Datenschutzkommission

Hohenstaufengasse 3

1010 Wien
01 531 15 2525
01 531 15 26 90
www.dsk.gv.at

An das
Bundeskanzleramt - Verfassungsdienst

Ballhausplatz 1
1010 Wien

Betrifft: DSG-Novelle 2010
Stellungnahme der Datenschutzkommission

A. Zu den Z 1 – 3 (neue verfassungsrechtliche **Kompetenzgrundlagen**):

Der Entwurf betrachtet den „Schutz personenbezogener Daten“ als eigenen Kompetenztatbestand nach **Art. 10 B-VG**, in dessen Rahmen Regelungen in Hinkunft nur durch Bundesgesetz geschaffen werden dürfen.

1. Diese Sichtweise setzt voraus, dass Regelungen über den „Schutz personenbezogener Daten“ eindeutig abgegrenzt werden können von jenen zahlreichen bundes- und insbesondere landesgesetzlichen materienspezifischen Regelungen, die Festlegungen aus einem datenschutzrechtlichen Aspekt darüber enthalten, unter welchen näheren Bedingungen personenbezogene Daten für den materienspezifischen Zweck verwendet werden dürfen. Ob die Aufteilung der Zuständigkeiten zur Handhabung der Querschnittsmaterie „Datenschutz“ mit einem anderen Kompetenzverteilungsmodell nicht klarer und eindeutiger regelbar wären, sollte nochmals überlegt werden.

2. Nur festgehalten sei, dass im Unterschied zur bisherigen Kompetenzbestimmung nach § 2 DSG 2000 der Kompetenztatbestand „Schutz personenbezogener Daten“ keinerlei Einschränkung hinsichtlich der technischen Form der Verwendung der geschützten personenbezogenen Daten enthält (siehe dazu ausführlich unter Pkt. C).

B. Zu den Z 11 und 12 (**Neuformulierung des Grundrechts** auf Geheimhaltung):

1. Der vorliegende Novellenentwurf schlägt eine Neuformulierung des Grundrechts vor. Aus diesem Anlass scheint es angemessen, die Frage aufzuwerfen, ob es nicht an der Zeit wäre, eine möglichst weitreichende Harmonisierung des Anwendungsbereichs des öDSG mit jenem der RL 95/46/EG anzustreben. Wesentliche Unterschiede zwischen dem Anwendungsbereich nationaler Vorschriften und jenem gemeinschaftsrechtlicher datenschutzrechtlicher Vorschriften sind geeignet, Hemmnisse im gemeinsamen Markt darzustellen und tragen jedenfalls zur erheblichen Verkomplizierung grenzüberschreitender datenschutzrelevanter Sachverhalte bei.

Der sachliche Anwendungsbereich der RL 95/46 /EG ist auf den Schutz solcher personenbezogener Daten beschränkt, die unter erhöhtem Gefährdungspotential verwendet werden, weil sie infolge der elektronischen Verarbeitung oder der Führung in einer (manuellen) Datei leichter und schneller auffindbar sind als nicht-strukturierte oder nicht-elektronisch verarbeitete Daten. Dem trug das DSG 2000 bisher immerhin in seinem einfachgesetzlichen Teil Rechnung. Der vorliegende Entwurf macht die Unterschiede im sachlichen Anwendungsbereich von öDSG und RL 95/46 nunmehr auch im einfachgesetzlichen Teil des Datenschutzgesetzes deutlich – dies sollte einer kritischen Prüfung unterzogen werden.

Hinzu kommt, dass mit dem Vertrag von Lissabon in den Art 7 und 8 der dann verbindlichen Grundrechtscharta (vgl Art 6 EUV) eigene Grundrechte über die Achtung des Privat- und Familienlebens und des Schutzes personenbezogener Daten, aber auch der Freiheit der Meinungsäußerung und der Informationsfreiheit (Art 11) festgelegt werden. Von diesen Regelungen durch wesentliche Unterschiede im Anwendungsbereich abzuweichen, scheint im Hinblick auf den Vorrang des Gemeinschaftsrechts nicht zielführend, da hiedurch unübersichtliche und unharmonische Strukturen des geltenden Rechts entstehen. Es scheint daher erwägenswert für eine umfassende Novellierung abzuwarten, ob der Vertrag von Lissabon in Kraft tritt.

2. Der Entwurf schlägt vor, das Konzept der Einschränkung des Grundrechts **im § 1 Abs. 1** auf jene Fälle, in welchen „schutzwürdige Geheimhaltungsinteressen“ bestehen, aufzugeben.

Dem kann unter der Voraussetzung zugestimmt werden, dass die notwendigen Privilegierungsbestimmungen für die Verwendung von „indirekt personenbezogenen Daten“

und „allgemein verfügbaren Daten“ *im einfachgesetzlichen Teil* des DSG (in der Folge als „DSG-egT“ bezeichnet) getroffen werden.

Aus Sicht der Datenschutzkommission sollten allerdings vor allem die besonderen Schutzvorschriften für spezielle Verwendungssituationen von allgemein verfügbaren Daten noch treffsicherer gestaltet werden als bisher (so z.B. bei Veröffentlichung von Daten im Internet oder bei Zweckänderung im Rahmen der Weiterverwendung von veröffentlichten Daten)

.

3. Die bisher im § 1 Abs. 1 enthaltenen Ausnahmen vom Grundrechtsschutz finden sich nunmehr nur hinsichtlich der „*zulässigerweise* allgemein verfügbaren Daten“ im § 1 Abs. 2 wieder.

a) Die Einschränkung auf „*zulässigerweise* allgemein verfügbare Daten“ macht diese Ausnahme insoweit wertlos, als Dritte in vielen Fällen nicht beurteilen können, ob „rechtliche Zulässigkeit der Verfügbarkeit“ vorliegt: So ist es etwa für einen Internetnutzer regelmäßig nicht erkennbar, ob eine datenschutzrechtlich gültige Zustimmung für veröffentlichte personenbezogene Daten eingeholt wurde oder nicht. Ob dieser Effekt weitgehender rechtlicher Unsicherheit über die Zulässigkeit der Weiterverwendung von allgemein verfügbaren Daten in einer Informationsgesellschaft wünschenswert ist, sollte nochmals eingehend überlegt werden. (Sollten Daten unzulässigerweise allgemein verfügbar sein, bestehen ja ohnehin alle Sanktionen – einschließlich von Schadenersatzansprüchen – gegen denjenigen, der die Daten unzulässigerweise allgemein verfügbar gemacht hat und ein Löschungsanspruch gegenüber jener Stelle, bei der die Daten allgemein verfügbar dargeboten werden.)

b) Was nunmehr im Grundrecht fehlt, ist die ausdrückliche Privilegierung der Verwendung von indirekt personenbezogenen Daten, die sich in der Praxis als wichtiges Instrument von „in-built data protection“ erwiesen haben. Durch diese unterschiedliche Behandlung der beiden derzeit in § 1 Abs. 1 enthaltenen Ausnahmen vom Grundrechtsschutz wird eine gewisse Unsicherheit auch dahingehend erzeugt, welche Schlüsse aus dieser ungleichen Behandlung interpretatorisch zu ziehen sind (– vgl hiezu im übrigen auch oben Pkt 2).

