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

GZ.: BMI-LR1420/0009-III/1/a/2009 Wien, am 18. Juni 2009

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 2010);
Stellungnahme des Bundesministeriums für Inneres

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

Beilage

Für die Bundesministerin:

Mag. Peter Andre

elektronisch gefertigt

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

GZ.: BMI-LR1420/0009-III/1/a/2009 Wien, am 18. Juni 2009

An das

Bundeskanzleramt-Verfassungsdienst

Ballhausplatz 2
1014 W I E N

Zu Zl. BKA-810.026/0005-V/3/2009

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 2010);
Stellungnahme des Bundesministeriums für Inneres

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

Zu Art. 1 (Bundes-Verfassungsgesetzes)

Die den Ländern gemäß § 2 Abs. 2 zweiter Satz DSG 2000 vorbehaltene Zuständigkeit zur Vollziehung des Datenschutzrechtes soll mit dem vorliegenden Entwurf (zur Änderung des Art. 10 Abs. 1 Z 13 und 102 Abs. 2 B-VG und dem Entfall des § 2 DSG 2000) beseitigt werden. In den Erläuterungen zu Art. 1 ist hiezu ua. angemerkt: „*Keine Vollziehung des Datenschutzrechts stellt die Verwendung von personenbezogenen Daten durch Länder und Gemeinden als Auftraggeber dar*."

Die Richtigkeit dieser Ausführungen muss angezweifelt werden, da z.B. die Führung eines Löschungsverfahrens gemäß § 27 DSG 2000 durch eine Bezirkshauptmannschaft (als Auftraggeber) wohl unzweifelhaft einen Akt der Vollziehung durch eine Landesbehörde darstellt. Würde „*die Verwendung von personenbezogenen Daten durch Länder und Gemeinden als Auftraggeber keine Vollziehung des Datenschutzrechts*" darstellen, könnten z.B. im Falle von rechtwidrigen Datenverwendungen auch keine Ansprüche gemäß § 1 Abs. 1 Amtshaftungsgesetz geltend gemacht werden. Der Entfall des Vollziehungsvorbehaltes zugunsten der Länder gemäß § 2 Abs. 2 zweiter Satz DSG 2000 würde jedenfalls bewirken, dass die Verwendung personenbezogener Daten selbst in

Angelegenheiten der Landesverwaltung zur Bundesverwaltung gehören müsste, was zu zahlreichen, unlösbaren Problemen führen würde.

Im Übrigen entstehen bereits aufgrund der derzeitigen Kompetenzrechtslage, wonach die Landesgesetzgeber - aufgrund der ausschließlichen Zuständigkeiten des Bundesgesetzgebers zur Datenschutzgesetzgebung im automationsunterstützten Bereich - keinerlei bereichsspezifische Datenschutzregelungen in ihren Landesgesetzen erlassen dürfen, Unklarheiten, die durch die vorgeschlagene „Bereinigung“ nicht geklärt werden: So stellt sich (abgesehen von der auftretenden Frage nach der Vollziehung von Datenschutzrecht durch die Länder) im Zusammenhang mit diversen landesgesetzlichen Bestimmungen, die Frage nach der kompetenzrechtlichen Einordnung und damit nach der Gesetzgebungskompetenz. § 2a Gesetz betreffend die Jugendwohlfahrt (Wiener Jugendwohlfahrtsgesetz 1990-WrJWG 1990) regelt etwa die Verarbeitung von personenbezogenen Daten zum Zwecke der Abwehr von Gefährdungen des Kindeswohles ebenso wie Übermittlungsermächtigungen und Löschungsfristen, sowie die Verpflichtung des Magistrats, „*organisatorische Vorkehrungen zu treffen, die den Schutz der Geheimhaltungsinteressen der Betroffenen im Sinne des § 1 Abs. 2 des Datenschutzgesetzes 2000 garantieren*.“

Zu Artikel 2 (Datenschutzgesetzes 2000):

