder Geschäftsgeheimnisses (§ 123 StGB) - oder der „bloße“ Suchtgiftmissbrauch sowie sonstige Delikte des Nebenstrafrechts oder Ordnungsstörungen. Bei konsequenter Verfolgung der dem Entwurf zu Grunde liegenden Intention würde dies etwa bedeuten, dass bei Ordnungsstörungen oder Betriebsspionage, eine Videoaufzeichnung nicht zulässig wäre. Beispielhaft sei etwa angeführt, dass, ein Tankstellenpächter, der in den letzten 10 Jahren noch nicht Opfer einer strafbaren Handlung wurde im Gegensatz zu einem bereits in der Vergangenheit überfallenen Tankstellenpächter nicht berechtigt wäre eine Videoüberwachung durchzuführen. Auch der bereits jetzt vieler Orten bestehende Schutz von Haus- bzw. Wohnungseigentümern und Mietern durch private Videoüberwachungsmaßnahmen wäre durch diese Regelung gefährdet.

Nicht nachvollziehbar ist die in Z 5 vorgesehene Lösung, wonach bei Zutreffen einer der aufgezählten Voraussetzungen die Gefährdungsprognose (Wahrscheinlichkeit eines künftigen gefährlichen Angriffs) gesetzlich fingiert wird. Dies erscheint insofern in einem kritischen Licht, als die Erlaubnistatbestände für Videoaufzeichnung auch ohne Verknüpfung mit der Gefährdungsprognose verankert werden könnten, darüber hinaus befindet sich der Vorschlag aber im klaren Widerspruch mit den Bestimmungen des SPG.

Das Sicherheitspolizeigesetz überträgt den Sicherheitsbehörden gemäß § 22 den vorbeugenden Schutz von Rechtsgütern. Gemäß Abs. 1 obliegt ihnen der besondere Schutz von verfassungsmäßigen Einrichtungen auch dann, wenn – wie im Regelfall - keine konkrete Gefährdungssituation gegeben ist. Wenn allerdings auf Grund von Tatsachen anzunehmen ist, es stehe ein gefährlicher Angriff auf Menschen oder Sachen bevor (§ 22 Abs. 2 SPG), haben die Sicherheitsbehörden selbstverständlich erhöhte Schutzmaßnahmen zu treffen, vor allem eine verstärkte Bewachung der Gefährdeten gemäß § 48 SPG. Präventive Videoaufzeichnung nach dem SPG ist aber auch unter den beschriebenen Voraussetzungen nicht zulässig. Eine Ausnahme findet sich lediglich in § 54 Abs. 7 SPG. Im Hinblick auf die vorgeschlagene Regelung gemäß § 50a Abs. 4, wonach Abs. 3 Z 4 bis 7

nicht für Hoheitsverwaltung gelten soll, ändert sich an der bestehenden Ermächtigung für die Sicherheitsbehörden letztlich nichts.

Die Annahme des § 50a Abs. 3 Z 5 lit. a bis e, wonach etwa verfassungsmäßige Organe, Personen des öffentlichen Lebens oder Objekte mit einem Wert von über 100.000 Euro nicht nur potentiell, sondern konkret (im Sinne von „Tatsachen, die die Annahme rechtfertigen“) gefährdet sind, entspricht erstens nicht den Tatsachen und kollidiert zweitens mit den Aufgaben und Befugnissen des SPG. Eine solche Gefährdungssituation würde nämlich, wäre sie real, in den aufgezählten Fällen eine sicherheitspolizeiliche Aufgabenstellung auslösen, der mit sicherheitspolizeilichen Befugnissen und nicht durch eine private Videoüberwachung zu begegnen wäre.

Aus Sicht des BM.I ist durch den vorliegenden Vorschlag auch nicht abgedeckt, dass für Zwecke des Objektschutzes, also unabhängig von vorangegangenen oder zu erwartenden Straftaten in Privatwirtschaftsverwaltung „Objekte“ überwacht werden, in denen sich keine verfassungsmäßigen Organe aufhalten oder besondere Geldwerte aufbewahrt werden, wie Außenstellen von Ministerien, Kasernen oder sonstige exponierte Gebäude.