C. Zu Z 18, 22, 23, 24, 26 und 27 (**Anwendungsbereich des** einfachgesetzlichen Teils des **DSG**):

Im Gefolge der in der Novelle vorgeschlagenen Verschiebung der Kompetenzgrundlage soll § 58, der bisher die Anwendung des DSG auf „manuelle Dateien" bewirkte, gestrichen werden. Die Geltung des DSG für manuelle Dateien soll nunmehr durch den neuen § 4 Abs. 2 und die Streichung der Bezugnahme auf „Datenanwendung" in den Definitionen von „verwenden", „verarbeiten" und „übermitteln" bewirkt werden – ein Vorhaben, das einfacher durch die Ausdehnung des Begriffes „Datenanwendung" auf die manuell-strukturierte Verwendung personenbezogener Daten erreicht würde.

Die Streichung der Bezugnahme auf die „Datenanwendung" im Begriff des „Verwendens" von Daten soll freilich noch einem weiteren Zweck dienen: Dadurch soll nunmehr die Geltung wesentlicher Teile des einfachgesetzlichen Teils des DSG (DSG-egT) – insbesondere im Rechtsschutzverfahren - **auch** für **manuelle, *nicht* strukturierte Datenverwendung** ausdrücklich festgeschrieben werden (vgl. § 4 Abs. 2). **Dies geht über den von der Richtlinie 95/46 vorgesehenen Anwendungsbereich von Datenschutz eindeutig** – wenn auch angesichts des EG 10 nicht gänzlich unzulässigerweise - **hinaus.** Ob eine derartige erhebliche Abweichung von der RL 95/46 noch zeitgemäß ist, sollte überdacht werden: Ein erkennbares Schutzdefizit besteht heute ja nicht mehr hinsichtlich der Datenverwendung in der „Papierwelt", sondern vielmehr im Hinblick auf die neuen Formen der Informationsverarbeitung, insbesondere im Internet. Aus der Anwendungspraxis der Datenschutzkommission ergibt sich jedenfalls kein Wunsch nach Einführung der vorgeschlagenen Neuregelungen. Dringender Regelungsbedarf scheint vielmehr hinsichtlich des Ausbaus des Rechtsschutzes für die Datenverwendung im Internet zu bestehen, der allerdings im vorliegenden Novellenentwurf nicht angeschnitten wird.

Hinsichtlich der ausdrücklichen Einbeziehung der manuellen, *nicht*-strukturierten Daten in das DSG –egT muss auch darauf aufmerksam gemacht werden, dass den Ausführungen in den Erläuterungen zu Z 18 und 27, wonach „manuelle Daten" nur solche seien, die schriftlich festgehalten sind, nicht ohne Weiteres gefolgt werden kann: Durch den Wegfall des Bezugs zu einer Datenanwendung oder einer Datei in den Definitionen von „Verarbeiten" und „Verwenden" ist es nicht mehr ganz eindeutig, dass nur aufgezeichnete Daten vom DSG 2010 erfasst sein sollen. Es könnte nunmehr wohl auch „Bassenatratsch", - jedenfalls aber eine Notiz darüber- Schutzobjekt des DSG sein. Ob dies angesichts der bekannten Ressourcenknappheit der DSK und der Gerichte sinnvoll ist, darf anheimgestellt werden,

umso mehr als es für diese Fälle ja ohnehin auch andere Schutzmechanismen gibt (vgl. etwa § 1330 ABGB).

D. Z 19 – 26 (**Definitionen**):

1. Definition des „**Auftraggeber**s“ (Z 19) und des „**Dienstleister**s“ (Z 20):

a) In der Praxis hat sich bei der Frage, wer „Auftraggeber“ sein kann, das Problem ergeben, dass durch Auslagerung von Aufgaben aus dem öffentlichen in den privaten Bereich, aber auch durch Schaffung neuer Rechtsträger im öffentlichen Bereich Verschiebungen in der Auftraggebereigenschaft drohen, die nicht sachgerecht sind: Immer wenn durch Gesetz Aufgaben einer Stelle übertragen werden, die nicht (mehr) „Organ einer Gebietskörperschaft“ ist, könnte an sich nur der Rechtsträger, dem die Stelle zuzuordnen ist, Auftraggeber sein, was aber gelegentlich im Widerspruch zur gesetzlichen Aufgabenübertragung steht.
Die Auftraggebereigenschaft sollte daher dahingehend ergänzt werden, dass auch jede Stelle Auftraggeber sein kann, der „gesetzlich Aufgaben übertragen wurden“.

b) Von der Frage, wer aufgrund seines faktischen Verhaltens (d.h. seiner Entscheidung, Daten zu verarbeiten) „Auftraggeber“ ist, ist die Frage zu unterscheiden, wer „rechtmäßiger Auftraggeber“ einer bestimmten Datenverwendung wäre. Angesichts der häufigen Verwechslung dieser Fragestellungen, scheint es erwägenswert, entsprechende Ausführungen in die Erläuterungen aufzunehmen. Die Datenschutzkommission ist gerne bereit, hiezu beizutragen, falls dieser Vorschlag aufgegriffen werden sollte.
Diese Frage ist deshalb von so großer Bedeutung, weil der Betroffene bei einer – fälschlichen - Gleichsetzung dieser Fragestellungen (siehe zu diesem Problem z.B. VfGH Erk 16. Juni 2008, B 494/07-16) Rechtschutz **nicht** gegenüber demjenigen zu suchen hätte, der seine Daten tatsächlich (und vielleicht rechtswidrigerweise) verarbeitet, sondern gegenüber demjenigen, *der zulässigerweise seine Daten verarbeiten dürfte*, was ins Leere gehen muss, wenn der theoretisch hiezu Befugte diese Daten nicht auch *tatsächlich* verarbeitet.