Zur Umsetzung des Rahmenbeschlusses 2008/977/JI des Rates vom 27. November 2008:
Am 27. November 2008 wurde vom Rat der EU der Rahmenbeschluss über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (Rahmenbeschluss 2008/977/JI), verabschiedet. Die Umsetzung hat bis 27.11.2010 zu erfolgen, wobei in Österreich die Regelungen des Rahmenbeschlusses zum überwiegenden Teil bereits im DSG 2000, das auch für den Bereich der Justiz und Polizei gilt, enthalten sind. Es wird allerdings in Zweifel gezogen, ob – etwa hinsichtlich der in Art 25 vorgesehenen nationalen Kontrollstelle oder der in Art 23 vorgeschriebenen Vorabkonsultation – tatsächlich kein Umsetzungsbedarf im DSG 2000 besteht.

Zu § 4 Abs. 2 iVm § 4 Abs. 1 Z 8 bis 10 und 12
Die Entflechtung der Begriffsbestimmungen von der Art der Datenverwendung, insbesondere die Loslösung des „Ermittlungsbegriffs“ von der Verwendung der Daten in einer Datenanwendung führt zu einer Erweiterung des Anwendungsbereichs des DSG. Diese Änderung der Systematik, mit der die Anwendbarkeit der §§ 6 Abs. 1 Z 1 bis 3 und Abs. 2

sowie §§ 7 bis 9 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. In den Erläuterungen wird ausgeführt, dass beim „bloßen Sehen“, das kein „gezieltes Beobachten“ darstellt, keine Daten (auch nicht bloß manuelle) iSd Gesetzes gewonnen werden. Diese Aussage findet im Wortlaut und der Systematik des Gesetzes nicht ihren Niederschlag, mit der Konsequenz, dass die bloße Wahrnehmung personenbezogener Daten (Kennzeichen oder bestimmbare Personen) durch ein Exekutivorgan etwa im Rahmen des Streifendienstes durch einen Betroffenen vor der DSK bekämpft werden könnte. Darüber hinaus widerspricht diese Änderung völlig der bisherigen Systematik, was sich darin zeigt, dass etwa im - hinkünftig für alle ermittelten personenbezogenen Daten unabhängig von ihrer weiteren Verarbeitung geltenden - § 7 Abs. 2 das Vorhandensein einer Datenanwendungen ausdrücklich vorausgesetzt wird, wodurch der Verweis unverständlich wird.

Zu § 7:

§ 7 DSG 2000, der die rechtliche Verantwortung für Übermittlungen dem Übermittelnden auferlegt, deckt den Sonderfall von Online - Übermittlungen nicht ab. Aus Sicht des BMI bedarf es einer ausdrücklichen Klarstellung dahingehend, dass eine gesetzliche Übermittlungsermächtigung, in der Übermittlungszweck und die Übermittlungsempfänger ausgewiesen sind, nicht auch zusätzlich eine ausdrückliche Regelung für den Online-Datenverkehr erfordert, oder aber, dass die entsprechenden Voraussetzungen im DSG 2000 ausdrücklich verankert werden.

Zu § 8 Abs. 4:

In der vorgeschlagenen Z. 4 wird die Datenweitergabe (Anzeigeerstattung) bestimmter strafbarer Handlungen – sowohl gerichtlich als auch verwaltungsbehördlich strafbarer Handlungen oder Unterlassungen – zur Verfolgung durch die zuständige Behörde geregelt.

Aufgrund des Wortlauts scheint es zweifelhaft zu sein, ob von dieser Bestimmung abgedeckt ist, dass Sachverhalte der für den Verdächtigen zuständigen Dienstbehörde oder Personalstelle zur Kenntnis gebracht werden. Gerade für die Dienstbehörde bzw. Personalstelle ist die Kenntnis derartiger Sachverhalte für die Einleitung von disziplinarrechtlichen Maßnahmen (beim Beamten) oder dienstrechtlichen Schritten (beim Vertragsbediensteten) von Bedeutung. Als Beispiel seien der Entzug einer waffenrechtlichen Urkunde oder der Entzug der Lenkerberechtigung angeführt.

