WIRTSCHAFTSKAMMER ÖSTERREICH

Bundeskanzleramt
Verfassungsdienst
per Mail: v@bka.gv.at

Wiedner Hauptstraße 63 | Postfach 195
1040 Wien
T +43 (0)5 90 900DW | F +43 (0)5 90 900114225
E margit.hirmann@wko.at
W www.wko.at/rp

cc: begutachtungsverfahren@parlament.gv.at

| Ihr Zeichen, Ihre Nachricht vom | Unser Zeichen, Sachbearbeiter | Durchwahl | Datum |
|---|---|---|---|
| BKA 810.026/0005-V/3/2009; 20.5.2009 | Rp 1761/09/Ro/MH | 3215 | 12.06.2009 |

**Entwurf eines Bundesgesetzes, mit dem das Bundes-Verfassungsgesetz, das Datenschutzgesetz 2000 und das Sicherheitspolizeigesetz geändert werden (DSG-Novelle 2010); Stellungnahme**

Sehr geehrte Damen und Herren!

Die Wirtschaftskammer Österreich teilt zu dem im Betreff genannten Entwurf Folgendes mit:

## 1. Allgemeines:

Im Vergleich zum Entwurf einer „DSG-Novelle 2008" ist zum nunmehr vorliegenden Entwurf positiv hervorzuheben, dass juristische Personen und Personengemeinschaften auch weiterhin dem Anwendungsbereich des Datenschutzgesetzes unterliegen sollen und dass der betriebliche Datenschutzbeauftragte, der im DSG-Novellenentwurf 2008 vorgesehen war und aus Sicht der Wirtschaft nur zu unverhältnismäßig hohen Kosten ohne einen Mehrwert geführt hätte, nunmehr nicht Eingang in das Gesetz findet.

Datenschutz ist eine für die Wirtschaft wichtige Rechtsmaterie; diese sollte jedoch nicht dazu führen, dass sowohl wirtschaftlich als auch juristisch notwendige, sinnvolle und auch europarechtlich vorgegebene Maßnahmen nicht adäquat umgesetzt werden können.
In diesem Zusammenhang wird insbesondere auf die in der Verbraucherkredit-Richtlinie, 2008/48/EG, vorgesehene Verpflichtung der kreditgebenden Wirtschaft verwiesen, wonach vor der Kreditvergabe Erkundungen über die Bonität der Kreditnehmer einzuholen sind.
(Höchst)gerichtliche Entscheidungen (vgl. insbes. OGH 1.10.2008, 6 Ob 195/08g) erschweren allerdings die Umsetzung der Vorgaben der Verbraucherkredit-Richtlinie, da Bonitätsdatenbanken von Kreditauskunfteien als „öffentlich zugängliche Dateien" iS des § 28 Abs 2 DSG 2000 qualifiziert wurden und damit jeder Betroffene ohne Angabe von Gründen gegen die Aufnahme in Bonitätsdatenbanken Widerspruch erheben kann.

Um der kreditgebenden Wirtschaft die Umsetzung jener Verpflichtungen aus der Verbraucherkredit-Richtlinie zu ermöglichen bzw generell die (volks-)wirtschaftlichen Erfordernisse in Zeiten der Wirtschafts- und Finanzkrise zu berücksichtigen, wird dringend angeregt, die Bestimmung des § 28 Abs 2 DSG 2000 entsprechend anzupassen (im Detail vgl. die Bemerkungen unten zu Z 46 und 47).

## 2. Zu den Bestimmungen im Einzelnen:

### Zu Art 1:

Die Zuordnung des „Schutzes personenbezogener Daten“ zur Gänze in die Gesetzgebungs- und Vollziehungskompetenz des Bundes wird begrüßt.

### Zu Art 2:

### Zu Z 11 und Z 12 (§ 1):

Die Aufrechterhaltung des Datenschutzes für juristische Personen und Personengemeinschaften ist ausdrücklich zu begrüßen.

Der Anspruch auf Geheimhaltung besteht gemäß § 1 Abs 2 des Entwurfes nur mehr dann nicht, „wenn Daten zulässigerweise allgemein verfügbar sind“. Der Entfall des Passus „oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind“ des geltenden § 1 Abs 1 wird in den Erläuterungen damit begründet, dass es selbstverständlich scheint, „dass Daten nur dann personenbezogen sein können und unter den Grundrechtstatbestand fallen, wenn eine Rückführbarkeit auf den Betroffenen möglich ist, wie das im Übrigen auch bei indirekt personenbezogenen Daten der Fall ist“. Jedenfalls müsste aber klargestellt sein, dass eine ausreichende Grundlage für die einfachgesetzlichen Sonderregelungen für indirekt personenbezogene Daten gegeben ist.

### Zu Z 19 (§ 4 Abs 1 Z 4):

Die ausdrückliche Klarstellung betreffend „Ermittlungsdienstleister“ wird begrüßt.
Zum letzten Halbsatz dieser Bestimmung fällt auf, dass anstelle der bisherigen Formulierung „aufgrund von Rechtsvorschriften, Standesregeln oder Verhaltensregeln gemäß § 6 Abs 4“ nur mehr von „Rechtsvorschriften und Verhaltensregeln“ die Rede ist. Zumindest in den Erläuterungen müsste daher ausdrücklich klargestellt werden, dass unter „Verhaltensregeln“ sowohl Standesregeln als auch Verhaltensregeln gemäß § 6 Abs 4 zu verstehen sind (derzeit ist in den Erläuterungen nur von „ Rechtsvorschriften“ die Rede). Weiters sollte - wie in der bisherigen Formulierung - im Gesetzestext ausdrücklich klargestellt sein, dass in den Fällen des letzten Halbsatzes der mit der Herstellung des Werkes Betraute als datenschutzrechtlicher Auftraggeber gilt.

### Zu Z 20 (§ 4 Abs 1 Z 5):

Entgegen der bisherigen DSK-Judikatur soll - wie die Erläuterungen zu dieser Bestimmung ausführen - als Dienstleister nicht angesehen werden, wer mit der Herstellung eines Werkes betraut ist und für die zu diesem Zweck überlassenen Daten ein Entgelt leistet. Der Grund für dieses Abgehen von der DSK-Judikatur ist nicht ersichtlich. Dieser Aussage in den Erläuterungen wird daher entgegengetreten.

### Zu Z 27 (§ 4 Abs 2):

Fraglich ist in diesem Zusammenhang der Bedeutungsinhalt des letzten Satzes dieser Bestimmung, insbesondere dahingehend, dass „für alle übrigen manuellen Daten“ auch die Bestimmungen „des 6. Abschnittes sinngemäß“ gelten. Die Rechte auf Auskunft, Richtigstellung

und Löschung, deren Verletzung nach den Bestimmungen der §§ 31 und 32 auch geltend gemacht werden kann, stehen nämlich nur bei automationsunterstützter Verarbeitung oder manuellen Dateien zu.