2. Definition der „Datenanwendung“ (Z 21):

a) Ausgehend von den vorstehenden Ausführungen zur Frage des Anwendungsbereichs des DSG sollte der Begriff der **Datenanwendung so definiert werden, dass dadurch der Anwendungsbereich im Hinblick auf die technische Form der Datenverwendung**

abschließend abgegrenzt wird. Falls Daten aus manuell-strukturierten Dateien ausnahmsweise von einer Regelung des DSG nicht betroffen werden sollen, wäre dies bei den einzelnen Regelungen (z.B. über die Meldepflicht) festzuhalten. Der Begriff der „Datenanwendung“ könnte daher definiert werden wie folgt:

„7. Datenanwendung: die Summe der in ihrem Ablauf logisch verbundenen Datenverwendungsschritte, die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind, *unabhängig davon, ob* die dabei verwendeten Daten automationsunterstützt, d.h. maschinell und programmgestützt gespeichert (automationsunterstützte Datenanwendung) *oder in einer manuell geführten Datei (manuelle Datenanwendung) enthalten sind;“*

b) Auch der Dateibegriff bedürfte, wie die Praxis zeigt, einer Schärfung: Als Begründung für Notwendigkeit der Einführung von Datenschutz wird regelmäßig der Umstand angeführt, dass durch strukturierte Aufbereitung von personenbezogenen Daten die Gefahr des Informationszugriffs wächst, weil direkt und daher leichter auf personenbezogene Daten zugegriffen werden kann. Dieses Argument kann auf „Dateien“ nur dann sinnvoll angewendet werden, wenn eine Datei nach einem **personenbezogenen** Suchbegriff (z.B. Namen) geordnet ist, da nur dann ein „Direktzugriff“ auf personenbezogene Informationen möglich ist (- so auch ausdrücklich Erwägungsgrund 27 der RL 95/46). Die Definition der „Datei“ sollte daher wie folgt lauten:

„6. ”Datei”: strukturierte Sammlung von Daten, die nach mindestens einem *personenbezogenen* Suchkriterium *geordnet* sind;“

3. Definition der Begriffe „verwenden“ (Z 22), „verarbeiten“ (Z 23), „ermitteln“ (Z 24) und „übermitteln“ (Z 26):

Ausgehend von den Äußerungen unter Pkt. C und D 2 a) sollten die im Novellen-Entwurf vorgeschlagenen Änderungen dieser Definitionen unterbleiben.

4. **Zusätzlich** zu den vorgeschlagenen Änderungen sollte die im Folgenden dargestellte **Änderung** in Erwägung gezogen werden:

Aufgrund der seit Inkraftsetzung des DSG 2000 gewonnenen Erfahrungen schlägt die Datenschutzkommission vor, im Zusammenhang mit „indirekt personenbezogenen Daten“ folgende definitorische Klarstellungen vorzunehmen:

„1. „……..

nur indirekt personenbezogen sind Daten für einen bestimmten Auftraggeber (Z 4) ~~Dienstleister oder Empfänger einer Übermittlung~~ dann, wenn der Personenbezug der Daten ~~derart~~ *verschlüsselt* ist und dieser Auftraggeber die Identität der Betroffenen *infolge rechtlicher, technischer und organisatorischer Vorkehrungen* nicht bestimmen kann;“

Die umfangreiche Erfahrungen, die die Datenschutzkommission in der Zwischenzeit über die wünschenswerten Rahmenbedingungen für die Verwendung indirekt personenbezogener Daten sammeln konnte, lassen die oben vorgeschlagenen Definitionsänderungen notwendig erscheinen: Durch das alleinige Abstellen auf den jeweiligen *Auftraggeber* wird gesichert, dass der Zweck der Datenanwendung als Maßstab der Glaubwürdigkeit der Verwendung bloß indirekt personenbezogener Daten mitberücksichtigt werden kann. Durch die Miteinbeziehung von technischen und organisatorischen Rahmenbedingungen in die Definition wird klargestellt, dass eine bloße vertragliche Absicherung nicht ausreicht, sondern auch sonstige *faktische* Vorkehrungen getroffen worden sein müssen, die den Zugriff des neuen Nutzers (des „Auftraggebers der Verwendung indirekt personenbezogener Daten“) auf die Entschlüsselungsinstrumente verhindern.

Dass Daten an Dienstleister nur mit verschlüsseltem Personenbezug überlassen werden, sollte hingegen nach den nunmehrigen Erfahrungen nicht als Anlass zur insgesamt privilegierten Datenverwendung unter dem Titel der Verwendung indirekt personenbezogener Daten genommen werden, solange der „Herr der Daten“, nämlich der Auftraggeber über die Entschlüsselungsinstrumente verfügt. (Die Überlassung nur indirekt personenbezogener Daten an einen Dienstleister kann allerdings eine wertvolle zusätzliche Schutzmaßnahme bei der Verarbeitung von Daten mit besonders hohem Nachteilspotential sein, wie z.B. bei Suchtmitteldaten.)

<u>E. Z 31 und 32 (**Internationaler Datenverkehr**):</u>

Auf die in der Stellungnahme zum vorigen Novellenentwurf von der DSK zu § 13 gemachten Anregungen wird nochmals hingewiesen: Es sollte das Registrierungsverfahren vom Genehmigungsverfahren nach § 13 entkoppelt werden und es sollte ausdrücklich festgeschrieben werden, dass Auftraggeber einseitige Erklärungen mit rechtlich verbindlicher Wirkung abgeben können, die die notwendige Publizität durch Eintragung im Datenverarbeitungsregister erlangen.

F. Z 33 – 41 (**Publizität der Datenanwendungen):**

a) Zu Z 37 : Ohne zu verkennen, dass diese Bestimmung an sich als ein weiterer - sinnvoller - Schritt zur Entlastung des Datenverarbeitungsregisters und der meldepflichtigen Behörden gedacht ist, muss doch auf Folgendes hingewiesen werden: Wenn die Festlegung des Inhalts einer Datenanwendung nunmehr durch Verordnung geschehen kann, wird dies zur Folge haben, dass die Rechtsunterworfenen und auch die Datenschutzkommission diese Verordnung für rechtmäßig ansehen müssen, solange die Verordnung nicht vom Verfassungsgerichtshof aufgehoben wurde. Dies sollte zum Anlass genommen werden, der DSK zur Herstellung des notwendigen Gleichgewichts das **Recht der Anfechtung von Verordnungen vor dem Verfassungsgerichtshof** einzuräumen. Sonst könnten nur die Betroffenen in einem kostenaufwendigen Beschwerdeverfahren vor dem VfGH allfällige Argumente gegen die Rechtmäßigkeit des Inhalts der durch die Verordnung geregelten Datenanwendung vorbringen.