Es sollte daher klargestellt werden, dass die Weitergabe (auch) an die zur Setzung gesetzlich zulässiger Sanktionen zuständige Dienststelle zulässig ist.

Zu § 14 Abs. 4 :

Über die Novellierungsvorschläge hinaus wird auch die Adaptierung von § 14 Abs. 4 DSG 2000 (Verwendungszwecke für Protokoll- und Dokumentationsdaten) dringend angeregt. Es ist erforderlich, die Einschränkung auf Verbrechen, die mit zumindest 5 Jahren Freiheitsstrafe bedroht sind, auf ein Jahr Freiheitsstrafdrohung herabzusetzen. Sowohl im Zusammenhang mit dem Verdacht auf Amtsmissbrauch gemäß § 302 StGB (wo bislang Protokolldatenauswertungen unter Berufung auf die „Prüfung der Zugriffsberechtigung“ stattgefunden haben), als auch etwa bei KFZ – Diebstählen nach § 128 Abs. 1 StGB (bei einer Wertgrenze unter 50 000 Euro) entstehen sachlich nicht rechtfertigbare Lücken.

Zu § 24 Abs. 2a:

Die Informationsverpflichtung Betroffener bei Kenntnis von „systematischer und schwerwiegender“ unrechtmäßiger Datenverwendung wirft eine Reihe von Fragen auf, die aus Sicht des BMI jedenfalls weiterer Diskussion bedürfen. Den Erläuterungen zufolge geht es um die Vermeidung von Vermögensschäden, was aus dem Wortlaut der Bestimmung aber nicht abgeleitet werden kann. Es ist weder klar, wie die Frage nach allfälligen Schäden zu beurteilen ist, noch wer diese Beurteilung vorzunehmen hat. Völlig offen bleibt auch, welche Konsequenzen eine Information Betroffener nach sich zieht, weshalb eine ersatzlose Streichung dieser Bestimmung vorgeschlagen wird. Jedenfalls müsste sichergestellt sein, dass die Bestimmung des § 26 Abs. 5 DSG betreffend das Auskunftsverweigerungsrecht dadurch nicht „ausgehebelt“ wird.

Zu § 26 Abs. 6:

Gemäß § 26 Abs. 6 DSG 2000 ist die Auskunft grundsätzlich unentgeltlich zu erteilen, wenn sie den aktuellen Datenbestand einer Datenanwendung betrifft und wenn der Betroffene im laufenden Jahr noch kein Auskunftsersuchen an den Auftraggeber zum selben Aufgabengebiet gestellt hat.

Im Hinblick auf diese Textierung kann nach herrschender Auffassung kein Kostenersatz verlangt werden, wenn ein Auskunftswerber Auskunft über den aktuellen Datenbestand sämtlicher Datenanwendungen eines Auftraggebers begehrt, mögen auch diese Auskünfte insgesamt sehr umfangreich sein, und erheblichen Bearbeitungsaufwand beim Auftraggeber verursachen (z.B.: in Fällen, in denen ein Auskunftswerber Auskunft über den jeweils aktuellen Datenbestand aus den 46 beim DVR registrierten Datenanwendungen des BM.I begehrt).

Eine Novellierung des § 26 Abs. 6 DSG 2000 dahingehend, dass auch bei umfangreichen Auskunftsbegehren bzw. Auskünften zum aktuellen Datenbestand mehrerer / sämtlicher

Datenanwendungen eines Auftraggebers ein Kostenersatz verlangt werden darf, erscheint gerechtfertigt, um dem Auftraggeber zumindest einen Teil der ihm tatsächlich erwachsenden Kosten für umfangreiche Auskünfte zu ersetzen.
Auch im Zusammenhang mit den „neuen“ Bestimmungen zur Auskunftserteilung über die Daten bzw. den aktuellen Datenbestand einer Videoüberwachung (gemäß § 50e des Entwurfes) erschiene eine Regelung zum Kostenersatz (des tatsächlichen Aufwandes beim Auftraggeber) gerechtfertigt.