Diese Ausweitung des Geltungsbereichs des einfachgesetzlichen Teils des DSG 2000 auf manuelle nicht strukturiert geführte Daten scheint überhaupt überschießend: So führt Erwägungsgrund 27 der Richtlinie 95/46/EG aus, dass die Richtlinie bei manuellen Verarbeitungen lediglich Dateien erfasst, nicht jedoch unstrukturierte Akten. Dabei muss der Inhalt einer Datei nach bestimmten personenbezogenen Kriterien strukturiert sein, die einen leichten Zugriff auf die Daten ermöglichen. Die Mitgliedstaaten können die Kriterien zur Bestimmung der Elemente einer strukturierten Sammlung personenbezogener Daten sowie die verschiedenen Kriterien zur Regelung des Zugriffs zu einer solchen Sammlung festlegen. „Akten und Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien strukturiert sind, fallen unter keinen Umständen in den Anwendungsbereich dieser Richtlinie."

Die Ausdehnung der Gültigkeit des einfachgesetzlichen Teiles des DSG 2000 bzw bestimmter Passagen auf „alle übrigen manuellen Daten" geht somit über den von der Richtlinie 95/46/EG vorgesehenen Anwendungsbereich hinaus; die Regelung ist daher problematisch.

**Zu Z 33 - 34 (§ 16):**

Nach § 16 Abs 2 kann jedermann in das Datenverarbeitungsregister Einsicht nehmen. Es müsste sichergestellt werden, dass künftig auch die elektronische Einsichtnahme möglich ist.

**Zu Z 35 (§ 17 Abs 1):**

Die vorgesehe Änderungsmeldung ist prinzipiell zu begrüßen. Es sollte jedoch eine Befristung mit aufgenommen werden. Dies könnte dadurch geschehen, dass festgelegt wird, dass die Meldepflicht bei der Änderungsmeldung dann als erfüllt gilt, wenn diese innerhalb von sechs Monaten erfolgt.

**Zu Z 36 (§ 17 Abs 1a):**

Nach Abs 1a soll die Meldung einer Datenanwendung zur Registrierung im Datenverarbeitungsregister in elektronischer Form im Wege der vom Bundeskanzler bereit zu stellenden Internetanwendung einzubringen sein. Eine Meldung in nicht-elektronischer Form soll (nur) für manuelle Dateien sowie bei einem längeren technischen Ausfall der Internetanwendung zulässig sein.

Wenngleich die Möglichkeit der Nutzung des Internets zur Meldung einer Datenanwendung zu begrüßen ist, ist ein Zwang dazu abzulehnen. Es sollte daher weiterhin generell dem Meldepflichtigen überlassen bleiben, ob er die (konventionelle) Schriftform oder die elektronische Form der Anmeldung wählt.

Begrüßt wird das Absehen von der verpflichtenden Verwendung der Bürgerkarte zum Zwecke der Identifizierung und Authentifizierung. In der neuen Bestimmung des § 17 Abs 1 a wird allerdings normiert, dass die näheren Bestimmungen über die Identifizierung und Authentifizierung in einer Verordnung zu regeln sind. Hier wäre sicherzustellen, dass eine Verpflichtung zur Verwendung der Bürgerkarte nicht über den Umweg der Verordnung geschaffen wird. Die Bürgerkarte kann nur als fakultatives, nicht aber als verpflichtendes Identifizierungs- und Authentifizierungsmittel in Frage kommen.

Zu hinterfragen ist der letzte Satz dieser Bestimmung: Bezieht sich der technische Ausfall der Internetanwendung auch auf die Nutzerseite oder lediglich auf die DVR-Seite? Unklar ist weiters die Formulierung „längerer technischer Ausfall“: Wann ist dies erfüllt? Nach zwei Tagen oder erst nach Wochen? Dies ist nicht zuletzt für die Aufnahme der Datenanwendung relevant (§ 18 Abs 1). Daher wird nochmals auf das eingangs vorgebrachte Anliegen hingewiesen, dass es dem Meldepflichtigen generell überlassen bleiben soll, ob er der Meldepflicht elektronisch oder manuell nachkommen will.

**Zu Z 39 (§ 20 - 22):**

In § 20 Abs 4 sollte es lauten: „unter Setzung einer angemessene Frist“.

In § 21 Abs 1 Z 4 müsste auch auf vorgenommene Verbesserungen gemäß Abs 2 Bezug genommen werden, sofern auf diesen Fall nicht bereits Z 2 Anwendung finden soll; Letzteres wäre aber klarzustellen.

Die Datenschutzkommission soll nach § 22 Abs 2 letzter Satz ohne Ermittlungsverfahren registrierte Datenanwendungen streichen können, wenn ihr „zur Kenntnis gelangt“, dass diese dauerhaft nicht mehr betrieben werden. Diese Bestimmung zur Beseitigung offensichtlicher Karteileichen aus dem DVR sollte dahingehend ergänzt werden, dass es keinen wie immer gearteten Zweifel geben darf, dass eine Datenanwendungen wirklich für immer eingestellt wurde.

Nach § 22 Abs 4 kann der Rechtsnachfolger eines registrierten Auftraggebers einzelne oder alle registrierten Meldungen des Rechtsvorgängers übernehmen, wenn er innerhalb von zwei Monaten nach Wirksamkeit der Rechtsnachfolge eine entsprechend glaubhaft gemachte Erklärung gegenüber der Datenschutzkommission abgibt.

Da es sich hier um Vorgänge der Rechtsnachfolge handelt, müssen (auch) die aus der Anmeldung für den Rechtsvorgänger sich ergebenden Rechtspositionen im Zuge dieser Nachfolge übergehen, ohne dass es einer Erklärung bedarf. Der Rechtsnachfolger sollte lediglich verpflichtet werden, die Rechtsnachfolge unter Glaubhaftmachung dieses Vorganges der Datenschutzkommission zu melden, wobei es ihm freilich auch freistehen soll, zu erklären, alle oder bloß einzelne Datenanwendungen nicht zu übernehmen.

Sollte dies nicht entsprechend geändert werden, so ist darauf hinzuweisen, dass im Hinblick darauf, dass zum Zeitpunkt der Rechtsnachfolge ein Unternehmen eine Vielzahl von Veränderungen treffen und viele Entscheidungen zu fällen sind, die Frist für die Erklärung gegenüber der Datenschutzkommission zu kurz ist und daher erheblich verlängert werden müsste.