b) Im § 19 sollte die generelle Möglichkeit geschaffen werden, dass Auftraggeber **einseitig erklären** können, bestimmte **geeignete Garantien** bei ihrer Datenanwendung **einzuhalten.** Diese Erklärung sollte durch die Registrierung verbindlich werden und durch besondere Strafbestimmung in § 52 sanktioniert werden.
Hinsichtlich näherer Ausführungen verweist die DSK auf ihre Stellungnahme zum seinerzeitigen Entwurf betr. den 4. Abschnitt des DSG (Pkt. 2 der „zusätzlichen Novellierungsanregungen der DSK“).

c) In einem neuen § 24 Abs. 2a (Z 41) soll eine Variante der in Europa derzeit heftig diskutierten „**data breach notification**“ eingeführt werden. Angesichts des Umstands, dass generelle europäischen Regelungen zu diesem Thema in der RL 95/46 (noch) fehlen, könnte es fraglich erscheinen, ob nationale Bestimmungen im gegenwärtigen Zeitpunkt überhaupt zulässig sind. Darüber hinaus bedürfte auch die gewählte Formulierung einer Präzisierung, ua dahingehend, was unter „schwerwiegend unrechtmäßig“ zu verstehen ist.

G. Zu Z 42 – 46 (**Auskunft, Richtigstellung und Löschung**):

1. Die hinsichtlich der Abs. 1 und 4 des § 26 vorgeschlagenen Änderungen sind aus Sicht der DSK nicht erforderlich, da Absatz 4 ohnehin eine „Negativauskunftsverpflichtung “ in Form der Pflicht zur Begründung einer nicht erteilten Auskunft enthält: Wenn keine Daten

verarbeitet werden, muss dies als Begründung der Nicht-Erteilung einer Auskunft (im Sinne des § 26 Abs. 1) angegeben werden.

Eine Ergänzung des § 26 sollte allerdings dahingehend aufgenommen werden, dass bei Fehlen des Identitätsnachweises der Auftraggeber das Auskunftsersuchen nicht ohne Weiteres als unbeachtlich behandeln darf, sondern die Behebung dieses Mangels innerhalb von 8 Wochen nach Eintreffen des Auskunftsersuchens vom Auskunftswerbers nachfordern muss. Erst wenn darauf keine Reaktion des Auskunftswerbers erfolgt, ist das Auskunftsersuchen unbeachtlich, weil nicht rechtsgültig. Die Datenschutzkommission hat diese Vorgangsweise - gestützt auf den Grundsatz von Treu und Glauben nach § 6 Abs. 1 Z 1 DSG 2000 – bereits mehrmals in ihren Entscheidungen vorgeschrieben.

2. Es wird darauf hingewiesen, dass im vorgeschlagenen Text des § 26 Abs. 1 entgegen der Formulierung in Art. 12 der RL 95/46 die Beschränkung auf „*verfügbare*“ Informationen über die Herkunft von Daten fehlt. Allgemein ist wohl davon auszugehen, dass die „Verfügbarkeit“ von derartiger Information nicht allein dem Zufall überlassen bleibt, sondern entsprechend dem Grundsatz von „Treu und Glauben“ nach § 6 Abs. 1 Z 1 DSG 2000 mit der zumutbaren Sorgfalt vorgekehrt sein muss.

3. Die Datenschutzkommission ist weiters der Ansicht, dass eine Klarstellung der inhaltlichen Zugehörigkeit des § 49 Abs. 3 zu § 26 am besten dadurch erzielt werden könnte, dass in § 26 Abs. 1 geregelt wird, dass neben der Bezeichnung allfälliger Dienstleister auch die Logik automatisierter Einzelentscheidungen auf besonderes Verlangen des Auskunftswerbers in allgemein verständlicher Form darzustellen ist.

4. Wie schon in der Stellungnahme zum früheren Novellenentwurf ausgeführt bestünde dringender Regelungsbedarf hinsichtlich der Abgrenzungskriterien nach denen zu entscheiden ist, ob Auskunft über konkrete „Empfänger“ zu geben ist oder eine Auskunft über „Empfängerkreise“ genügt.

5. Auch eine gesetzliche Klärung des Begriffs des „**aktuellen** Datenbestandes“ im Abs. 6 wäre erforderlich.

6 Z 44 wird begrüßt.

7. Zu Z 45: Der letzte Satz des vorgeschlagenen § 26 Abs. 10 scheint eine Zirkelverweisung zu erzeugen, indem er auf § 50 Abs. 1 verweist, der seinerseits auf § 26 Abs. 10 verweist.

8. Der Entfall des Wortes „öffentliche“ in § 27 Abs. 9 scheint nicht ohne Weiteres möglich, da die Begriffe „Bücher“ und „Register“ allein nicht hinlänglich abgrenzend zum Begriff der „Datenanwendung“ sind. Dass aber **für alle** Datenanwendungen von Auftraggebern des öffentlichen Bereichs vom § 27 abweichende Regelungen geschaffen werden könnten, sollte angesichts der Leitfunktion des DSG nicht zulässig gemacht werden.

H. Z 47 (Widerspruchsrecht nach § 28):

1. Die vorgeschlagene Ergänzung des § 28 ist nützlich.

2. Wesentlich wäre jedoch auch der **Ausbau der Rechte der Betroffenen hinsichtlich von Veröffentlichungen im Internet,** wofür § 28 Abs. 2 möglicherweise ein Ansatzpunkt wäre:

a) Vorauszuschicken ist, dass seit der Novelle zum Mediengesetz BGBl I 49/2005 und 151/2005 jeder Betreiber einer Website - aber auch jeder Versender von Massen–Mails - mit gedanklichem Inhalt „Medieninhaber“ im Sinne des Mediengesetzes ist und daher den besonderen Persönlichkeitsschutzbestimmungen des Dritten Teiles des Mediengesetzes unterliegt. **Zusätzlich dazu** unterliegt er dem DSG 2000 zur Gänze, wenn er nicht gleichzeitig ein „Medienunternehmer“ iSd § 48 DSG 2000 ist (Als Medienunternehmen gilt nach § 48 DSG 2000 und – nach den Erläuterungen zu § 1 Abs. 1 Z 6 idF der Mediengesetznovelle 2005 – nur ein solches Unternehmen, dessen Unternehmensgegenstand schwerpunktmäßig journalistischer/publizistischer Natur ist.)