Zu § 26 Abs. 8:

In den Erläuterungen zu dieser Bestimmung wird festgehalten, dass die Auskunftsberechtigung insoweit bestehen soll, als der Auskunftswerber ein Recht auf Einsicht in die zu seiner Person verarbeiteten Daten hat. Damit wird – so weiter in den Erläuterungen – insbesondere auch die immer häufiger werdende Führung elektronischer Verfahrenakten durch Behörden jedenfalls hinsichtlich der Verfahrensparteien umfasst (z.B. §§ 17 AVG, 90 f BAO). Daraus würde folgen, dass auch hinsichtlich der im Dienste der Strafjustiz geführten Verfahrensakten im PAD insoweit eine Auskunftsverpflichtung besteht, als der Auskunftswerber ein Recht auf Akteneinsicht hat. Über die behauptete Verletzung des Rechtes auf Auskunft würde gemäß § 31 DSG die Datenschutzkommission entscheiden. Soweit dadurch eine mögliche zweifache Beschwerdemöglichkeit einer Verfahrenspartei – einerseits gemäß den Bestimmungen der StPO (§§ 106 ff) wegen Verletzung des Rechtes auf Akteneinsicht und andererseits gemäß § 31 DSG bei der DSK wegen Verletzung der Auskunftspflicht – folgern würde, würde eine solche Regelung abgelehnt.

Diesbezüglich wird auch auf die Ausführungen zu § 1 Abs. 5 DSG 2000 i.V.m. § 31 DSG-Novelle 2010 verwiesen.

Überdies sollte der letzte Satz des § 26 Abs. 8 ersatzlos gestrichen werden, da damit eine Umgehung der Beschränkung von Einsichtsrechten durch das Auskunftsrecht ermöglicht werden könnte. Zumindest würde die Regelung einen nicht unbeachtlichen Mehraufwand für den Auskunftspflichtigen darstellen.

Zu § 26 Abs. 10:

Entsprechend den Erläuterungen zu § 26 Abs. 10 soll in den beiden neuen Sätzen der Schluss einer Lücke im System des Auskunftsrechts erfolgen: „*Wenn der Auskunftswerber ein Auskunftsbegehren irrtümlich an einen Dienstleister richtet, so hat ihm dieser nunmehr den Auftraggeber zu benennen.*“

Es wird offenbar davon ausgegangen, dass jeder Dienstleister (in jeder Phase einer Datenverwendung) immer in die Lage versetzt ist, einem Betroffenen den jeweiligen Auftraggeber für die Datenverwendung zu benennen. Dies ist jedoch z.B. dann nicht der Fall, wenn der Dienstleister die Daten des Betroffenen nach Herstellung des aufgetragenen Werkes (oder nach Beendigung der Dienstleistung) bereits vernichten musste (siehe § 11 Abs. 1 Z 5 DSG 2000 oder § 3 Abs. 6 PassG) oder er schlichtweg keine Kenntnis darüber haben darf oder hat, welche Daten welcher Betroffener er eigentlich verarbeitet hat (siehe z.B.: § 67 Abs. 2, letzter Satz SPG).

Hinsichtlich der bloß zweiwöchigen Frist zur Umsetzung der gegenständlichen Dienstleister - Verpflichtung darf nochmals auf die bereits getätigten Ausführungen zum DSG-Entwurf aus dem Jahr 2008 hingewiesen werden:
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 bloßer 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 ist 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. Soweit im Ergebnis Gleiches ungleich behandelt werden soll, wäre die Bestimmung des § 26 Abs. 10 DSG 2000 als „unsachlich“ zu qualifizieren.
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 ein 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.