Für bloße Echtzeitübertragung als technisch verstärktes Sehen besteht kein Regelungsbedarf im DSG. Im Datenschutzbericht 2007 (Seite 65) geht die Datenschutzkommission (im Gegensatz zu den Erläuterungen, S 12 Mitte, zur gegenständlichen Novelle) davon aus, dass es sich beim sog. „real time monitoring“ nicht um eine Datenanwendung handelt, da nur Videoüberwachung mit Aufzeichnung unter die Definition des § 4 Z 7 DSG fällt. Es existieren ohne Aufzeichnung nämlich keine logisch verbundenen Datenverwendungsschritte im Sinne der Z 8, die zur Erreichung eines bestimmten Zwecks geordnet sind und zur Gänze oder teilweise automationsunterstützt erfolgen. Dieser Auffassung schließt sich das Bundesministerium für Inneres an. Der in den Erläuterungen getroffene Hinweis auf Umsetzungsbedarf nach der Datenschutzrichtlinie 95/46/EG erscheint nicht zutreffend, es wird dazu auf den 15. Erwägungsgrund der Datenschutzrichtlinie (95/46/ EG) verwiesen, wonach die „*Verarbeitung solcher Daten (Bild- und Tondaten) von dieser Richtlinie* ***nur*** *erfasst wird, wenn sie automatisiert erfolgt oder wenn die Daten, auf die sich die Verarbeitung bezieht, in Dateien enthalten oder für solche bestimmt sind, die nach bestimmten personenbezogenen Kriterien strukturiert sind, um einen leichten Zugriff auf die Daten zu ermöglichen*“.

Es bleibt den Mitgliedstaaten immer überlassen, strengere Regelungen vorzusehen, die Notwendigkeit, Kriterien für die Zulässigkeit bloßer Übertragungssysteme festzulegen, wird allerdings nicht gesehen.

Die sprachliche Gleichstellung von Personen, Orten und Gegenständen in dieser Bestimmung sollte überdacht werden.

Die in § 50b Abs. 1 enthaltene Regelung, dass jeder Verwendungsvorgang (Abfrage, Übermittlung, Änderung, Löschung von Daten) einer Videoüberwachung zu protokollieren ist, ist aus Gründen der Datensicherheit zu begrüßen. Es stellt sich allerdings die Frage, ob Videoüberwachungsanlagen, die über derartige, insb. programmgesteuerte Protokollierungsfunktionalitäten verfügen, bereits auf dem Markt erhältlich sind bzw. ob die angeordnete Vollprotokollierung „Stand der Technik“ ist.

Soweit die aufgezeichneten Daten gemäß 50b Abs. 2 regelmäßig spätestens nach 48 Stunden zu löschen sind, wäre es auch zweckmäßig, eine ausdrückliche Regelung bezüglich der Aufbewahrungsdauer der Protokolldaten iSd § 50b Abs. 1 zu normieren. Davon abgesehen scheint die Frist von 48 Stunden für Menschen, die mit einer Videoüberwachung ihr Eigentum während eines Urlaubs schützen wollen, wenig hilfreich, weil sie eine Übermittlung an die zuständige Behörde oder das zuständige Gericht wohl erst nach ihrer Rückkehr vom Urlaub bewerkstelligen werden können. Mit der Frist von 48 Stunden wird man im privaten Bereich wohl nicht das Auslangen finden können.

Weiteres:

Es wird (wie auch schon anlässlich der Vorarbeiten zum DSG 2000) angeregt, „Sonderregelungen“ für den Online-Datenverkehr und die jeweiligen Verantwortlichkeiten von Auftraggebern und Übermittlungsempfängern im Verhältnis zu § 7 Abs. 2 Z 2 und 3 DSG 2000 vorzusehen. Es zeigt sich, dass die in § 50 Abs. 1 DSG 2000 normierte spezielle Verantwortung der Betreiber von Informationsverbundsystemen, insb. auch bezüglich der Gewährung des Direktzugriffs, nicht ausreicht, um im Einzelfall die Zulässigkeit von „Online-Anfragen“, vor allem wenn sie nicht wie etwa in *Art X § 1 StrÄG 1996 oder in § 16 a Abs. 4 Meldegesetz* ausdrücklich vorgesehen ist, eindeutig beurteilen zu können.

Gleichzeitig wird dem Präsidium des Nationalrates diese Stellungnahme in elektronischer Form übermittelt.

Für den Bundesminister:

Mag. Sabine Halbauer

elektronisch gefertigt