Der Persönlichkeitsschutz nach dem DSG ist in erster Linie auf die Herstellung des rechtmäßigen Zustandes, insbesondere durch Beseitigung (Löschung/Vernichtung rechtswidrig verwendeter Daten) gerichtet. Die Durchsetzung der Beseitigung datenschutzgesetzwidriger Veröffentlichungen im Internet könnte für den Betroffenen erleichtert werden, wenn z.B. das Widerspruchsrecht nach § 28 Abs. 2 DSG 2000 generell auf Veröffentlichungen im Internet, die ohne ausdrückliche gesetzliche Grundlage erfolgen, ausgedehnt würde und zwar unabhängig davon, ob die Veröffentlichung in „Dateien“ erfolgt oder nicht. Dies wäre sachlich dadurch gerechtfertigt, dass durch die flächendeckende Anwendung von Suchmaschinen das Internet ohnehin weitestgehend ein dateiförmig aufbereitetes Informationsangebot enthält.

Zu überdenken wäre auch, inwieweit der Ausschluss der Anwendbarkeit des DSG 2000 auf „Datenverwendung für private Zwecke“ in § 45 DSG 2000 auch für das Internet gelten soll:

Gerade in „Freundschaftsnetzwerken“ können gravierende Datenschutzprobleme durch die Publikation von Daten über „Freunde“ entstehen.

Weiters wäre auch die Bestimmung des § 9 Z 1 DSG 2000, der Daten für nicht-schutzwürdig erklärt, wenn der Betroffene die Daten selbst öffentlich gemacht hat, zu überdenken: Auch wenn dem Betroffenen diesfalls wohl sicherlich vorweg kein Schadenersatzanspruch einzuräumen ist, sollte ihm ein späteres Löschungsbegehren im Hinblick darauf, dass seine Daten auf einer Website dauernd einsehbar dargeboten werden, nicht absolut verwehrt sein.

I. Z 48 – 60 (**Rechtsschutzverfahren** vor der DSK und den ordentlichen Gerichten):

1. Generelle Bemerkungen:
Das Rechtsschutzverfahren, das noch immer weitgehend von historischen (noch aus der Zeit des DSG 1978 stammenden) Ausgangspositionen geprägt ist, bedürfte des grundsätzlichen Überdenkens, auch unter Beachtung der Vorgaben der RL 95/46/EG. Dies gilt vor allem für das Verhältnis der Kompetenzen der Vollzugsorgane DSK und Gerichte, die unterschiedlichen Staatsgewalten angehören, und für die geltenden Sanktionsmöglichkeiten nach § 52.

a) Insbesondere bei der vorgeschlagenen neuen Möglichkeit der DSK (§ 30 Abs. 6a), die Weiterführung einer Datenanwendung bei Gefahr im Verzug mit Mandatsbescheid zu untersagen, wird das Abgrenzungsproblem deutlich und es erhebt sich die Frage, wer bei Datenanwendungen von Auftraggebern des privaten Bereichs zur Beurteilung der Rechtmäßigkeit einer Datenanwendung eigentlich und letztendlich berufen ist – die Datenschutzkommission (und damit der Verwaltungsgerichtshof) oder die Gerichte (und damit der OGH)?

b) Zum geltenden Sanktionensystem finden sich Ausführungen unter Punkt N.

2. Spezielle Bemerkungen zu einzelnen vorgeschlagenen Neuerungen:
a) Zu Z 49 (§ 30 Abs. 5):
Im zweiten Satz der Neuformulierung des § 30 Abs. 5 sollte auch auf die Weiterverwendung von Informationen vor den Verwaltungsstrafbehörden eingegangen werden.

b) Zu Z 50 (§ 30 Abs. 6):
Die Formulierung des § 30 Abs. 6 könnte – schon derzeit – so gelesen werden, dass die Zulässigkeit der Ergreifung der Mittel nach § 30 Abs. 6 Z 1 – 3 an die Bedingung gebunden ist, dass vorher eine Empfehlung erfolglos erstattet wurde. Sollte davon im Interesse beschleunigter Durchschlagskraft der DSK nicht überhaupt Abstand genommen werden, so müsste jedenfalls der Eintritt der Verfolgungsverjährung nach VStG für die Dauer des Verfahrens zur Erlassung einer Empfehlung ausdrücklich ausgeschlossen werden.

c). Zu Z 51 (§ 30 Abs. 6a):
Siehe hiezu die Ausführungen unter Pkt. 1
Weiters ist aufzuzeigen, dass es sich bei der Untersagung einer gesamten Datenanwendung (etwa der Kontenführung einer Bank; vgl auch § 22a Abs des Entwurfs) um einen sehr intensiven Eingriff handelt, der auch die Interessen Dritter massiv betreffen kann. Deren verfahrensrechtliche Stellung bedürfte daher allenfalls einer eigenen Regelung, da das AVG auf das Verfahren nach § 30 nicht zweifelsfrei anwendbar ist.

d) Zu Z 52 (§ 31):
Eine bessere Abgrenzung der Zurechnung von Datenverwendungen zu den unterschiedlichen Staatsgewalten ist sicherlich wünschenswert, da davon die Zuständigkeit zum Rechtsschutz abhängt. Sie sollte aber in § 1 Abs. 5 und in den §§ 31 und 32 in gleicher Weise erfolgen. Auch sollte klargestellt werden, wann nun ein Organ z.B. des Nationalrats „im Dienste der Gesetzgebung“ tätig ist, also ob etwa der gesamte Geschäftsapparat des Parlaments „im Dienste der Gesetzgebung“ tätig ist oder teilweise eben doch nicht „Gesetzgebung“ sondern „Verwaltung“ darstellt.
Auch sollte im Text des § 31 vermieden werden, einmal von „Akte im Dienst der Gesetzgebung oder Gerichtsbarkeit“ (Abs. 1) und einmal von „Organ im Dienst der Gesetzgebung oder Gerichtsbarkeit“ (Abs. 2) zu sprechen.
Voraussichtlich würde es zur besseren Abgrenzung genügen klarzustellen, ob eine Abgrenzung immer nach organisatorischen oder nach materiellen Gesichtspunkten vorzunehmen ist.

e) Die verfahrensrechtlichen Klarstellungen werden begrüßt.
Freilich ergeben sich aus den praktischen Erfahrungen der DSK noch immer viele Detailfragen zum Rechtsschutzverfahren – und zwar zum Teil auch im Hinblick auf die vorgeschlagenen Neuregelungen.

f) Zu Z 53 (neuer § 31a):
§ 31a Abs. 2 soll den vorläufigen Rechtsschutz bei Datenanwendungen von Auftraggebern des öffentlichen Bereichs offenbar an § 32 (gerichtlicher Rechtsschutz) angleichen: Es fehlt jedoch eine Klarstellung, ob ein Antrag des Beschwerdeführers notwendig ist wie im gerichtlichen Verfahren. Auch wäre eine Wortwahl, wonach die Gefahr im Verzug vom Antragsteller *glaubhaft* zu machen ist, besser als die Verwendung des Ausdrucks „zu bescheinigen“, da bei einem so tief greifenden Eingriff in die Aufgaben des Auftraggebers – die auch Dritte, deren Daten verarbeitet werden, betreffen - nur objektiv nachprüfbare Kriterien den Ausschlag geben können. Weiters wäre das Verhältnis des § 31a Abs. 1 DSG (2010) zu § 57 AVG (Mandatsbescheid) zu klären.