Zu § 31 Abs. 1 und 2 iVm § 1 Abs. 5 DSG 2000 und dem Regierungsprogramm

Im Regierungsprogramm für die XXIV. Gesetzgebungsperiode (siehe Seite 100, Punkt E.1. Klarstellung bei der DSK-Zuständigkeit) wurde ua. ausgeführt, dass im Datenschutzgesetz

(DSG) klargestellt wird, dass der Datenschutzkommission (DSK) dann keine Zuständigkeit zukommt, wenn die Kriminalpolizei im Dienste der Strafrechtspflege tätig wird.
In § 31 Abs. 1 und 2 ist nunmehr die Zuständigkeit der DSK in jenen Fällen ausgeschlossen, in denen sich das Begehren auf die „Verwendung von Daten für Akte im Dienste der Gesetzgebung oder Gerichtsbarkeit bezieht."
Wenn die Kriminalpolizei Daten im eigenen Auftrag (iSd § 4 Z 4 DSG 2000) verwendet, und die DSK für derartige Datenverwendungen (und Grundrechtseingriffe) nicht mehr zuständig sein soll, wären aber auch die im Verfassungsrang stehenden Bestimmungen der §§ 1 Abs. 5 und 35 Abs. 2 DSG 2000 entsprechend abzuändern. Ob die erfolgten Änderungen in den einfachgesetzlichen Bestimmungen des § 31 Abs. 1 und 2 DSG 2000 ausreichen, die DSK-Zuständigkeit hinsichtlich der Datenverwendungen der Kriminalpolizei restlos zu beseitigen, mag im Hinblick auf Stufenbau der Rechtsordnung zweifelhaft erscheinen.

Zu § 40 Abs. 2:

Wie schon in der Stellungnahme des BMI zum Entwurf einer Novelle zum DSG 2000, (DSG-Novelle 2008) Zl. BMI-LR1420/0011-III/1/a/2008, ausgeführt, soll im Sinne einer DSG unmittelbaren, generellen Amtsbeschwerdemöglichkeit gegen Bescheide der Datenschutzkommission der letzte Satzes des § 40 Abs. 2 gestrichen werden.

Zum Abschnitt 8 - Besondere Verwendungszwecke von Daten:

Eine ausdrückliche gesetzliche Regelung zur Führung von Aktenverwaltungssystemen (für Zwecke der Büroautomation) existiert im DSG 2000 gegenwärtig nicht.

Da die gesetzlichen Grundlagen für die Führung der Standardanwendung SA029 Aktenverwaltung (Büroautomation) der Standard- und Muster-Verordnung 2004, BGBl. II Nr. 312/2004, insb. im Bereich der nachgeordneten Sicherheitsbehörden / Kommanden strittig sind, darf angeregt werden, im Abschnitt 8 entsprechende gesetzliche Regelungen für die Führung von Aktenverwaltungssystemen durch alle Auftraggeber des öffentlichen und privaten Bereichs vorzusehen. Diese ausdrücklichen gesetzlichen Regelungen sollten den Zweck der Datenanwendung, die jeweiligen Auftraggeber, die betroffenen Personengruppen, die Datenarten, die Dauer der Aufbewahrung der Daten sowie die Übermittlungen und Übermittlungsempfänger enthalten. Weiters sollte auch eine ausdrückliche Klarstellung durch den Gesetzgeber dahingehend erfolgen, dass nicht nur Sicherheitsbehörden, sondern auch Polizeikommanden als Auftraggeber (iSd § 4 Z 4 DSG 2000) eines Aktenverwaltungssystems fungieren können.

Zum Abschnitt 9a - Videoüberwachung:

Den Regelungen zur Videoüberwachung im neu geschaffenen Abschnitt 9a. kann nicht entnommen werden, ob und in welchem Umfang Gerätschaften zur Tonaufzeichnung (bzw. Tonübertragung) als Bestandteil einer Videoüberwachungsanlage eingesetzt werden dürfen.