Daneben kommt es bei Rechtsnachfolge in der Regel auch zu Umstrukturierungen, so dass am Anfang nicht klar ist, welche Datenanwendungen tatsächlich noch aktuell sind bzw benötigt werden. Auch deshalb sollte die Frist verlängert werden. Durch die Verlängerung der Frist kann auch dem Datenverarbeitungsregister Arbeit erspart werden. Ansonsten wäre binnen 2 Monaten eine Meldung einzubringen; in Folge, nach Vornahme der Umstrukturierungen, käme es zu weiteren (Änderungs)meldungen.

Aus Sicht der Bundessparte Information und Consulting sollte im Register dafür gesorgt werden, dass der „historische“ Auftraggeber der Datenanwendung sowie der Zeitpunkt der Rechtswirksamkeit der Übernahme vermerkt ist.

**Zu Z 41 (§ 24 Abs 2a):**

Mit dieser Bestimmung soll eine neue besondere Informationsverpflichtung für Auftraggeber geschaffen werden: Wenn dem Auftraggeber bekannt wird, dass Daten aus einer seiner Datenanwendungen systematisch und schwerwiegend unrechtmäßig verwendet wurden, hat er darüber unverzüglich die Betroffenen zu informieren. Nach den Erläuterungen soll dies vor allem der Vermeidung von Vermögensschäden der Betroffenen dienen. Diese Bestimmung ist aus mehreren Gründen problematisch: Zum einen wird nicht näher ausgeführt, wann davon auszugehen ist, dass Daten „systematisch und schwerwiegend unrechtmäßig verwendet" wurden und kommt es nach dem Wortlaut der Bestimmung gar nicht darauf an, ob überhaupt ein Schaden für Betroffene droht, zum anderen ist nicht klar, wie die Information zu erfolgen hat: An jeden Betroffenen gesondert, durch öffentliche Bekanntmachung oder auf sonstige Weise? Abgesehen davon, dass großer Aufwand für Auftraggeber entstehen könnte, käme eine solche Information u.U. auch einer Selbstbezichtigung gleich, die auch im Lichte des Art 6 EMRK problematisch wäre.

**Zu Z 42 (§ 26 Abs 1):**

Hier wird im Text das Wort „verfügbaren" in Bezug auf die Informationen über die Herkunft der Daten gestrichen.
Der geltende Text entspricht Art 12 lit a der RL 95/46/EG und muss daher jedenfalls beibehalten werden.

Nach Abs 1 hat ein Auftraggeber jeder natürlichen Person oder Personengemeinschaft, die dies schriftlich verlangt und ihre Identität in geeigneter Form nachweist, Auskunft über die zu dieser Person oder Personengemeinschaft verarbeiteten Daten zu geben. Wenn zur Person des Auskunftswerbers keine Daten vorhanden sind, genügt die Bekanntgabe dieses Umstandes (Negativauskunft).

Um dem damit verbundenen Aufwand Rechnung zu tragen, vor allem aber auch, um Missbräuche oder gar schikanöse Anfragen zu verhindern, sollte der Auftraggeber berechtigt sein, die Auskunft von der vorherigen Leistung eines Kostenersatzes in angemessener Höhe abhängig zu machen. Dies sollte jedenfalls für die Negativauskunft gelten.

**Zu Z 43 (§ 26 Abs 6):**

Der pauschalierte Kostenersatz ist mit Euro 18,89 festgelegt. Einerseits scheint hier eine Valorisierung und andererseits eine Glättung des Betrages zB auf Euro 25,00 angemessen.

Angeregt wird auch eine Präzisierung der Formulierung „im laufenden Jahr": Ist damit das Kalenderjahr gemeint oder, bei Unternehmen mit abweichendem Wirtschaftsjahr, dieses?

**Zu Z 45 (§ 26 Abs 10):**

In dieser Bestimmung wird jedem Dienstleister aufgetragen, den Auftraggeber namhaft zu machen, wenn er (vom Auskunftswerber irrtümlich) als Auftraggeber betrachtet wird. Alternativ kann das Auskunftsbegehren an den Auftraggeber weitergeleitet werden und ist der Auskunftswerber davon zu verständigen.

Diese Bestimmung ist in mehrfacher Hinsicht unklar:

Während im Text vom Irrtum hinsichtlich der Rollenverteilung zwischen Auftraggeber und Dienstleister die Rede ist, löst nach den (unpräzise formulierten) Erläuterungen offenbar jeder „Irrtum" eine Antwortverpflichtung aus, also auch etwa dann, wenn der Auskunftswerber den Dienstleister selbst für auskunftspflichtig hält.

Ein besonderes Problem stellt diese Bestimmung in Verbindung mit der Negativauskunft gem. § 26 Abs1 dar. Die Auskunftspflicht gemäß der Bestimmung des § 26 Abs 10 ist ein Derivat des Auskunftsanspruches. Daher ist der Auskunftsanspruch offenbar von einer tatsächlichen Datenverwendung (der Daten eines bestimmten Betroffenen) unabhängig. Daraus könnte u.U. geschlossen werden, dass der Dienstleister jeden möglichen Auftraggeber, also jeden Kunden bekannt geben muss. Die Verpflichtung zur Nennung von Kunden ist ein Eingriff in die Geschäftsgeheimnisse und kann keinem Unternehmer auferlegt werden (insbesondere wenn es sich beim Auskunftswerber um jemanden handelt, dessen Daten nicht verwendet wurden).

Unklar ist weiters, wie ein „Irrtum" nach § 26 Abs 10 zu Stande kommen sollte. Es ist nicht sehr wahrscheinlich, dass ein Betroffener einen Dienstleister kennt, der grundsätzlich nicht in Erscheinung tritt, nicht aber den Auftraggeber.

Das Gesetz lässt zusätzlich offen, wer die Beweislast dafür trägt, dass „ein an ihn gerichtetes Auskunftsbegehren" erkennen lässt, dass der Auskunftswerber ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält.

Weiters können beim Dienstleister durch die Anfragen erhebliche Aufwendungen entstehen (Identitätsprüfung, Protokollierungen der Antworten an den Auskunftswerber, etc.).

**Zu Z 46 und 47:**

Die Bundessparte Information und Consulting weist auf Folgendes hin: „Im Gegensatz zu § 26 (Auskunftsrecht) enthält auch der Entwurf zu § 27 (Recht auf Richtigstellung oder Löschung) und § 28 (Widerspruchsrecht) weiterhin keine Bestimmung für eine Verpflichtung des Betroffenen, seine Identität in geeigneter Form nachzuweisen. Dies stellt in der Praxis eine erhebliche Rechtsunsicherheit, sowohl für den Betroffenen, als auch die Kreditauskunfteien dar, da bestenfalls eine nachträgliche Identitätsprüfung möglich ist und einem Missbrauch „Tür und Tor" geöffnet sind. Es wird daher vorgeschlagen, eine Nachweispflicht der Identität in den §§ 27 und 28 analog zu § 26 DSG 2000 vorzusehen."

Im Entwurf ist folgender neuer § 28 Abs 3 enthalten: „§ 27 Abs 4 bis 6 gelten auch in den Fällen der Abs 1 und 2". Diese Anordnung ist insbes. im Hinblick auf § 28 Abs 2 unklar und entbehrlich.

**Zu § 28 Abs 2 geltende Fassung (Widerspruchsrecht):**

§ 28 Abs 2 DSG sieht in der geltenden Fassung ein Recht des Betroffenen vor, gegen eine nicht gesetzlich angeordnete Aufnahme in eine öffentlich zugängliche Datei jederzeit auch ohne Begründung seines Begehrens Widerspruch zu erheben.

In mehreren gerichtlichen Entscheidungen (vgl. insb. auch OGH 1.10.2008, 6 Ob 195/08g) wurden die Bonitätsdatenbanken von Kreditauskunfteien als „öffentlich zugängliche Dateien" i.S. des § 28 Abs 2 DSG 2000 eingestuft.

Dies führt zu dem wirtschaftspolitisch ungewollten Ergebnis, dass aufgrund von Widersprüchen richtige und aktuelle Bonitätsdaten zu löschen sind und Kreditgebern nicht mehr zur Verfügung gestellt werden können. Die Qualität der Kreditprüfung wurde durch dieses Widerspruchsrecht erheblich gesenkt. In Zeiten der Finanzkrise ist es im Allgemeininteresse und von großer Relevanz, dass Kreditgeber über profunde Informationen über die Bonität verfügen, um sich ein genaues Bild machen zu können. Dies trifft auf alle kreditgebenden Unternehmen zu und dient überdies auch dem Konsumentenschutz. Wenn einem überschuldeten Verbraucher mangels Kenntnis des Kreditgebers über die Bonität weiterhin Kredite gewährt werden, hat dies negative wirtschaftspolitische und konsumentenschutzrechtliche Effekte.

Sollte, was aufgrund aktueller Entwicklungen in der Judikatur nicht auszuschließen ist, die Geltung des generellen Widerspruchsrechts gem. § 28 Abs 2 DSG 2000 auch für die Kleinkreditevidenz und die Warnliste der Österreichischen Kreditinstitute angenommen werden, so hätte dies noch weitergehende gravierende Auswirkungen auf den Wirtschaftsstandort Österreich.

Die Notwendigkeit für das Führen der Warnliste und KKE ergibt sich aus:

- § 39 BWG - Sorgfaltspflichterfüllung
- FMA-Mindesstandards für das Kreditgeschäft und andere Geschäfte mit Adressenausfallsrisiko vom 13.01.2005
- Solvabilitätsregime: §§ 22ff BWG, Solvabilitätsverordnung
- Leitfaden der OeNB und FMA zum Thema Kreditvergabeprozess und Kreditrisikomanagement aus 2004
- Verbraucherkredit-Richtlinie, 2008/48/EG.

Die Kreditinstitute müssen sich im Rahmen ihrer Geschäftstätigkeit an obige Bestimmungen halten.

Eine Auslegung des § 28 Abs 2 DSG 2000, wonach auch gegen eine Aufnahme in die oben genannten Dateien jederzeit Widerspruch ohne Begründung erhoben werden kann, steht im Widerspruch zu diesen Bestimmungen.

Aufgrund der Entwicklungen in der Rechtsprechung muss, um verlässliche Bonitätsinformationen für die kreditgebende Wirtschaft gewährleisten zu können, anlässlich der Datenschutzgesetz-Novelle 2010 eine adäquate Lösung gefunden und § 28 Abs 2 DSG 2000 entsprechend neu formuliert werden. Diese Notwendigkeit ergibt sich insbesondere auch im Hinblick auf die Vorgaben aus der Verbraucherkredit-Richtlinie, die bis spätestens 12. Mai 2010 umzusetzen ist.

**Zu Z 48 (§ 30 Abs 2a):**

Die Bezugnahme auf Abs 1a (der im Entwurf nicht mehr enthalten ist) hat zu entfallen.

**Zu Z 49 (§ 30 Abs 5):**

In diese Bestimmung soll folgender Passus eingefügt werden: „Dazu zählt auch die Verwendung für Zwecke der gerichtlichen Rechtsverfolgung durch den Einschreiter oder die Datenschutzkommission nach § 32."

Diese Bestimmung stellt einen erheblichen Eingriff in die Rechtssphäre aller der Kontrolle der Datenschutzkommission unterliegenden Unternehmen dar und ist aus folgenden Gründen abzulehnen: Durch diese Erweiterung können alle Informationen, die durch die Kontrolltätigkeit

der Datenschutzkommission erlangt werden, für zivilrechtliche Prozesse verwendet und dadurch mittelbar an die Öffentlichkeit herangetragen werden. Dadurch wird der Datenschutz von Geschäftsgeheimnissen aller von der Datenschutzkommission kontrollierten Unternehmen ausgehöhlt. Die Aussage in den Erläuterungen, wonach das Gericht einem besonderen Geheimhaltungsinteresse durch Ausschluss der Öffentlichkeit auf Grundlage der ZPO Rechnung tragen kann, hängt letztlich von einem Ermessen des entscheidenden Gerichtes ab und ist daher kein taugliches Mittel, die mit dieser Regelung einhergehende Aushöhlung des Datenschutzes von Geschäftsgeheimnissen zu kompensieren.

Es käme angesichts der der Datenschutzkommission zustehenden Ermittlungsbefugnisse weiters zu einem mit den Grundsätzen der ZPO nicht zu vereinbarenden Waffenungleichgewicht, würden doch nach dem vorliegenden Vorschlag behördlich ermittelte Informationen insbesondere auch in einem zwischen privaten Parteien anhängigen Zivilprozess zu Lasten einer der Parteien eingebracht.

Bei Umsetzung dieser Bestimmung würde die DSK weiters ihrer Amtsverschwiegenheit enthoben. Bei Gericht vorgelegte Akten sind parteiöffentlich und die Parteien können nicht effektiv zur Geheimhaltung gezwungen werden.

Im Übrigen sind Einschränkungen der Amtsverschwiegenheit generell kritisch zu betrachten.

**Zu Z 50 (§ 30 Abs 6):**

Seitens der Bundessparte Information und Consulting wird zu dieser Bestimmung Folgendes ausgeführt: „Das DSG sieht quasi als ein Mittel zur Herstellung eines datenschutzrechtlich konformen Zustandes die Empfehlung vor. Vor Erlassung einer Empfehlung wird zwar der Auftraggeber angehört, doch hat er keine weiteren rechtlichen Möglichkeiten seine Rechtsmeinung hinsichtlich des Gegenstandes des „Eingabeverfahrens“ zu vertreten bzw gegen die Empfehlung vorzugehen.
Es wird daher angeregt, dass die Empfehlungen nur für die Einschreiter und den Auftraggeber veröffentlicht werden.“

**Zu Z 51 (§ 30 Abs 6a):**

Durch diese Bestimmung wird die Möglichkeit geschaffen

- ohne verfahrenseinleitenden Akt,
- ohne Ermittlungsverfahren,
- ohne aufschiebende Wirkung

per Mandatsbescheid ganze Anwendungen zu untersagen.

Damit kann die wirtschaftliche Tätigkeit eines Unternehmens massiv eingeschränkt werden, wenn das Unternehmen damit nicht sogar in den Ruin getrieben wird. Angesichts des fehlenden Parteiengehörs für den Auftraggeber und des unbestimmten Begriffes der „*wesentlichen Gefährdung schutzwürdiger Geheimhaltungsinteressen*“ ohne jegliche Determinierung ist diese Bestimmung gerade wegen der gravierenden Konsequenzen, die aus einem solchen Eingriff entstehen können, in grundrechtlicher Hinsicht äußerst bedenklich und wird daher abgelehnt.

Sollte diese Bestimmung trotz dieser Ablehnung beibehalten werden, müsste zumindest vorgesehen werden, dass eine Vorstellung gem § 57 Abs 2 AVG auch in diesem Falle aufschiebende Wirkung haben kann.
Auch sei darauf hingewiesen, dass „Gefahr im Verzug" eine (zeitlich) „unmittelbare" Gefährdung voraussetzt, was im Entwurfstext nicht zum Ausdruck kommt.

**Zu Z 52 (§ 31):**

In Abs 1 müsste es - in Entsprechung zu § 26 - lauten „... über Beschwerden von Personen und Personengemeinschaften".

Die Bundessparte Bank und Versicherung führt zu dieser Bestimmung aus: „Die automatisierten Einzelentscheidungen werden bei Bonitätsprüfungen verwendet. In diesem Bereich kommt es zum Einsatz sogenannter Scorecards, deren Abläufe nur das jeweilige Kreditinstitut kennt. Durch Offenlegung des Ablaufs der automatisierten Entscheidungsfindung kommt es zur Offenlegung wesentlicher Teile des Betriebsgeheimnisses. Daher stehen wir dem neuen in § 31 (1) geregelten Beschwerderecht sehr kritisch gegenüber.

In diesem Zusammenhang ist auch darauf hinzuweisen, dass das Erklären der Scorecard sehr aufwändig bzw für Nichtfachleute nur sehr schwer verständlich ist."

**Zu Z 53 (§ 31a):**

In Abs 2 kann es keinesfalls ausreichen, dass der Beschwerdeführer „eine wesentliche Beeinträchtigung seiner schutzwürdigen Geheimhaltungsinteressen bescheinigt". Es müssten jedenfalls objektive Kriterien erfüllt sein und eine unmittelbare Gefährdung vorliegen, damit die Datenschutzkommission nach § 30 Abs 6a vorgehen kann. Im Übrigen wird auf die Bemerkung zu § 30 Abs 6a und die Ablehnung dieser Bestimmung hingewiesen.

**Zu Z 55 (§ 32 Abs 4):**

Schon bisher gab es eine doppelte Zuständigkeit (Ort des Beklagten und Ort des Klägers) - nun soll eine dritte hinzukommen (Ort einer Niederlassung des Beklagten). Aus rechtsökonomischer Sicht wäre ein einheitlicher Gerichtsstand mit dem Ort des Beklagten bei weitem vorzuziehen: Datenschutzrecht ist eine rechtlich komplexe und IT-technisch enorm verzahnte Materie. Jedes Gericht muss sich in einem aufwändigen Beweisverfahren Kenntnisse und Verständnis des jeweiligen Datenmodells verschaffen. Und dies ist bei jedem Auftraggeber anders, selbst wenn es sich um ähnliche Geschäftsmodelle handelt. Daher scheint es sinnvoll, alle Verfahren zu einem Auftraggeber örtlich zu konzentrieren. Besser wäre also statt Schaffung zahlreicher weiterer Gerichtsstände die Konzentration auf einen einzigen im Sinne einer Senkung der Rechtskosten.

**Zu Z 57 (§ 32 Abs 7):**

Diese Regelung scheint zu weitgehend: Zum einen ist auch nach § 31a Abs 1 nur „erforderlichenfalls" nach den §§ 22 und 22a vorzugehen, zum anderen ist eine Verständigung der Parteien durch das Gericht überschießend.

**Zu Z 81 (§ 50 Abs 2a):**

Nach Abs 2a sollen weitere Teilnehmer an einem Informationsverbundsystem die Meldung auf einen Verweis auf den Inhalt der Meldung eines bereits registrierten Auftraggebers beschränken können, wenn sie eine Teilnahme im genau gleichen Umfang anstreben. Es sollte klargestellt werden, dass dies auch dann möglich ist, wenn die Meldung nach Abs 2 durch den Betreiber vorgenommen wurde.

**Zu Z 82 (9a Abschnitt Videoüberwachung, §§ 50a bis 50e):**

Grundsätzlich wird die Schaffung von expliziten Regelungen für die Zulässigkeit von Videoüberwachung begrüßt; jedoch sind die vorgeschlagenen Regelungen im Einzelnen nach wie vor praxisfern und wird dem Gedanken der Prävention durch Videoüberwachung nicht in ausreichendem Maße Rechnung getragen.

Nicht zuletzt um den mit der Meldepflicht verbundenen erheblichen Verwaltungs- und Zeitaufwand zu vermeiden, ist es unbedingt erforderlich, dass von der durch § 50c Abs 2 eröffneten Möglichkeit der Schaffung von Standardanwendungen für Videoüberwachung in ausreichendem Maße Gebrauch gemacht wird. Eine entsprechende Änderung der Standard- und Muster-Verordnung 2004 müsste daher jedenfalls zeitgleich mit gesetzlichen Regelungen betreffend die Videoüberwachung in Kraft treten.

Zu § 50a Abs 1:

Die Definition der Videoüberwachung ist sehr weit und weicht insbesondere auch von jener Definition ab, die die Datenschutzkommission den Ausführungen zur Videoüberwachung im Anhang des Datenschutzberichtes 2007 (Seite 64) sowie ihrer bisherigen Judikatur zu Grunde gelegt hat.

Anders als die Datenschutzkommission (vgl. Datenschutzbericht 2007, Seite 65) geht der Entwurf auch davon aus, dass bloße Echtzeitwiedergabe eine Datenanwendung (die Erläuterungen zitieren in diesem Zusammenhang „§ 4 Z 7"; richtig müsste es wohl lauten „§ 4 Abs 1 Z 7") darstellt und unterwirft diese daher dem neuen 9a Abschnitt. (Siehe dazu auch die Bemerkung zu § 50a Abs 4 Z 3.)

Zu § 50a Abs 2:

Im Vergleich zum Begutachtungsentwurf 2008 ist dieser Absatz, vor allem auch durch die Wortfolge „jeweils einschließlich der Beweissicherung" (statt ursprünglich „oder zur Beweissicherung"), enger gefasst.

Zu § 50a Abs 4:

Zu Z 1 fällt insbesondere auf, dass die demonstrative Aufzählung datenschutzrechtlich zulässiger Eingriffe, die im Entwurf 2008 im Gesetztestext selbst enthalten war, nunmehr (geringfügig modifiziert) in die Erläuterungen aufgenommen wurde.

Diese Erläuterungen sind widersprüchlich und müssten insgesamt angepasst werden: Im Gesetzestext selbst wurde hinsichtlich des Begriffs „gefährlicher Angriff" der Verweis auf § 16 Abs 1 Z 1 des Sicherheitspolizeigesetzes gestrichen und ergibt sich aus dem letzten Teil der

Erläuterungen dazu, dass der Begriff des „gefährlicher Angriffs“ über den im Sicherheitspolizeigesetz definierten Begriff des „gefährlichen Angriffs“ hinaus geht. So sollen unter Z 1 „auch konkrete Gefährdungen von Geschäfts- und Betriebsgeheimnissen sowie allenfalls auch die konkrete Gefahr einer groben Verwaltungsübertretung fallen“. Diesen - zu begrüßenden - Ausführungen widersprechen die Erläuterungen in ihren Eingangssätzen zu Z 1.

Weiters wird in den Erläuterungen zu Z 1 ausgeführt, dass unter Videoüberwachungen nach Abs 4 Z 1 auch präventive Videoüberwachungen fallen können. Diese äußerst wichtige Aussage scheint allerdings insbesondere durch die lit a der in der Folge vorgenommenen beispielsweisen Aufzählung zulässiger Eingriffe wieder relativiert zu werden. Auch im Sinne der Stellungnahme 4/2004 der Art 29 - Datenschutzgruppe der EU vom 11.2.2004 zum Thema „Verarbeitung personenbezogener Daten aus der Videoüberwachung“, wo Videoüberwachung zur Verhütung von Straftaten, etwa zur Verhinderung von Überfällen, angesprochen wird, müsste die Zulässigkeit von Videoüberwachung zu Präventionszwecken unmissverständlich klargestellt sein.

Abgesehen von diesen grundsätzlichen Erwägungen ist hinsichtlich der lit a anzuführen, dass eine zeitliche Einschränkung auf gefährliche Angriffe innerhalb der vergangenen 10 Jahre nicht nachvollziehbar ist; weiters haben Verjährungsvorschriften allein mit dem Strafbedürfnis und dem Präventionszweck im Hinblick auf den jeweiligen Täter, keinesfalls aber mit der Wahrscheinlichkeit eines erneuten gefährlichen Angriffs (etwa durch andere Täter) zu tun, sodass durch den Verweis auf die Verjährungsvorschriften ein unsachlicher Bezug hergestellt wird.

In den Erläuternden Bemerkungen sollte daher in lit a jedenfalls die Passage ab „und sich dieser gefährliche Angriff .... “ entfallen.

Weiters sollte in der lit a auf „vergleichbare“ überwachte Objekte oder überwachte Personen Bezug genommen werden.

In lit d müsste jedenfalls klargestellt sein, dass die Gesamtheit der Gegenstände, die sich im überwachten Objekt befinden, gemeint ist.

Abgesehen von den vorstehenden Bemerkungen wäre in den Erläuterungen klarzustellen, dass sämtliche Beispiele alternativ zu verstehen sind; dh es müsste nach lit a das Wort „oder“ eingefügt werden.

Hinsichtlich Z 2 wird seitens der Bundessparte Gewerbe und Handwerk gefordert, auch „vertragliche Verpflichtungen“ aufzunehmen.

Nach Z 3 ist ein Betroffener durch eine Videoüberwachung dann nicht in seinen schutzwürdigen Geheimhaltungsinteressen verletzt, wenn „sich die Überwachung in einer bloßen Echtzeitwiedergabe von das überwachte Objekt die überwachte Person betreffenden Ereignissen erschöpft.... und sie zum Zweck des Schutzes von Leib, Leben oder Eigentum des Auftraggebers erfolgt“. Diese Bestimmung müsste jedenfalls in der Weise ergänzt werden, dass auch die Überwachung zum Zweck des Schutzes von Leib, Leben oder Eigentum Dritter die Geheimhaltungsinteressen Betroffener nicht verletzt.

Weiters sollte - wie im Begutachtungsentwurf 2008 - ein Betroffener dann nicht in seinen schutzwürdigen Geheimhaltungsinteressen verletzt sein, wenn „ die Videoüberwachung zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche des Auftraggebers vor

einem Gericht im Sinn von Art 234 EGV erforderlich ist". § 50a Abs 4 sollte um eine entsprechende Z 4 ergänzt werden.

Zu Abs 5:

Nach dieser Bestimmung ist ua die Videoüberwachung zum Zeck der Mitarbeiterkontrolle an Arbeitsstätten untersagt. Ein solches pauschales Verbot wird aus mehreren Gründen abgelehnt:

Aufgrund der existierenden arbeitsrechtlichen Regelungen und der dazu ergangenen Judikatur ist eine generelle Videoüberwachung eines Arbeitsplatzes bereits derzeit nur unter äußerst engen Voraussetzungen zulässig. Soweit es sich um die Menschenwürde verletzende Maßnahmen handelt, sind diese sittenwidrig und damit in jedem Fall unzulässig. Soweit die Menschenwürde durch die Maßnahme „berührt" ist, bedarf es der nicht ersetzbaren Zustimmung des Betriebsrates. Ist kein Betriebsrat eingerichtet, so ist die Zustimmung des einzelnen Arbeitnehmers erforderlich (vgl § 96 Abs 1 Z 3 ArbVG und § 10 AVRAG). Ein Auszug aus der Judikatur: Durch ein Videosystem mit vier Kameras, mit dem die Arbeitsbereiche von Arbeitnehmern erfasst werden, ist die Menschenwürde der Arbeitnehmer berührt (OLG Wien 7. 6. 1995, 8 Ra 68/95, SWK 1996, B 18). Überwacht hingegen eine Fernsehkamera einen Verladevorgang nur zum Teil, so stellt dies keine die Menschenwürde berührende Kontrolle dar (EA Wien II Re 61/68; weitere Nachweise siehe *Reissner* in ZellKomm § 96 ArbVG Rz 26).

Die Frage der Auswirkungen auf die Menschenwürde, ist also im Einzelfall im Rahmen einer Güterabwägung zu treffen und daher keiner Pauschalbeurteilung durch Ge- oder Verbot zugänglich. Im Übrigen sei auch auf § 96a ArbVG hingewiesen.

Unklar ist weiters das Verhältnis dieses generellen Verbotes zur Regelung in den Abs 3 (etwa Zulässigkeit der Überwachung im lebenswichtigen Interesse einer Person) und Abs 4 (etwa Ziel oder Ort eines gefährlichen Angriffs). Es kann jedenfalls Fälle geben, bei denen eine Überwachung zum Schutz der Mitarbeiter erforderlich ist (etwa bei gefährlichen Maschinen oder in Banken auch im Schalterbereich). Auch aus Datensicherheitsgründen kann es erforderlich sein, dass besondere Sicherheitsbereiche (zB Serverräume) videoüberwacht werden und davon auch Mitarbeiter betroffen sind.

Darüber hinaus weist der allgemeine Fachverband des Gewerbes eindringlich darauf hin, dass „eine Untersagung der Video-Mitarbeiterüberwachung aus versicherungsrechtlichen Gründen zum sofortigen Erliegen der Geldbearbeitung und -manipulation in den privaten (gewerblichen) Cash-Centern aber möglicherweise auch in den Geldbearbeitungszentren der Nationalbank führen würde und damit die Bargeldversorgung in Österreich akut gefährdet wäre.

Es ist daher auch nicht richtig, dass - wie in den Erläuterungen zu dieser Bestimmungen behauptet wird - bei Videoüberwachungen zur Mitarbeiterkontrolle an Arbeitsstätten davon auszugehen ist, dass auf Grund der Eingriffstiefe stets ein gelinderes Mittel zur Kontrolle von Mitarbeiterinnen und Mitarbeiter gefunden werden kann, da diese im Bereich der Geldbearbeitung und -manipulation vielmehr die unabdingbare Voraussetzung für den Abschluss von diesbezüglichen internationalen Versicherungsverträgen darstellt".

Daher hält der Allgemeine Fachverband des Gewerbes fest, „dass die im vorliegenden Gesetzesentwurf vorgesehene, ausnahmslose Untersagung der Videoüberwachung zum Zwecke der Mitarbeiterkontrolle an Arbeitsstätten und der damit zeitgleich einhergehende Verlust der Versicherungsdeckung (und damit auch der Bearbeitungsverträge) für die in diesem Bereich

tätigen Unternehmen des Bewachungsgewerbes unmittelbar existenzbedrohend wäre und diese Bestimmung daher ohne Schaffung von expliziten Ausnahmen keinesfalls akzeptiert werden kann".

Zu Abs 7:

Ein absolutes Verbot eines automationsunterstützten Bilddatenabgleichs ist abzulehnen, weil durch diese Bestimmung zB Zutrittskontrollsysteme (ZKS) mit Gesichtserkennung zukünftig nicht mehr installiert und verwendet werden dürften. Diese Art von ZKS ist in hochsicherheitskritischen Bereichen (zB Flughäfen) heute aber state of the art. Wir regen daher an, dieses absolute Verbot durch eine Genehmigungspflicht zu ersetzen.
Das Verbot sollte weiters nicht für Fälle des Abs 6 gelten.

Die Bundessparte Gewerbe und Handwerk und die Wirtschaftskammer Wien schlagen folgende alternative Lösung für die Zulässigkeit von Videoüberwachung vor (wonach nicht bereits die Bildaufzeichnung durch Maschinen, sondern erst die Sichtung und Auswertung durch Menschen datenschutzrelevant ist):

„Die Technik ist derart weit fortgeschritten, dass eine absolut sichere Verschlüsselung von Bilddaten möglich ist. Die technische Möglichkeit zur Entschlüsselung (der Schlüssel) kann beim Datenverarbeitungsregister zusammen mit einer vereinfachten Meldung der Videoaufzeichnung (ohne inhaltliche Prüfung oder Vorabkontrolle durch die Datenschutzkommission) hinterlegt werden.

Erst wenn ein Anlassfall eine Datenauswertung erfordert, prüft die Behörde auf Antrag, ob der Anlassfall die Datenauswertung rechtfertigt. Nur wenn die Behörde die Datenauswertung im Anlassfall als berechtigt ansieht, folgt sie den Schlüssel zur Datenauswertung aus.

Die Normunterworfenen sollten die Wahl haben, ob sie sich dieses Verfahrens bedienen (vereinfachte Meldung der Bildaufzeichnung bei strenger Kontrolle jeder Auswertung) oder die Videoaufzeichnung - wie bisher - melden und die Vorabkontrolle durch die Datenschutzkommission abwarten."

Zu § 50b:

Die Löschungsverpflichtung nach spätestens 48 Stunden ist für die Praxis viel zu kurz. Videoaufzeichnungen von Freitag Abend müssten Sonntag Abend wieder gelöscht werden. Angesichts der Tatsache, dass nicht alle Unternehmen am Wochenende tätig sind, ist diese Frist völlig praxisfremd. Es wird eine grundsätzlich zulässige Speicherdauer von zumindest ca. 1 Woche angeregt und in diesem Zusammenhang insbes. auch darauf hingewiesen, dass die DSK bereits in etlichen - va jüngeren - Registrierungsverfahren längere Speicherfristen als im Entwurf vorgesehen als zulässig angesehen hat.

Zu § 50c:

An dieser Stelle wird nochmals auf das Anliegen der Schaffung von ausreichenden Standardanwendungen für Videoüberwachung hingewiesen.

Zu § 50d:

Die im Begutachtungsentwurf aus dem Jahr 2008 enthaltene Ausnahme von der Kennzeichnungspflicht „wenn sie angesichts der Unwahrscheinlichkeit einer Beeinträchtigung der Betroffenenrechte oder der Beschaffenheit des überwachten Objekts, insbesondere dessen Mobilität einerseits und der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordern würde“ sollte wieder aufgenommen werden.

Weiters sollte eine Ausnahme aufgenommen werden, wonach die Kennzeichnung der Videoüberwachung auch dann entfallen kann, wenn zu befürchten ist, dass die Kennzeichnung nur zur Verlagerung eines gefährlichen Angriffes in einen durch das Überwachungsgerät nicht erfassbaren Bereich führen würde.

Die Kennzeichnungspflicht sollte jedenfalls auf ein zumutbares Ausmaß reduziert werden und den Auftraggeber nicht in die Situation versetzen, bauliche Extramaßnahmen treffen zu müssen, um dieser Pflicht nach § 50 d nachkommen zu können.

Zu § 50e:

Diese Bestimmung normiert ein generelles Auskunftsrecht aus Videoüberwachung. Ein solches generelles Auskunftsrecht wird abgelehnt.

In diesem Zusammenhang wird insbesondere auf die jüngste Judikatur der Datenschutzkommission hingewiesen, wonach ein Auskunftsrecht aus nicht ausgewerteten Videoaufzeichnungen nicht besteht (vgl zB DSK, K121.425/003-DSK/2009; DSK, K121.402/0010-DSK/2008). Die Datenschutzkommission argumentiert im Wesentlichen damit, dass das Bestehen eines Auskunftsrechts aus nicht ausgewerteten Videoaufzeichnung in gleicher Weise zu beurteilen ist wie bei indirekt personenbezogenen Daten, für die ebenfalls kein Auskunftsanspruch besteht (vgl. § 29). Sie führt weiters aus, dass die Annahme des Bestehens eines Auskunftsrechts aus nicht ausgewerteten Videoaufzeichnungen durch die allein dadurch notwendig gewordene Auswertung jedenfalls die Datenschutzrechte der übrigen Personen, die von der Aufzeichnung betroffen sind, unverhältnismäßig beeinträchtigen würde. Diesem Einwand kann auch § 50e Abs 2 des Entwurfes nicht Rechnung tragen.

Weiters könnten im Falle von Auskunftsersuchen die - den Geheimhaltungsinteressen der Betroffenen einschließlich des Auskunftswerbers dienenden - Löschfristen nicht eingehalten werden (vgl § 26 Abs 7).

Abgesehen von der Ablehnung eines generellen Auskunftsrechts sind folgende Punkte anzumerken:

Es ist völlig fraglich, wie diesem besonderen Auskunftsrecht nachgekommen werden kann, ohne dass damit in die Rechte Dritter, aber auch die Interessen des Auftraggebers, wie insbesondere dessen Betriebs- und Geschäftsgeheimnisse, eingegriffen wird bzw diese verletzt werden. Im Falle der Beibehaltung der vorgeschlagenen Bestimmung wäre daher zumindest klar zu stellen, dass im Falle einer möglichen Beeinträchtigung der Interessen des Auftraggebers oder der Rechte Dritter durch die Offenlegung der Aufzeichnung mit einer schriftlichen oder mündlichen Beschreibung des überwachten Verhaltens des Auskunftswerbers das Auslangen gefunden werden kann. Von einer Zustimmung des Auskunftswerbers sollte die mündliche Auskunftserteilung allerdings nicht abhängen.

Eine Auskunft über technisches Format ist zB für Kreditinstitute aus zwei Gründen nicht möglich: Einerseits sind auf den Videos normalerweise weitere Personen ersichtlich, denen ein Recht auf Geheimhaltung zukommt. Darüber hinaus ergeben sich Sicherheitsprobleme, da auf dem Video i.d.R. das Innere einer Filiale ersichtlich ist.

Weiters wäre sicherzustellen, dass das Auskunftsbegehren möglichst präzise erfolgen muss; so etwa wäre zu definieren, für welchen x-Minuten nicht überschreitenden Zeitraum das Auskunftsrecht geltend gemacht werden kann. Hinzuweisen ist aber darauf, dass selbst bei Benennung des Anfangs- und Endpunktes und Einschränkung des Zeitraums durch den Betroffenen es einiger Zeit bedarf, um die entsprechende Stelle zu finden; dieses im Entwurf vorgesehene Auskunftsrecht führt zu einem beträchtlichen Arbeitsaufwand und damit erheblichen (Personal-)Mehrkosten.

Es müsste daher, auch um Missbräuche oder gar schikanöse Auskunftsersuchen zu vermeiden, vorgesehen werden, dass die Auskunftserteilung erst nach vorheriger Leistung eines Kostenersatzes in angemessener Höhe erfolgen muss.

In Abs 3 sollte ergänzt werden, dass ein Auskunftsrecht auch in den Fällen des § 50a Abs 3 Z 2 (auf öffentliche Wahrnehmung gerichtetes Verhalten) und in den Fällen des § 50a Abs 6 (Verdacht auf gerichtlich strafbare Handlung oder Abwehr oder Beendigung eines gefährlichen Angriffs) ausgeschlossen ist, wobei für die Fälle des § 50a Abs 6 auf die Bestimmungen der StPO über die Akteneinsicht verwiesen werden kann.

**Zu Z 84 (Entfall von § 51 Abs 2):**

Abs 2, wonach bei einer Datenverwendung in Gewinn- oder Schädigungsabsicht der Täter nur mit Ermächtigung des Verletzten zu verfolgen ist, soll nach dem Entwurf entfallen, das Ermächtigungsdelikt somit zum Offizialdelikt werden.
In den Erläuterungen findet sich keine Begründung für diese Änderung; uE sollte Abs 2 bestehen bleiben.
Die im Entwurf neu aufgenommene Passage „oder mit der Absicht, einen anderen dadurch in seinem von § 1 Abs 1 gewährleisteten Anspruch zu schädigen“ ist insbes. im Kontext der gesamten Strafbestimmung unklar, zudem auch überschießend, und sollte daher entfallen.

**Zu Z 85 - 89 (§ 52):**

Es fehlen nachvollziehbare Erläuterungen, weshalb die Höchststrafen derart stark angehoben werden sollen. Insbesondere die Änderungen in § 52 Abs 1 entsprechen einer Erhöhung von mehr als 30%; derartige Erhöhungen sind durch Valorisierung nicht zu rechtfertigen.

Die Möglichkeit des Verfalls von Bildübertragungs- und Bildaufzeichnungsgeräten scheint überschießend.

**Zu Z 94 (§ 61 Abs 6):**

Die Übergangsbestimmung des § 61 Abs 6 wird begrüßt und im Sinne des Vertrauens der Auftraggeber in die Rechtmäßigkeit bereits erfolgter Registrierungen von Videoüberwachungen (nach zum Teil langwierigen und schwierigen Registrierungsverfahren) als unverzichtbar erachtet.

**Abschließend** darf noch darauf hingewiesen werden, dass in der „Textgegenüberstellung" Abweichungen vom Entwurfstext enthalten sind, so insbes. eine (offenbar noch irrtümlich aus dem Entwurf 2008 stammende) Änderung des § 4 Abs 1 Z 3 und das Fehlen der Z 83 bis 89 des vorliegenden Entwurfs.

Im Übrigen wird zu gleichlautenden Bestimmungen auch auf die Stellungnahme der WKÖ vom 19.5.2008 zum Entwurf einer „DSG-Novelle 2008" hingewiesen.

Die Stellungnahme wird auch dem Präsidium des Nationalrates im Wege elektronischer Post an die Adresse begutachtungsverfahren@parlament.gv.at übermittelt

Mit freundlichen Grüßen

Dr. Christoph Leitl
Präsident

Mag. Anna Maria Hochhauser
Generalsekretärin