Zusammenfassend hält die Datenschutzkommission fest, dass hinsichtlich der vorgeschlagenen Neufassung der §§ 30 und 31 – 31a aus Sicht der DSK noch **Diskussionsbedarf in Detailfragen** besteht.

J. Z 61 – 68 und 70 (Zusammensetzung und Rechtsstellung der DSK):

1. Die Datenschutzkommission weist darauf hin, dass der Datenschutzkommission auch zumindest ein hauptberufliches Mitglied angehören sollte. Dazu würde auch gehören, dass die berufliche Unabhängigkeit des oder der hauptberuflich tätigen Mitglieder so sichergestellt ist, dass die Forderung der RL 95/46/EG (Art. 28) nach „vollständiger Unabhängigkeit“ der nationalen Datenschutzkontrollstelle erfüllt ist. Dies muss nach der ständigen Rechtssprechung des EGMR auch in eine für Außenstehende *sichtbare* Unabhängigkeit münden, was nicht nur rechtliche, sondern auch dementsprechende organisatorische Vorkehrungen erfordert.

2. Mit diesem “Erscheinungsbild“ (vgl etwa *Grabenwarter*, Europäische Menschenrechtskonvention[3], 326) einer unabhängigen Kontrollstelle ist das nunmehr ausdrücklich vorgesehene Recht des Bundeskanzlers, „sich **jederzeit** über alle Gegenstände der Geschäftsführung der Datenschutzkommission beim Vorsitzenden und dem geschäftsführenden Mitglied zu unterrichten“ (§ 38 Abs. 2 letzter Satz in Z 67 des Entwurfs) schwer vereinbar. Es wird außer Streit gestellt, dass dem Anliegen nach Transparenz der Tätigkeit der DSK ein hoher Stellenwert einzuräumen ist. Dem dient die Verpflichtung zur regelmäßigen Berichterstattungspflicht an die Öffentlichkeit gemäß § 38 Abs 4 DSG.

Doch geht es insgesamt um die Dichte der Eingriffe, die im Rahmen der eng in die Verwaltung integrierten Organisationsstruktur der DSK und ihres Geschäftsapparates ermöglicht werden.

Ähnliches ist zu den nach der neuen Z 4a in § 41 Abs. 2 (Z 70 des Entwurfs) nunmehr zusätzlich dem **Datenschutzrat** (in seiner Funktion als Beratungsorgan der Bundesregierung) eingeräumten Aufsichtsrechtsrechten festzuhalten. Dass davon naturgemäß auch die (Geheimhaltungs-)Interessen der Parteien der Verfahren bei der DSK berührt sein können („Einsicht in deren Unterlagen“) ist im Hinblick auf die unterschiedliche Organisationsstruktur von DSK und Datenschutzrat ebenfalls als rechtlich problematisch aufzuzeigen. Dieses Aufsichtsrecht ist im Übrigen weiter als dasjenige, das dem Datenschutzrat gegenüber den Bundesministerien in ihrer Eigenschaft als Auftraggeber des öffentlichen Bereichs zusteht, da es gegenüber der DSK ohne jede einschränkende Bedingung gelten soll.

Wenn den Bedenken gegen ein jederzeitiges Unterrichtungsrecht des Bundeskanzlers entgegengehalten werden sollte, dass dies nur die Umsetzung des Art. 20 Abs. 2 B-VG in der Gestalt der Bundesstaatsreform-Novelle, BGBl. I 2008/2, sei, muss darauf hingewiesen werden, dass Art. 20 Abs. 2 kein geeignetes Organisationsmodell für eine Datenschutz-Kontrollstelle nach Art. 28 der RL 95/46 ist: Diese hat Aufgaben, insbesondere in Form der zwingend vorzusehenden Kontrollkompetenzen, die sinnvollerweise nicht unter der Kontrolle des zu Kontrollierenden ausgeübt werden können.

Dass für die DSK ein besonderes Organisationsmodell notwendig ist, hatte im Übrigen schon der Verfassungsgesetzgeber des Jahres 1978 erkannt, als er im ersten Datenschutzgesetz (1978) die Datenschutzkommission mit einer besonderen, verfassungsgesetzlich eigens abgesicherten Unabhängigkeit ausstattete und in den Erläuterungen darauf hinwies, dass dies erforderlich sei, da der DSK nicht nur Aufgaben im Sinne der Entscheidung über Beschwerdefälle zukämen. Die Zahl dieser andersgearteten Aufgaben der DSK hat sich seit der Umsetzung der RL 95/46 durch das DSG 2000 noch wesentlich vermehrt.

3. Z. 65 (§ 38 Abs. 1)
Die Festlegung der Möglichkeit der Betrauung des geschäftsführenden Mitglieds mit der Erlassung von Mandatsbescheiden im 2. Satz weicht von der Festlegung der Möglichkeit der Erhebung einer Vorstellung in § 40 Abs 1 des Entwurfs ab. Insoweit wäre eine Präzisierung anzustreben.

K. Z 73 – 77 (§§ 46 und 47 DSG):

1. Anstelle der zahlreichen punktuellen Änderungen der Abs. 1 – 3 des § 46 sollte besser eine gesamte bereinigende Neuformulierung dieser Bestimmungen ins Auge gefasst werden.

2. Dem in Z 76 zum Ausdruck kommenden Gedanken ist an sich zuzustimmen. Eigens vorzusehen, dass auch ein Exekutionstitel anstelle der Erklärung des Dateninhabers vorgelegt werden könne, scheint allerdings nicht erforderlich.

3. Im Zusammenhang mit e-Government-Services der Verwaltung für Bürger stellt sich vermehrt das Problem, dass diese meist allein auf die Zustimmung der Betroffenen gegründet werden, was im Bereich der Hoheitsverwaltung nicht ohne Weiteres zulässig ist. Die Schaffung einer eigenen Rechtsgrundlage für Bürgerservices im DSG wäre daher überlegenswert, und zwar z.B. im Anschluss an § 47, der ebenfalls aus der Notwendigkeit von Kommunikationserleichterungen zwischen Verwaltung und Bürger geschaffen wurde.