Zu § 41 Abs. 2 Z 4a:

Während der Datenschutzrat gemäß Z4 Auskünfte sowie Berichte und Einsicht in Unterlagen nur unter eingeschränkten Voraussetzungen verlangen darf (arg. mit wesentlichen Auswirkungen auf den Datenschutz), sollen diese Einschränkungen gerade gegenüber der DSK nicht zur Anwendung gelangen, was als nicht stimmig erachtet wird.
Z4a wäre daher allenfalls auf Auskünfte zu beschränken.

Zu § 50a:

Hinsichtlich der massiven Bedenken des BMI, als Anknüpfungspunkt für das Vorliegen eines überwiegenden Interesses an Videoüberwachung (durch Private) die Wahrscheinlichkeit eines im Sicherheitspolizeigesetz definierten „gefährlichen Angriffs“ zu wählen, wird auf die Stellungnahme BMI-LR1420/0011-III/1/a/2008 verwiesen.
Durch die nunmehr vorgenommene Ergänzung, dass eine Videoüberwachung durch Auftraggeber des Privatrechts auch gerechtfertigt ist, wenn -abgesehen von „Objekten“- Personen Ziel eines gefährlichen Angriffs werden könnten, wird die Kollision mit den hoheitlich zu besorgenden Aufgaben des vorbeugenden Schutzes vor wahrscheinlichen gefährlichen Angriffen gemäß § 22 Abs. 2 SPG (mit den Sicherheitsbehörden zur Verfügung stehenden Befugnissen) noch evidenter, weil die Überwachung einer „gefährdeten Person“ mittels Videoaufzeichnung auch dann zulässig zu sein scheint, wenn sich diese im öffentlichen Raum bewegt.
Aus den erläuternden Bemerkungen ergibt sich nunmehr, dass der im Entwurf verwendete Terminus „gefährlicher Angriff“ nicht im Sinne des Sicherheitspolizeigesetzes zu verstehen ist, da auch die konkrete Gefährdung von Geschäfts- und Betriebsgeheimnissen sowie allenfalls auch die konkrete Gefahr einer Verwaltungsübertretung für die Zulässigkeit der Überwachung genügen soll. Die Verwendung des Begriffs des „gefährlichen Angriffs“ - mit einer anderen Bedeutung als im SPG – und ohne Legaldefinition im Gesetz ist umsomehr abzulehnen.

Für bloße Echtzeitübertragung als technisch verstärktes Sehen besteht aus Sicht des BMI kein Regelungsbedarf im DSG, wodurch sich auch die in Artikel 3 des Entwurfs vorgeschlagene Änderung des SPG erübrigen würde.

In § 50a Abs. 1 enthält eine Subsidiaritätsklausel des § 50a Abs. 2 bis 7 im Verhältnis zu gesetzlichen Sonderregelungen wie z.B. § 54 Abs. 4 SPG. Im Hinblick auf vorhandene spezialgesetzliche Regelungen über Auskunft oder Löschung ist es erforderlich eine Subsidiaritätsklausel auch hinsichtlich der §§ 50b bis 50e aufzunehmen.

Zu § 50b Abs. 1:

Die in 50b Abs. 1 enthaltene Regelung, dass jeder Verwendungsvorgang (Abfrage, Übermittlung, Änderung, Löschung von Daten) einer Videoüberwachung zu protokollieren ist, wäre aus der Sicht der Datensicherheit grundsätzlich zu begrüßen. Es stellt sich allerdings – gegenwärtig - 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.

Zu § 50b Abs. 2:

Die Löschungsfrist von 48 Stunden sollte jedenfalls merkbar angehoben werden, da sicherheits- und/oder kriminalpolizeiliche (Daten-) Ermittlungen oft erst aus den verschiedensten Gründen (z. B. spätere Anzeige von Geschädigten) später als 48 Stunden nach Beginn der Aufzeichnung erfolgen und dann in diesen Fällen notwendige Ermittlungsansätze für die Kriminalpolizei nicht mehr zur Verfügung stünden.

Die gegenständliche Stellungnahme wird dem Präsidium des Nationalrates in elektronischer Form übermittelt.

Für die Bundesministerin:

Mag. Peter Andre

elektronisch gefertigt