L. Z 81 (Informationsverbundsysteme, § 50):

Die neue Bestimmung des § 50 Abs. 2a könnte entfallen, wenn - so wie von der DSK vorgeschlagen- die Anerkennung einseitiger Erklärungen im Registrierungsverfahren im § 19 vorgesehen würde. Der Vorteil wäre eine allgemeine Anwendbarkeit dieses Instruments und damit Effizienzsteigerung im Registrierungsverfahren. Es sei außerdem darauf hingewiesen, dass dieses Instrument auch im Genehmigungsverfahren nach § 13 dringend gebraucht wird.

Die Datenschutzkommission ersucht daher um eine entsprechende Änderung der §§ 19 und 13 sowie 52 (Strafbestimmung, wenn einseitig gemachte Zusagen nicht eingehalten werden)**.**

M. Z 82 (Videoüberwachung, §§ 50a – 50e):

Zunächst ist festzuhalten, dass sich in der Zwischenzeit aus der Anwendungspraxis der DSK bereits ein Konzept für die datenschutzrechtliche Behandlung von Videoüberwachung ergeben hat. Im Gegensatz zur seinerzeitigen Stellungnahme der DSK zum Entwurf der Novelle 2008 wird daher eine so umfassende gesetzliche Regelung für die Videoüberwachung nicht mehr als unerlässlich angesehen. Ziel einer neuen gesetzlichen Regelung sollte jedenfalls erhöhte Klarheit über die für die Zulässigkeit von Videoüberwachung entscheidenden Kriterien sein.

1. Zu § 50a (Allgemeines):

a) Der Entwurf geht von einem **Grundkonzept** aus, das von dem von der DSK für die Registrierung von Videoüberwachung entwickelten Konzept in einem wesentlichen Punkt verschieden ist: Während die DSK als Anknüpfungspunkt für die Interessensabwägung im Sinne des § 7 vorrangig die Art des von der Videokamera erfassten Raumes und die darüber bestehende Verfügungsgewalt gewählt hat, wählt der vorliegende Entwurf als Anknüpfungspunkt das mit Hilfe der Videoüberwachung „geschützte Objekt“ bzw. die dadurch „geschützte Person“. Letzteres wird im Konzept der DSK als „Zweck der Videoüberwachung“ releviert. Wie diese beiden Konzepte voll zur Deckung gebracht werden könnten, wäre noch zu diskutieren. Was jedenfalls zu fehlen scheint, ist eine Klarstellung, dass „private“ Videoüberwachung ein „hausrechtsähnliches Verfügungsrecht“ des Überwachenden über den überwachten Raum voraussetzt und dementsprechend im „öffentlichen Raum“ grundsätzlich nicht stattfinden darf.

b) Meist lässt sich nicht vorhersehen, wer von einer Videoüberwachung erfasst sein wird. Abs. 3 enthält nun eine Aufzählung von Fällen, in welchen eine einzelne bestimmte Person von Videoüberwachung nicht beschwert ist – ob dies in allen denkmöglichen Zusammenhängen “richtig“ ist, kann nicht abschließend beurteilt werden, da sich diese Fragen in der Praxis so bisher kaum gestellt haben. Wenn man eine Regelung von der Art des Abs. 3 aber aufnehmen möchte, dann sollte man in dieser Aufzählung auch jene Personen erfassen, die sich *rechtswidrigerweise* im jenem Bereich aufhalten, der von der Videokamera erfasst wird – dies würde z.B. alle Fälle abdecken, in welchen Videokameras nur in der Nachtzeit in einem (versperrten) Bereich in Betrieb genommen werden, in welchem sich rechtens niemand aufhalten sollte.

c) Zielführend wäre es nach Ansicht der DSK, stärker auf unterschiedliche Zwecke von „Videoüberwachung“ einzugehen und dementsprechend zumindest teilweise unterschiedliche Regelungen zu treffen. Der Gebrauch einer Videokamera zum Festhalten des „high life“ in einer Disco bedarf wohl anderer Zulässigkeitsvoraussetzungen als der Einsatz von Videokameras zur Aufzeichnung strafrechtlich relevanten Verhaltens in Fußballstadien.

Sofern der Zweck der Videoüberwachung Eigen- oder Verantwortungsschutz („Schutz von Eigentum, Gesundheit und Leben des Auftraggebers und jener Personen, für die der Auftraggeber besondere rechtlich anerkannte Sorgpflichten hat“) ist, lassen sich aus der

Entscheidungspraxis der DSK **klare Regeln für die Zulässigkeit** ableiten, die im vorliegenden Novellentext nicht ohne weiteres wieder zu finden sind. So wäre es im Interesse der Rechtsklarheit günstig, ausdrücklich festzuhalten, dass

aa) Video*überwachung* für *behördliche* Zwecke nur aufgrund einer ausdrücklichen gesetzlichen Ermächtigung für die einzelne Fallkategorie zulässig ist und dass

bb) Video*überwachung* für *nicht*-behördliche Zwecke nur unter gewissen Bedingungen (- besondere Gefahrensituation -) und zu bestimmten Zwecken (- Eigen- und Verantwortungsschutz des Auftraggebers -) zulässig ist und dass sie sich weiters nicht auf den „öffentlichen Raum“ erstrecken darf, da dieser von jedermann grundsätzlich ungehindert betreten und benützt werden darf.

d) Beim **Verbot der Videoüberwachung zur Mitarbeiterkontrolle** (§ 50a Abs. 5) sollte im Text, zumindestens aber in den Erläuterungen klargestellt werden, dass nur die *Leistungs*kontrolle der Mitarbeiter durch Videoüberwachung verboten ist, hingegen die Kontrolle eines Arbeitsumfelds zu anderen Zwecken, also etwa *zum Schutz* der Mitarbeiter vor besonderen Gefahren (z.B. im Bereich einer gefährlichen Maschine, aber auch der Schalterbereich von Kassenräumen in Banken) oder auch infolge der Besonderheit des Arbeitsbereiches (z.B. Intensivstation oder Aufwachräume einer Krankenanstalt) von diesem Verbot nicht betroffen ist. Desgleichen gehört es zum Stand der Technik, dass besondere Sicherheitszonen, wie etwa Serverräume, unter dauernder Videoüberwachung stehen, um unbefugte Eingriffe hintan zu halten. Letzteres ist zweifellos eine „Kontrolle (auch) der Mitarbeiter“ und darf schon im Interesse des Datenschutzes nicht unmöglich gemacht werden.

2. § 50b (Besondere Protokollierungs- und Löschungspflichten):

a) Ein zentrales Problem der Videoüberwachung ist die Frage, wann eine Auswertung der aufgenommenen Daten zulässig ist und an wen Videoüberwachungsdaten in ausgewerteter Form oder zur Auswertung weitergegeben werden dürfen. Es wäre für den Rechtsunterworfenen wohl klarer, wenn dies nicht nur erschließbar in § 50a Abs. 2, sondern in § 50b ausdrücklich angesprochen würde und dementsprechend auch in der Überschrift erwähnt würde:
Es sollte ein klar formuliertes Verbot der Auswertung ohne Vorliegen des in der Meldung bzw. in gleichwertigen Grundlagen (z.B. Standards) konkret umschriebenen Anlassfalles aufgenommen werden. Dieses Verbot sollte nur insoweit durchbrochen werden dürfen, als die Videoaufzeichnungen im Falle eines staatsanwaltlichen Sicherstellungsauftrags nach § 110 StPO – und offenbar nun auch für sicherheitspolizeiliche Zwecke nach § 53Abs. 5 SPG

auf Anforderung der Sicherheitsbehörden – an die gerichtlichen bzw. sicherheitpolizeilichen Behörden zur Auswertung weitergegeben werden dürfen/müssen.

b) Unklar sind die Konsequenzen von rechtswidrig vorgenommenen Videoaufzeichnungen für ihre spätere Verwertung als Beweismittel. Das gleiche gilt für Zufallsfunde.

c)Zur Frage der angemessenen **Speicherdauer** (über 48 Stunden hinaus) enthält der Entwurf eine Regelung (§ 50b Abs. 2), wonach die Datenschutzkommission dies „festzusetzen“ habe. Dies würde die Möglichkeiten der ressourcenknappen Datenschutzkommission voraussichtlich bei Weitem übersteigen, da eine „Festsetzung“ wohl nur in Form eines Bescheides stattfinden kann. Es wäre sehr hilfreich vorzusehen, dass durch die Aufnahme einer bestimmten Speicherdauer in die Registrierung (samt Begründung der Notwendigkeit für die Abweichung von der gesetzlichen Höchstspeicherdauer) die Speicherdauer als bewilligt gilt. Dadurch bedürfte es regelmäßig keines eigenen Bescheides, wenn dem Antrag gefolgt werden kann, weil er sachlich gerechtfertigt ist. Wenn dem Antrag bezüglich der Speicherdauer hingegen nicht gefolgt werden kann, wäre nach wie vor ein ablehnender Bescheid zu erlassen.

Hinzuzufügen ist, dass nach den praktischen Erfahrungen der DSK eine gesetzliche Speicherdauer von 48 Stunden, die ja den Standardfall darstellen sollte, zu kurz ist, da die meisten Auftraggeber an Wochenenden kein Personal im Einsatz haben, das den Eintritt eines Anlassfalls feststellen könnte. Der Standardfall sollte daher 96 Stunden betragen.

3. § 50c (Meldepflicht und Registrierungsverfahren):

Die Videoüberwachung wird von § 50c allgemein der Vorabkontrolle unterworfen.
Aus Sicht des § 18 Abs. 2 ist dies inkonsequent, da nicht jede Videoüberwachung einen Fall des § 18 Abs. 2 darstellt (vgl. hiezu auch die Spruchpraxis der DSK). Konsequenterweise wäre „Videoüberwachung“ als weiterer Fall in den § 18 Abs. 2 aufzunehmen.

4. § 50e (Auskunftsrecht):

Der Entwurf enthält eine Regelung, die der Judikatur der DSK ohne weiteres Eingehen auf die zugrundeliegenden Probleme widerspricht: Die DSK hat sich in mehreren Fällen eingehend mit der Auskunftserteilung aus Videoaufzeichnungen auseinander gesetzt und das Auskunftsrecht des Auskunftswerbers gegen die Datenschutzrechte der übrigen Betroffenen abgewogen; sie hat weiters eine kurze Speicherdauer in Beziehung gesetzt zu

der durch das Auskunftsbegehren verhinderten Löschung, wodurch für alle Betroffenen die Speicherdauer wesentlich verlängert würde; sie hat außerdem in Rechnung gestellt, dass die verbale Beschreibung des Betroffenen eine klare Identifikation auf Bilddaten, die wesentliche Voraussetzung für eine Auskunftserteilung ist, oft nicht zulässt. Dies alles spricht dafür, dass „Auskunft“ aus Videoüberwachungsdaten im üblichen Sinn die Rechte anderer Betroffener unverhältnismäßig beeinträchtigt, und zwar schon deshalb, weil quasi „künstlich“ ein Anlassfalls für eine Auswertung erzeugt wird, wogegen bei Nicht-Erteilung der Auskunft die Daten *aller* Beteiligten geheim geblieben und innerhalb kürzester Frist - in den Anlassfällen waren es 48 Stunden – gelöscht worden wären. Dies sollte bei der Beurteilung der Frage, ob es nicht einer differenzierteren Regelung bedürfte, beachtet werden.

5. Technischer Fortschritt:

Im Übrigen wird nochmals darauf hingewiesen, dass technische Möglichkeiten der datenschutzfreundlichen Gestaltung von Videoüberwachung entsprechend berücksichtigt und durch Verwendungsprivilegierung gefördert werden sollten. Durch Einsatz von Technik, die z.B. das Entschlüsseln des Abbilds einzelner von mehreren nicht-erkennbar aufgenommenen Person(en) ermöglicht, könnte auch das Problem des Eingriffes in die Datenschutzrechte Dritter bei Auskunftsersuchen aus Videoaufzeichnungen befriedigender gelöst werden als derzeit.
Eine gesetzliche Regelung der Videoüberwachung sollte jedenfalls technische Datenschutzvorkehrungen fördernd miteinbeziehen.

<u>N. Z 83 – 89 (Strafbestimmungen):</u>
Die Reformbedürftigkeit des Sanktionensystems im Datenschutzgesetz – auch unter Beachtung der Vorgabe der RL 95/46 betr. effektive Sanktionen - wurde schon unter Pkt I.1 angesprochen. Dieses Problem bedürfte einer eingehenden Diskussion, zu der die Datenschutzkommission jederzeit gerne zur Verfügung steht.
In einer eben abgeschlossenen Studie betr. die Ausgestaltung des Sanktionensystems in den NL, B, F, D, Lux und Ö hat sich jedenfalls herausgestellt, dass in Ö die Strafrahmen des § 52 weit unter jenen der anderen Staaten liegen.

14. Juli 2009
Für die Datenschutzkommission
Der stellvertretende Vorsitzende:
HR des OGH Dr. KURAS

Für die Richtigkeit
der Ausfertigung: