WIRTSCHAFTSKAMMER ÖSTERREICH

Abteilung für Rechtspolitik
Wiedner Hauptstraße 63 | Postfach 195
1040 Wien
T +43 (0)5 90 900DW | F +43 (0)5 90 900233
E rp@wko.at
W www.wko.at/rp

An das
Bundeskanzleramt/Verfassungsdienst
Per Mail: v@bka.gv.at

cc: begutachtungsverfahren@parlament.gv.at

Ihr Zeichen, Ihre Nachricht vom	Unser Zeichen, Sachbearbeiter	Durchwahl	Datum
BKA 810.026/0002-V/3/2008 4.3.2008	Rp 1761/08/DrRo/SM	3215	19.05.2008

Entwurf eines Bundesgesetzes, mit dem das Bundesgesetz über den Schutz personenbezogener Daten geändert wird (DSG-Novelle 2008); Stellungnahme

Sehr geehrte Damen und Herren!

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

1. Allgemeines:

Der vorliegende Entwurf einer Novelle zum Datenschutzgesetz 2000 enthält eine Reihe von Neuerungen, die massiv zu Lasten der Wirtschaft gehen: Hervorgehoben seien vor allem die Abschaffung des Datenschutzes für juristische Personen und die verpflichtende Einführung eines betrieblichen Datenschutzbeauftragten für Betriebe mit mehr als 20 Mitarbeitern. Auch die Erweiterung der (Prüf)befugnisse der Datenschutzkommission, viele - manchmal nur durch sprachliche Veränderungen hervorgerufene - neu aufgeworfene Interpretationsprobleme und nicht zuletzt der Regelungsvorschlag zur Videoüberwachung ergeben aus Sicht der Wirtschaftskammer Österreich erheblichen Diskussionsbedarf zum vorliegenden Entwurf.

Eine komplexe Materie wie der Datenschutz, der naturgemäß auch in einem gewissen Spannungsfeld beheimatet ist, sollte nicht überstürzt, sondern in Ruhe und ohne unnötigen Druck diskutiert werden. Aus diesem Grund wird dringend appelliert, die Novelle zum Datenschutzgesetz nicht wie im Arbeitsprogramm der Bundesregierung für das Jahr 2008 vorgesehen, bis Juni dJ unter Zeitdruck abzuhandeln, sondern gemeinsam mit der Wirtschaft, die besonders betroffen ist, eine Diskussion zu führen und eine Lösung zu finden.

2. Zu den Bestimmungen im Einzelnen:

Zu Z 10 (§ 1):
Der Entwurf sieht eine sprachliche Neugestaltung des Grundrechts auf Datenschutz und seine Beschränkung auf natürliche Personen vor.

Die Erläuterungen begründen die Abschaffung des Datenschutzes für juristische Personen damit, dass die meisten europäischen Datenschutzgesetze, ebenso wie die Datenschutzrichtlinie 95/46/EG, nur den Datenschutz natürlicher Personen regeln und der auch auf juristische Personen bezogene Anwendungsbereich des DSG 2000 „immer wieder - auch im europäischen Kontext - vielfach auf Unverständnis" stieß.
Aus Sicht der Wirtschaftskammer Österreich ist jedoch für die **Abschaffung des Datenschutzes juristischer Personen** keinerlei Grund ersichtlich, sondern stellt dies vielmehr einen Rückschritt dar und ist daher **aufs Schärfste abzulehnen.** Die Einbeziehung juristischer Personen in das Grundrecht auf Datenschutz erfolgte bereits durch das „erste" Datenschutzgesetz, nämlich das DSG 1978, und wurde auch bei der Umsetzung der Datenschutzrichtlinie 95/46/EG durch das DSG 2000 beibehalten. Selbst wenn die genannte Richtlinie dies nicht erfordert, spricht sie auch nicht gegen einen Datenschutz für juristische Personen. Auch ist Österreich nicht das einzige EU-Land, das einen Datenschutz für juristische Personen normiert.

Durch die Abschaffung des Datenschutzes für juristische Personen würde nicht nur mit einer seit 1978 bestehenden Tradition gebrochen, sondern es würde auch vom konsensualen Ergebnis des Ausschusses IV des Österreich-Konvents abgewichen, das eine derartige Einschränkung nicht vorgesehen hat (siehe dazu den Bericht des Ausschusses IV vom 3.6.2004, Seite 36).

Hinzuweisen sei auch darauf, dass nach dem Wortlaut des Art. 8 Abs. 1 der Charta der Grundrechte der Europäischen Union „jeder Person" das Grundrecht auf Datenschutz zusteht; dem Wortlaut nach daher auch juristischen Personen. Dazu kommt, dass im Kontext sonstiger europäischer „Datenschutzrichtlinien", nämlich konkret in der DatenschutzRL für elektronische Kommunikation 2002/58/EG, auch die berechtigten Interessen juristischer Personen geschützt werden.

Dass juristische Personen nicht mehr vom Recht auf Datenschutz umfasst sein sollen, steht zudem nicht in Einklang mit Art. 8 der Europäischen Menschenrechtskonvention (EMRK). Der Europäische Gerichtshof für Menschenrechte (EGMR) hat seine Rechtsprechung dahingehend entwickelt, dass auch juristische Personen den Schutz des Art. 8 EMRK genießen (vgl. z.B. Grabenwarter, Europäische Menschenrechtskonvention^3, 192 mwH). Weshalb der Schutz personenbezogener Daten juristischer Personen in § 1 DSG 2000 als auch zu Art 8 EMRK innerstaatlich korrespondierendes Grundrecht abgeschafft werden soll, ist daher auch aus diesem Grund nicht nachvollziehbar.

Die erhebliche praktische Bedeutung des Grundrechts auf Datenschutz juristischer Personen, zeigt etwa das VfGH-Erkenntnis VfSlg 16.369/2001, wo der VfGH der nicht anlassfallbezogenen Datensammlung der Telekom-Regulierungsbehörde im Hinblick auf § 1 DSG 2000 Einhalt geboten hat. Die gleiche Problematik betrifft u.a. auch die Mitglieder des Fachverbandes Gas Wärme, soweit diese Erdgasunternehmen sind und daher der Aufsicht durch die Energie-Regulierungsbehörden unterliegen.

Wörtlich führt der VfGH in der zitierten Entscheidung u.a. aus:
„Wie der VfGH bereits zum Gewährleistungsumfang der jedenfalls insoweit mit § 1 DSG 2000 übereinstimmenden Fassungen des Grundrechts auf Datenschutz in der Fassung des DSG, BGBl 565/1978, (also vor dem DSG 2000) aussprach (vlg VfSlg 12.228/1989, 12.880/1991), können auch Wirtschaftsdaten personenbezogene Daten im Sinne des § 1 DSG und somit Schutzobjekt des Grundrechts sein. Der VfGH bleibt auch bei der in den zitierten Erkenntnissen bereits vertretenen Auffassung, daß der Anspruch auf Geheimhaltung schutzwürdiger personenbezogener Daten nicht bloß auf die Nicht-Weitergabe erhobener Daten gerichtet ist, sondern es auch verbietet, daß der Betroffene zur Offenlegung verpflichtet wird. Diese Überlegungen zusammenfassend verbürgt somit das Grundrecht auf Datenschutz einen verfassungsrechtlichen Schutz vor Ermittlung personenbezogener Daten, bei denen es sich auch um Wirtschaftsdaten handeln kann“ (VfSlg 16369/2001). Angesprochen ist daher u.a. auch der Schutz juristischer Personen vor ungerechtfertigten Offenlegungsverpflichtungen.

Darüber hinaus schützt das Grundrecht auf Datenschutz gerade auch juristische Personen vor überzogenen Anforderungen betreffend die Datenübermittlung für Zwecke der Statistik (vgl. etwa VfSlg 12.228/1989).

Sachlich nicht nachvollziehbar ist auch, dass der Datenschutz durch die vorgeschlagene Bestimmung nunmehr insofern aufgesplittert werden soll, als er auf der einen Seite bei natürlichen Personen (und damit auch Einzelunternehmern) zur Anwendung gelangen soll und andererseits bei juristischen Personen und nach der Textierung des Entwurfes offenbar auch für Personengesellschaften (OG, KG) nicht mehr gelten soll. Die in den Erläuterungen angeführte Begründung kann sachlich nicht nachvollzogen werden und kann unseres Erachtens daher nicht zu einer Rechtfertigung für die Einschränkung dieses verfassungsgesetzlich gewährleisteten Rechtes führen.

Die Aussage in den Erläuterungen zur DSG-Novelle, die Geheimhaltungsinteressen juristischer Personen seien durch die bestehenden gesetzlichen Regelungen z.B. im gewerblichen Rechtsschutz oder Urheberrecht ohnedies ausreichend geschützt, ist nicht zutreffend:

Es ist nachdrücklich darauf hinzuweisen, dass die angeführten Rechtsmaterien des gewerblichen Rechtsschutzes oder des Urheberrechts den Datenschutz gemäß DSG nicht in adäquater Weise kompensieren können. Zu den Rechten des gewerblichen Rechtsschutzes werden traditioneller Weise das Patentrecht, das Musterrecht, das Markenrecht sowie die Abwehrrechte des UWG, im konkreten Konnex insbesondere das Recht auf Geschäfts- und Betriebsgeheimnis (§§ 11, 12 UWG), verstanden. Der Datenschutz verfolgt gemäß § 1 Abs. 1 DSG idgF den Schutz eines Geheimhaltungsinteresses.

Da bei den gewerblichen Schutzrechten des Patent-, Muster- und Markenrechtes der Schutz erst durch Eintragung in ein öffentliches Register (!) entsteht, scheiden diese Rechtsmaterien wohl von vornherein als geeignete Instrumente zum Schutz des Geheimhaltungsinteresses aus. Diese Rechtsmaterien verfolgen keinerlei Geheimhaltungsschutzinteressen, sondern bezwecken den Schutz von Investitionen in Forschung und Entwicklung, sowie einzelner äußerlicher Individualisierungsmerkmale von Waren und Dienstleistungen vor Verwechslungen und Zuordnungsproblemen.

Die Bestimmungen des Lauterkeitsrechtes verfolgen ebenso wenig wie die bereits oben ausgeführten Materien Datenschutzinteressen. Das Gesetz gegen Unlauteren Wettbewerb (UWG) soll fairen Wettbewerb sichern und beinhaltet daher ausschließlich wettbewerbsbezogene

Handlungsge- und -verbote. Das UWG setzt in vielen Bestimmungen auch ein Wettbewerbsverhältnis voraus, was aber in vielen Situationen nicht gegeben ist, so z.B. im Verhältnis zum Staat (Ausnahme: privatwirtschaftliche Tätigkeiten des Staates). Lediglich die Bestimmungen der §§ 11 und 12 UWG beinhalten einen (eingeschränkten) Schutz von Geschäfts- oder Betriebsgeheimnissen. Nach den genannten Bestimmungen liegt nur dann ein Verstoß gegen die Betriebsgeheimhaltungspflicht vor, wenn dabei ein Bediensteter des Unternehmens involviert ist. Insbesondere muss auch hier ein Handeln zu Zwecken des Wettbewerbes vorliegen. Die genannten Bestimmungen können also auch keinen mit dem DSG vergleichbaren umfassenden Schutz gewährleisten.

Der Schutz des Urheberrechts hängt davon ab, ob 1. eine eigentümliche geistige Schöpfung vorliegt und 2. diese Schöpfung in eine der vom Urheberrechtsgesetz erfassten Werkkategorien subsumiert werden kann. Gerade die Voraussetzung der eigentümlichen geistigen Schöpfung ist höchst ermessensabhängig vom Entscheidungsorgan und ist in vielerlei Hinsicht nicht zu erwarten, dass Zahlen, Daten oder Fakten eines Unternehmens, für die ein Schutz begehrt wird, als eigentümlich gewertet werden können[1]. Aus den unbestimmten Begriffen der eigentümlichen geistigen Schöpfung resultiert weiters, dass im Vorhinein kaum Aussagen getroffen werden können, ob ein bestimmtes Datum diese Eigenschaften erfüllt oder nicht. Klärung über die Frage eines allfälligen Schutzes kann also erst eine gerichtliche Entscheidung fällen, wodurch aber das wesentliche Anliegen, nämlich, dass bereits im Vorfeld ein Schutz klargestellt ist, nicht erreicht wird.

Durch die Abschaffung des Datenschutzes für juristische Personen kämen diesen auch keine Betroffenenrechte (Recht auf Auskunft, Richtigstellung, Löschung, Widerspruch) mehr zu. Auch dies wäre höchst problematisch und ist strikt abzulehnen. Der in den Erläuterungen angegebene Entlastungseffekt steht in keinerlei Verhältnis zur Abschaffung eines Grundrechts!

Zusammenfassend wird daher nochmals betont, dass die Einschränkung des Grundrechts auf Datenschutz und der Bestimmungen des DSG 2000 auf personenbezogene Daten natürlicher Personen abgelehnt wird.

In den Erläuterungen wird angeführt, dass der Passus in der derzeit geltenden Bestimmung des § 1 Abs. 1, nämlich *„oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind“* insofern entfallen kann, als es als selbstverständlich erscheint, dass Daten nur dann personenbezogen sein können, wenn eine Rückführbarkeit dieser Daten gegeben ist. Die Ausnahme vom Grundrechtsschutz für die Verwendung von nur indirekt personenbezogenen Daten sollte jedenfalls zur Klarstellung und als Grundlage für die einfachgesetzlichen Sonderregelungen für indirekt personenbezogene Daten aufrecht bleiben.

Zu Z 11 (§ 2):
Die ausschließliche Zuordnung von Angelegenheiten des Schutzes personenbezogener Daten in die Gesetzgebungs- und Vollziehungskompetenz des Bundes wird begrüßt.

---

[1] Als eigentümlich wertet der OGH Schöpfungen, die sich vom landläufigen, alltäglichen oder üblicher Weise hervorgebrachten unterscheiden und die persönlichen Züge des Werkschaffenden durch die Gestaltung und durch die gedankliche Bearbeitung des Werkes zur Geltung kommen (Vgl. *Dittrich*, UrhR[5] 2007 § 1 E 34f). Der OGH hat z.B. einem einzigen Wort kein Urheberrecht zugestanden (OGH 22.4.1997, 4 Ob 96/97i - „Ramtha“).

Zu Z 14 bis Z 24 (§ 4):
Die Veränderungen in den Begriffsbestimmungen, die in den Erläuterungen zum Teil nur als „Vereinfachungen" oder „Klarstellungen" bezeichnet werden, scheinen nicht zielführend. Zum einen werfen sie mehr neue Fragestellungen auf, als sie „klarstellen" können, zum anderen ist die Entflechtung der Begriffsbestimmungen vom Vorliegen einer „Datenanwendung" nicht sinnvoll. Auch bei der geänderten Kompetenzrechtslage könnte die Regelungstechnik des § 58 geltende Fassung aufrecht erhalten bleiben; diesfalls wäre die komplizierte Regelung des vorgeschlagenen § 4 Abs. 2 entbehrlich und auch sonstige damit im Zusammenhang stehende Auslegungsprobleme könnten vermieden werden.

Seitens des Fachverbandes der Finanzdienstleister wird zu den Z 16 und 17 (§ 4 Abs. 1 Z 4 und 5) folgendes ausgeführt:

„Vorausschickend darf auf die Begrifflichkeiten hingewiesen werden: Jeder, der Daten verwendet, ist entweder „Auftraggeber" oder „Dienstleister". Für einen Auftragnehmer (Dienstleister), der im Auftrag des „Eigentümers" der Daten („Auftraggebers") tätig wird, kann es nachteilig sein, selbst als Auftraggeber betrachtet zu werden. Insbesondere knüpfen sich folgende Pflichten an die Stellung als Auftraggeber:

- *Meldepflichten gem. § 17 ff DSG*
- *Informationspflicht gem. § 24 DSG*
- *Auskunftsrecht gem. § 26 DSG*
- *Richtigstellungs- und Löschungsrecht gem. § 27 f DSG*

*Die neuen Formulierungen der Z 16 und 17 des Entwurfes bringen eine Änderung dahingehend, dass in § 4 Abs. 1 Z 4 E die Wendung entfällt, dass ein Datenverwender („Dienstleister"), der Daten über den Auftrag hinaus verwendet, als Auftraggeber betrachtet wird. Weiters entfällt der Begriff „Auftragnehmer"; dieser wird jetzt als „Dienstleister" bezeichnet. Die Bestimmung des § 4 Abs. 1 Z 5 DSG wird nach dem Text des Entwurfes scheinbar geringfügig geändert: im Entwurf wird im letzten Teilsatz der Begriff **„nur"** eingefügt („..., **wenn sie Daten nur zur Herstellung eines ihnen aufgetragenen Werkes verwenden**" anstelle von „...Daten, die ihnen zur Herstellung eines aufgetragenen Werkes überlassen wurden, verwenden").*

In den EB zu Z 17 (§ 4 Abs. 1 Z 5 E) werden einige Fälle erwähnt, die nicht als Dienstleister anzusehen sind:

- *Ein Empfänger von Daten, der für die Weitergabe an ihn ein Entgelt leistet;*
- *Ein Auftragnehmer, der Daten die er im Zuge der Erteilung verschiedener Aufträge erhalten hat, verknüpft; oder*
- *Der Empfänger von Daten, der über die Verwendung von Daten entgegen einer Anordnung dessen entscheiden kann, welcher ihm die Daten weitergegeben hat.*

Daraus kann der Schluss gezogen werden, dass mit dieser Novelle alle „Nicht-Dienstleister" als Auftraggeber betrachtet werden sollen.

Es sind jene Unternehmen (z.B. Auskunfteien) besonders betroffen, die Datenbestände zum Monitoring übernommen haben, ohne dass die hinterlegten Daten in die Auskunftei-Dienstleistung einfließen (dürfen). In der Wirtschaft stark angefragte und notwendige Produkte wie Insolvenz-Monitoring wären durch diese Novelle nicht mehr möglich.

Zusätzlich betrifft diese Regelung Outsourcing-Dienstleister. Hier werden die Daten ausschließlich im Kundenauftrag verarbeitet. Diese Verarbeitung von kundeneigenen Kunden - oder Sperrlisten ist aber ohne „Verknüpfung" mit Auskunftei-Datenbanken unmöglich. Davon sind unzählige Unternehmen als Kunden der Auskunfteien betroffen, die derartige Outsourcing-Dienstleistungen nicht mehr verwenden können.

Das Verknüpfen von Daten ist oftmals sogar ein wesentlicher Teil angebotener Dienstleistungen verschiedenster Unternehmungen. Neben den Auskunfteien sind unter anderem auch Inkasso-Unternehmen oder Paketzusteller betroffen. Bei ersteren wird abgeglichen, ob es sich um Personen mit gleichen Namen handelt, um festzustellen, ob die richtige Person betroffen ist. Bei Paketzustellern ist wichtig zu erkennen, ob an einen Haushalt mehrere Sendungen (unterschiedlicher Versender) abzuliefern sind, um routeneffizient und wirtschaftlich Planen zu können.

Durch dieses Gesetz wird allerdings versucht, die Auftraggebereigenschaft an der Verknüpfung von Daten zu orientieren. Dies ist unseres Erachtens nicht mit § 14 Abs. 2 Z 7 DSG idgF in Einklang zu bringen, der alle Datenverarbeiter (unabhängig davon, ob es sich um einen Auftraggeber oder Dienstleister handelt) dazu verpflichtet, alle Verwendungsvorgänge von Daten zu einer Person zu protokollieren. Dadurch werden die Daten über die Erfüllung der konkreten Aufträge hinaus verknüpft, weil alle Verwendungsvorgänge aller Auftraggeber zu einer Person nachvollziehbar sein müssen. Aus dieser Interpretation kann geschlossen werden, dass es keine Dienstleister mehr geben kann, da eine Verknüpfung der Daten immer notwendig ist, um gesetzeskonform tätig sein zu können.

Da von unserer Seite allerdings angenommen wird, dass es nicht das Ziel dieser Novelle sein kann, in Zukunft keine Dienstleister mehr zu haben, ist die „Verknüpfung" von Daten kein geeigneter Anknüpfungspunkt für die Abgrenzung Auftraggeber - Dienstleister. Entscheidend sollte vielmehr die tatsächliche Verfügungsmacht über Informationsinhalte sein.

Die Überlassung von Daten ist typischer Weise an eine entsprechende zivilrechtliche Zusicherung des Auftragnehmers (Dienstleisters) gebunden, die Daten nicht abseits des Auftrages zu verwenden.

Wird dem Auftragnehmer die Verknüpfung verboten (oder nur um den Preis der Auftraggeber-Eigenschaft zumutbar), sind viele Aufträge nicht mehr erfüllbar. Zusätzlich würde die Regelung zukünftige (Produkt-)Innovationen behindern, wenn nicht sogar unmöglich machen, da eine Auskunftei keine anderen Produkte mehr anbieten kann.

Ein wesentliches Problem der erweiterten Auftraggeber-Eigenschaft liegt in den damit verbundenen Richtigstellungs- und Löschungsansprüchen. Zur Erläuterung kann folgendes Beispiel angeführt werden:

Ein Unternehmer A ist der Auftraggeber; das Unternehmen B ist nach bisheriger gesetzlicher Definition der Dienstleister. Der Dienstleister nimmt einen Datenabzug von anderen Unternehmen (ebenfalls Auftraggeber) vor. Der Dienstleister (Unternehmer B) selbst hat nicht die relevanten Daten, sondern die jeweils anderen Unternehmer.

Wenn in der Zukunft ein Betroffener eine Löschung oder Richtigstellung von Unternehmer B verlangt (wie es durch die Auftraggeber-Eigenschaft von Unternehmer B in Zukunft möglich sein soll), dann müsste Unternehmer B diese Daten löschen. Wird nun auf dem Datenabzug eine

„Richtigstellung" oder „Löschung" vorgenommen, wird diese bei der nächsten Synchronisation des Unternehmers A (der der eigentliche Auftraggeber und „Herr der Daten" ist) überschrieben, da eine beidseitige Synchronisation von Datenbanken in der Praxis nicht durchführbar ist. Somit ist eine nachhaltige Richtigstellung oder Löschung auch technisch nicht möglich.

Zusammenfassend ist es daher sinnvoller, Richtigstellungen und Löschungen beim Auftraggeber zu begehren, der diese Daten juristisch auch „besitzt". Die vorhandene gesetzliche Lage deckt daher die betroffenen Interessen vollständig ab und muss nicht zusätzlich erweitert werden."

Zu Z 29 (§ 8 Abs. 4):

Seitens der Bundessparte Information und Consulting wird zur Neueinfügung einer Z 4 in § 8 Abs. 4 folgendes ausgeführt:
„Sofern mit dieser Bestimmung auch das Daten-Ermitteln erfasst sein soll, ist hier eine Ergänzung angebracht, als die schutzwürdigen Geheimhaltungsinteressen bei Verwendung nicht-sensibler Daten nur insofern nicht verletzt sind, als die Datenweitergabe „über Anforderung der Behörde" erfolgt. Damit soll sichergestellt werden, dass die Daten nur von der zuständigen Behörde zweckgebunden lediglich zum Zweck einer Anzeigenerstattung sowie deren Bearbeitung verwendet werden. Dadurch kann verhindert werden, dass z.B. das Fernmeldegeheimnis gem. Art 10a Staatsgrundgesetz bzw. das Kommunikationsgeheimnis gem. § 93 TKG ausgehöhlt wird.

Ist diese Interpretation unzutreffend und setzt diese Bestimmung bereits das rechtmäßige Besitzen der Daten voraus (bevor die Daten an die zuständigen Behörden iSd der neuen Regelung weitergegeben werden dürfen), sollte dies in den EB deutlich zum Ausdruck gebracht werden, damit Fehlinterpretationen vermieden werden können."

Zu Z 34 (§ 15a), Z 40 (§ 19 Abs. 1 Z 8) und Z 50 (§ 30 Abs. 1a):

Die Einführung eines verpflichtenden betrieblichen Datenschutzbeauftragten wird seitens der Wirtschaftskammer Österreich strikt abgelehnt.

Mit dem DSG 2000 wurde die Datenschutzrichtlinie 95/46/EG umgesetzt. Art 18 dieser Richtlinie legt fest, dass das nationale Recht entweder die Meldung der Datenanwendung an eine Kontrollstelle oder - anstelle (bzw. zur Vereinfachung) einer solchen Meldeverpflichtung - einen (betrieblichen) Datenschutzbeauftragten vorzusehen hat. Der österreichische Gesetzgeber entschloss sich für die erste Variante, nämlich dass Datenanwendungen an eine Kontrollstelle, die Datenschutzkommission, zu melden sind. Vor diesem Hintergrund ist nicht ersichtlich, weshalb zusätzlich ein Datenschutzbeauftragter eingeführt werden soll. Die zusätzliche Einführung eines betrieblichen Datenschutzbeauftragten ist weder durch die EU-rechtlichen Vorschriften verlangt, noch auf nationaler Ebene erforderlich.

Das Erfordernis einer zwingenden Bestellung eines betrieblichen Datenschutzbeauftragten in Betrieben mit mehr als 20 Beschäftigten ist vielmehr nicht nachvollziehbar, sehen doch auch die Erläuterungen keine inhaltliche Begründung für diese Maßnahme vor.[2] Den Unterlagen zur Pressekonferenz betreffend die DSG-Novelle der Frau Staatsekretärin im Bundeskanzleramt Heidrun Silhavy sowie des Abg. z. NR Johann Maier ist zu entnehmen, dass die Installierung eines

[2] Die Erläuterungen zu Z 34 enthalten lediglich den Hinweis, dass die Einführung eines betrieblichen Datenschutzbeauftragten eine langjährige Forderung der Arbeitnehmervertretungen sei.

betrieblichen Datenschutzbeauftragten ihren Grund (auch) in den jüngst in Deutschland zu Tage getretenen Überwachungsmaßnahmen eines deutschen Lebensmitteldiskonters hat.

Es muss aber bezweifelt werden, dass ein zwingend einzurichtender betrieblicher Datenschutzbeauftragter die geeignete Maßnahme ist, Vorfälle wie in Deutschland zu verhindern.
Vielmehr gewährleisten in Österreich die im Arbeitsverfassungsgesetz normierten Befugnisse des Betriebsrates bereits einen ausreichenden Schutz der Interessen der Mitarbeiter, sodass die Einführung eines zwingend zu bestellenden betrieblichen Datenschutzbeauftragten jedenfalls nicht notwendig ist:

Der Betriebsrat hat das Recht, in allen Angelegenheiten, die die Interessen der Arbeitnehmer berühren, beim Betriebsinhaber und erforderlichenfalls bei den zuständigen Stellen außerhalb des Betriebes entsprechende Maßnahmen zu beantragen und die Beseitigung von Mängeln zu verlangen. Insbesondere ist der Betriebsrat berechtigt, Maßnahmen zur Einhaltung und Durchführung der die Arbeitnehmer des Betriebes betreffenden Rechtsvorschriften zu beantragen (§ 90 Abs. 1 ArbVG).

Die Einführung von Systemen zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten des Arbeitnehmers, die über die Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen hinausgehen, bedarf zu ihrer Rechtswirksamkeit der Zustimmung des Betriebsrates. Die Zustimmung des Betriebsrates kann nur durch die Entscheidung der Schlichtungsstelle ersetzt werden.

Die Einführung von Kontrollmaßnahmen und technischen Systemen zur Kontrolle der Arbeitnehmer, sofern diese Maßnahmen (Systeme) die Menschenwürde berühren, sind ohne die Zustimmung des Betriebsrates jedenfalls unzulässig (§ 96 Abs. 1 Z 3 ArbVG).

In Betrieben ohne Betriebsrat ist die Einführung von Kontrollmaßnahmen und technischen Systemen, welche die Menschenwürde berühren, nur mit Zustimmung der Arbeitnehmer zulässig (§ 10 Abs. 1 AVRAG).

Abgesehen davon können im Bedarfsfall im Rahmen der Bildungsfreistellung (§ 118 ArbVG) verstärkt Lehrveranstaltungen zum Thema Datenschutz besucht werden.

Es ist somit ein umfangreiches und völlig ausreichendes rechtliches Instrumentarium für die Wahrung des Datenschutzes (betreffend die Arbeitnehmer) in den Betrieben vorhanden. Die Einführung des Datenschutzbeauftragten würde vor allem dazu führen, dass die Arbeitgeber weiteren Arbeitnehmern bezahlte Freistellungen für Aktivitäten gewähren müssten, die nicht im Arbeitsvertrag vorgesehen sind und nicht dem Unternehmensziel dienen. Schon derzeit werden bezahlte Freistellungen für Betriebsräte, Jugendvertrauensräte, Behinderten-Vertrauenspersonen, Sicherheitsvertrauenspersonen, etc. gewährt. Zusätzliche Aufgaben und Weiterbildungserfordernisse (sofern diese im Einzelfall tatsächlich notwendig sein sollten) sind daher im Rahmen der schon vorhandenen Belegschaftsorgane und deren Freistellungs- und Weiterbildungsmöglichkeiten wahrzunehmen.

Im Übrigen ist es nicht Aufgabe des DSG, Mitwirkungsrechte des Betriebsrates, wie im § 15a Abs. 2 des Entwurfs vorgesehen, zu normieren. Solche Regelungen sind in der Arbeitsrechtsordnung grundsätzlich dem Arbeitsverfassungsgesetz zugeordnet und wäre eine Regelung im DSG systemwidrig. Zudem lässt die vorgeschlagene Formulierung des § 15a die Frage offen, zu

welcher Seite von innerbetrieblichen Sozialpartnern so ein Datenschutzbeauftragter zuzuordnen wäre. Auch hier kommt es zu einer Konstellation, die auf das geltende Recht als Fremdkörper einwirkt.
Weiters scheint auch aus arbeitsverfassungsrechtlicher Sicht fraglich, ob es nicht allein Sache des Arbeitgebers ist, wen er zum Datenschutzbeauftragten bestellt. Dies gilt umso mehr für die Möglichkeit der Bestellung einer betriebsfremden Person, die jedenfalls dem Betriebsinhaber allein zustehen muss (wobei es innerhalb verbundener Unternehmen möglich sein muss, den Mitarbeiter eines anderen Unternehmens auch für das eigene Unternehmen zum Datenschutzbeauftragten zu bestellen). Eine vergleichbare Regelung über Mitwirkungsrechte des Betriebsrats bei den in den Erläuterungen angesprochenen Sicherheitsfachkräften findet sich auch in den §§ 73ff AschG nicht. Mitwirkungsrechte des Betriebsrates sind grundsätzlich im ArbVG zu regeln.

Völlig abzulehnen ist die geplante Regelung des Abs. 4. Es wären u.a. allen MitarbeiterInnen, die mit der Verwendung von personenbezogenen Daten betraut sind, zumindest vier (im ersten Dienstjahr acht) Stunden p.A. für Beratungen mit dem Datenschutzbeauftragten zur Verfügung zu stellen. In vielen Dienstleistungsunternehmen sind nahezu alle MitarbeiterInnen „mit der Verwendung von Daten betraut". Hier fielen insgesamt erhebliche Beratungsstunden p.A. an. Dem betrieblichen Datenschutzbeauftragten selbst sind im ersten Jahr seiner Tätigkeit zumindest 40, in den folgenden Jahren zumindest 20 Stunden an Arbeitszeit zum Erwerb von Fachkenntnissen und zur Weiterbildung auf dem Gebiet des Datenschutzes zur Verfügung zu stellen.

Die Regelung des Abs. 4 würde insgesamt erhebliche Kosten für die Wirtschaft nach sich ziehen: Für die Erfüllung der Bestimmung des § 15a Abs. 4 des Entwurfs betreffend den betrieblichen Datenschutzbeauftragten würden für alle unter die Bestimmung des § 15a des Entwurfs fallenden Unternehmen allein der Bundessparte Information und Consulting insgesamt ca. 2,5 Mio. Euro pro Jahr an Kosten verursacht; die Erfüllung der Bestimmung des § 15a Abs. 4, 1. Satz des Entwurfs würde allein für die Unternehmen der Bundessparte Information und Consulting ca. 39 Mio. Euro pro Jahr nach sich ziehen.

Diese Kosten könnten auf Grund des Betriebsbegriffes in § 15 a Abs. 1 sogar noch wesentlich höher sein! § 15 a Abs. 1 stellt nämlich auf „Betriebe iSd § 34 ArbVG" ab, womit nicht zwingend die rechtliche Einheit (= Unternehmen), auf welche die Beschäftigungsstatistik abstellt, gemeint ist, sondern beispielsweise jede Filiale erfasst sein kann, sofern sie die Beschäftigtengrenze überschreitet." Diese Konsequenz, auch noch für „Teile" eines Unternehmens eigene Datenschutzbeauftragte bestellen zu müssen, ist - abgesehen von der generellen Ablehnung der Regelung - extrem überschießend.

(In diesem Zusammenhang stellt sich im Übrigen auch die Frage, ob die Definition des „Betriebes" gemäß § 34 Abs. 1 des Arbeitsverfassungsgesetzes im Sinne des § 15a Abs. 1 DSG auch Körperschaften öffentlichen Rechts (z.B. auch Kammern) und sonstige öffentliche Rechtsträger umfasst.)

Allein die beispielsweise dargestellten Kosten zeigen, welche wirtschaftlichen Konsequenzen die Bestellung eines betrieblichen Datenschutzbeauftragten für Unternehmen nach sich zieht, ohne dass ein Mehrwert für den Datenschutz erkannt werden kann.

Der Hinweis im Vorblatt der Erläuterungen „durch die Einführung eines betrieblichen Datenschutzbeauftragten kommt es zu einem marginalen Mehraufwand für Unternehmen, weil

ein zusätzliches Feld in der DVR-Meldung ausgefüllt werden muss", scheint angesichts der dargestellten erheblichen Kostenbelastung für Unternehmen nicht nachvollziehbar. Auch wenn das Standard-Kosten-Modell nur den Aufwand für Meldeverpflichtungen berücksichtigt, ist es keineswegs gerechtfertigt, hinsichtlich der Einführung eines betrieblichen Datenschutzbeauftragten von einem lediglich „marginalen Mehraufwand für Unternehmen" zu sprechen.

Im Übrigen sind die Rechte und Pflichten des Datenschutzbeauftragten überschießend geregelt: Gemäß § 15a Abs. 3 des Entwurfes hat er die Pflicht, bei Verdacht einer Verletzung datenschutzrechtlicher Vorschriften auf die Herstellung des rechtmäßigen Zustandes hinzuwirken. Außerdem hat er die Einhaltung der datenschutzrechtlichen Vorschriften zu überwachen, zu beraten und kann sich unter den Voraussetzungen des § 30 Abs. 1 a sogar an die Datenschutzkommission wenden. Wie oben dargestellt, sind die derzeitigen Instrumentarien über den Betriebsrat erheblich besser geeignet und ausreichend.

Dass der betriebliche Datenschutzbeauftragte per Gesetz in seiner Funktion nicht an Weisungen des Betriebsinhabers gebunden sein soll - selbst wenn diese konform mit dem DSG sein sollten - ist jedenfalls abzulehnen. Ein gesetzlicher Eingriff in die betriebsinternen Abläufe eines privatrechtlich organisierten Unternehmens ist sowohl wirtschaftlich als auch rechtlich bedenklich.

Die Verantwortlichkeit des Datenschutzbeauftragten nach der vorgeschlagenen Bestimmung ist zudem unklar. Die Verantwortung für die Einhaltung der Bestimmungen des DSG trägt auch weiterhin der „Betriebsinhaber". Dem Betriebsinhaber (dem Unternehmer) sollte es überlassen bleiben, mittels welcher Maßnahmen er für die Einhaltung der ihm obliegenden Verpflichtungen nach dem DSG Sorge trägt.

Angesichts der Tatsache, dass in Österreich mit dem System der freiwilligen Bestellung von Datenschutzbeauftragten gute Erfahrungen gemacht werden konnten, eine obligatorische Bestellung eines betrieblichen Datenschutzbeauftragten als ungeeignet angesehen wird und zu unverhältnismäßig hohen Kosten bei den Unternehmen ohne einen Mehrwert führen würde, **lehnt die Wirtschaftskammer Österreich dieses Vorhaben strikt ab.**

Zu Z 38 (§ 17 Abs. 1a und b):

Vereinfachungen beim Registrierungsverfahren sind grundsätzlich zu begrüßen.

In diesem Zusammenhang regen wir zusätzlich an, in Unternehmen standardmäßig stattfindende Datenanwendungen, die heute noch dem Registrierungsverfahren unterliegen, in den Katalog der Standardanwendungen aufzunehmen.

Zu begrüßen ist grundsätzlich auch die Möglichkeit, der Meldepflicht in elektronischer Form nachzukommen. Zu bedenken ist aber zum einen, dass manche Meldepflichtige, insbesondere traditionelle Handwerksmeister, mitunter über keinen Internetzugang verfügen. Aus diesem Grund sollte auch eine praktikable Alternative zur automationsunterstützten Form der Meldung (d.h. wie bisher eine Möglichkeit in „konventioneller" Papierform) vorgesehen werden.
(Auch nicht auszuschließende technische Probleme sprechen für die Möglichkeit einer Meldung in Papierform. Denn - anders als nach den geltenden Bestimmungen - bedeutet eine fehlgeschlagene Online-Registrierung die Unzulässigkeit der Aufnahme der Datenanwendung.)

Vor allem ist jedoch die in **§ 17 Abs. 1a** vorgesehene verpflichtende Verwendung der Bürgerkarte problematisch und abzulehnen.

Es wäre dies das erste verwaltungsrechtliche Verfahren, bei dem eine Einbringung ausschließlich mit der Bürgerkarte erfolgen müsste, ohne dass ein Zweifelsgrund betreffend die Identität vorliegen muss. Bis dato konnten Eingaben auch ohne einen Identifikationsnachweis erfolgen. Mit der vorliegenden Änderung müssten Betriebe unter Umständen Investitionen für die Anschaffung von Lesegeräten etc. tätigen, die in keiner Relation zum Ausmaß der Benötigung stehen. Im Sinne des Projektes der Bundesregierung „Verwaltungskosten Senken für Unternehmen" ist die Wirtschaftskammer Österreich der Ansicht, dass Eingaben an das DVR auch weiterhin in unkomplizierter Form möglich sein sollen und ein Identitätsnachweis (auch in anderer Form als der Bürgerkarte) nur in Zweifelsfällen zu erbringen ist (§ 13 Abs. 4 AVG). Es ist nicht nachvollziehbar, dass bei Internetanwendungen betreffend die Identität andere Maßstäbe angewendet werden sollen, als in der „realen Welt". Dazu kommt Folgendes: Zumal juristische Personen selbst keine Bürgerkarte besitzen können, müsste eine natürliche Person (vertretungsbefugtes Organ) mit seiner persönlichen Bürgerkarte, auf der die Vertretungsbefugnis für die juristische Person aufscheint, einschreiten. Dies scheint unbefriedigend, zumal dies ja auch voraussetzt, dass jeder Vertretungsbefugte für eine juristische Person im Besitz einer persönlichen Bürgerkarte ist, die er zur Verfügung stellt, um den Verpflichtungen der juristischen Person nachkommen zu können.

Sollte ein solches Vorhaben trotz der oben angeführten Ablehnung realisiert werden, wäre jedenfalls erforderlich, dass parallel dazu Erleichterungen für die Unternehmen geschaffen werden (z.B. in Form von Förderungen) und auch das In-Kraft-Treten dieser Identifikations- und Authentifizierungsbestimmung zu einem späteren Zeitpunkt erfolgt.

Nach der Bestimmung des **§ 17 Abs. 1b** des Entwurfs soll der Betrieb einer meldepflichtigen Datenanwendung erst nach ihrer Registrierung aufgenommen werden dürfen. Dies ist in praktischer Hinsicht von großem Nachteil. Auch wenn gem. § 20 Abs. 1 des Entwurfs die Meldungen von Datenanwendungen lediglich einer Vollständigkeits- und Plausibilitätsprüfung unterzogen werden sollen, können kleine, irrelevante Fehlermeldungen dazu führen, dass der Betrieb der Datenanwendung gehemmt ist, ohne dass ein triftiger Grund für die Untersagung der Datenanwendung vorliegt.
Datenanwendungen sollen daher wie bisher gem. § 17 geltende Fassung grundsätzlich unmittelbar nach Abgabe der Meldung aufgenommen werden dürfen. Verzögerungen behindern die österreichische Wirtschaft in unverhältnismäßiger Weise und schaden dem österreichischen Wirtschaftsstandort.

Zu Z 42 (§§ 20 bis 22):

Gem. § 20 Abs. 3 geltende Fassung ist bei vorabkontrollpflichtigen Datenanwendungen gleichzeitig mit einem allfälligen Auftrag zur Verbesserung darüber abzusprechen, ob die Verarbeitung bereits aufgenommen werden darf. Es sollte überlegt werden, eine solche Möglichkeit auch in § 20 Abs. 4 neu vorzusehen.

Nach § 20 Abs. 5 soll eine Registrierung künftig formlos mittels schriftlicher Mitteilung abgelehnt werden und sollen überdies nach Fristablauf erstattete Verbesserungen nicht mehr berücksichtigt werden.
Es ist kein Grund erkennbar, warum die Behörde mit einfachen Mitteilungen Registrierungen ablehnen können soll. Da mit einer Ablehnung über Rechte/rechtliche Interessen von

Registrierungswerbern entschieden wird, hätte dies auch in Form einer Bescheiderlassung zu erfolgen.
Daran anknüpfend sei erwähnt, dass aus verfahrensökonomischen Gründen auch nachträgliche Verbesserungen zulässig sein sollten (vor Bescheiderlassung).

Gem. § 21 Abs. 3 ist der Auftraggeber von der Durchführung und vom Inhalt der Registrierung „in geeigneter Weise" zu verständigen. Da gem. § 17 Abs. 1b der Betrieb der Datenanwendung erst nach ihrer Registrierung aufgenommen werden dürfen soll, ist diese Verständigung von zentraler Bedeutung. Es müsste daher bei Beibehaltung des vorgeschlagenen § 17 Abs. 1b (vgl. aber die Bemerkung oben zu § 17 Abs. 1 b!) konkreter angegeben werden, auf welche Weise die Verständigung erfolgen soll.

§ 22 Abs. 1 letzter Satz ordnet an, dass Änderungen bei der Datenanwendung des registrierten Auftraggebers für die Dauer von 3 Jahren weiterhin ersichtlich gemacht werden müssen. Die Sinnhaftigkeit dieser Regelung ist nicht erkennbar. Diese Bestimmung könnte zu Auskunftsbegehren nach § 26 DSG führen, die letztlich mit einer Negativ-Auskunft im Sinne des § 26 Abs. 1 beantwortet werden müssen, da die Daten ja nicht mehr oder nicht mehr in der ursprünglichen Form verwendet werden.
Da auch den Erläuterungen keine Begründung für diese Bestimmung entnehmbar ist, sollte § 22 Abs. 1 letzter Satz entfallen.

Nach der Bestimmung des § 22 Abs 4 kann ein Auftraggeber im Falle der Rechtsnachfolge einzelne oder alle registrierten Meldungen des Rechtsvorgängers übernehmen, wenn er das innerhalb von 2 Monaten bekannt gibt. Die Frist ist im Hinblick darauf, dass zum Zeitpunkt der Rechtsnachfolge ein Unternehmen eine Vielzahl von Veränderungen treffen und viele Entscheidungen zu fällen sind, zu kurz und sollte auf zumindest 6 Monate verlängert werden.

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.

Zu Z 43 (§ 22a):

Abgelehnt wird der Vorschlag, der DSK mit dem Argument der in der Regel nur mehr automationsunterstützten Prüfung jederzeit die Überprüfung bereits registrierter Meldungen zu ermöglichen. Im Sinne der Rechtssicherheit muss Klarheit bestehen und darf eine Registrierung (Entscheidung) nicht nachträglich abgeändert werden, da sich sonst Sinn und Zweck der Registrierung bzw. der behördlichen Tätigkeit der Registrierung für den Auftraggeber erübrigen.

Zu Z 44 (§ 26 Abs. 1):

Entsprechend dem im Entwurf vorgesehenen neuen § 1 wird ausdrücklich angeführt, dass zwar natürliche Personen ein Auskunftsrecht haben, dem auch von Seiten juristischer Personen als Auftraggeber nachzukommen ist. Umgekehrt steht juristischen Personen kein Auskunftsrecht zu. Dies wird ausdrücklich abgelehnt (vgl. dazu auch die Bemerkungen zu § 1).

Ein Auftraggeber hat nach dem Entwurf jeder natürlichen Person Auskunft über die zu dieser Person verarbeiteten Daten zu geben, wenn sie dies schriftlich verlangt und ihre Identität in geeigneter Form nachweist. 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 47 (§ 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.

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 Negativ-Auskunft gem. § 26 Abs.1 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 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. Zusätzlich sei hier auf § 50 DSG hingewiesen, wonach ein Betreiber eines Informationsverbundsystems ohnehin für die Namhaftmachung des Auftraggebers zu sorgen hat.

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.

Diese Bestimmung führt zu einer Überreglementierung: das Datenschutzrecht statuiert mit seinem sehr weit gefassten Auskunftsrecht ohnehin schon ein hohes Maß an (derzeit kostenfreier) Befassung des Auftraggebers durch den Betroffenen. Die Unternehmen müssten allenfalls durch einfache Anfragen, ob es Datenverarbeitungen zur Person des Auskunftswerbers gibt, sämtliche möglichen Auftraggeber nennen oder die tatsächlichen Auftraggeber eruieren.

Zu Z 52 (§ 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.

Zu Z 54 (§ 30 Abs. 6a):

Mit dieser Bestimmung soll die Rechtssicherheit, die aus Registrierungsvorgängen resultiert, dezidiert in Frage gestellt werden. Die Datenschutzkommission hätte damit die Möglichkeit, in bereits erteilte Registrierungen rückwirkend massiv einzugreifen.

In den Erläuterungen werden einige Fälle aufgezählt, bei denen ein derartiger Eingriff zulässig sein soll, denen offenbar jedenfalls eine künftige „Gefahr im Verzug"-Eigenschaft zugeschrieben werden soll.

Durch diese Bestimmung wird die Möglichkeit geschaffen

- ohne verfahrenseinleitenden Akt/Bescheid,
- ohne Prüfungsverfahren,
- 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 unbestimmten Begriffes der *„wesentlichen Gefährdung schutzwürdiger*

Geheimhaltungsinteressen" ohne jegliche Determinierung ist diese Bestimmung gerade angesichts der gravierenden Konsequenzen, die aus einem solchen Eingriff entstehen können, in grundrechtlicher Hinsicht äußerst bedenklich.

Ob eine Datenanwendung regelkonform ist, hat bei der Registrierung beurteilt zu werden. Ist diese abgeschlossen, soll Rechtssicherheit bestehen und das Vertrauen darauf nicht nachträglich „erschüttert" werden.

Im Vertrauen auf die vollzogene Registrierung werden von Unternehmen äußerst teure Investitionen in sichere Datenverarbeitungssysteme gesteckt. Diese Bestimmung bedeutet einen wesentlichen Unsicherheitsfaktor für die gesamte Wirtschaft.

Sollten Daten tatsächlich „systematisch" unrichtig oder nicht aktuell sein, würde sich ein Anbieter in einem lebenden, von Konkurrenz geprägten Markt nicht behaupten können. Ein Telefonbuch mit falschen Telefonnummern wäre sicherlich unverkäuflich. Der kommerzielle Erfolg einer Datenanwendung ist ein Indikator dafür, dass verwendete Daten aktuell, richtig und vollständig sind. Wäre es nicht so, würden diese Informationen keinesfalls nachgefragt werden.

Sollen daher diese in den Erläuterungen verwendeten Begriffe wie etwa *„systematisch"*, *„unrichtig"* und *„nicht aktuell"* als wesentliche Gefährdungsindikatoren herangezogen werden, ist darauf zu verweisen, dass auch diesen Begriffen ein breiter Interpretationsspielraum innewohnt. Bis eine überprüfende Instanz eine endgültige Entscheidung trifft, kann das Unternehmen bereits in Konkurs sein.

Das Datenschutzgesetz regelt die Rechte von Betroffenen. Es gibt ausreichende Instrumentarien wie das Recht auf Richtigstellung und Löschung sowie Strafandrohungen, um Betroffene zu schützen.

Die Richtigkeit von Daten auf systematischer Ebene, also generelle Brauchbarkeit im Hinblick auf den Zweck der Verwendung, ist bei der Registrierung zu prüfen. Wenn die Rechtmäßigkeit einer Datenanwendung festgestellt wurde, ist es Sache des Marktes, Geschäftsmodelle und damit die Wirtschaftlichkeit von Vorhaben zu prüfen.

Zusammengefasst bewirkt diese Bestimmung einen Komplettumbau der bestehenden Kontroll- und „Verbesserungsarchitektur" des Datenschutzrechtes, insbesondere im Hinblick auf die bestehenden rechtlichen Möglichkeiten der Datenschutzkommission, und kann nicht in rechtsstaatlich befriedigender Weise bewerkstelligt werden.

Aus diesem Grund ist diese Bestimmung des § 30 Abs. 6a abzulehnen.

Zu Z 55 (§ 31):

In Abs. 1 der genannten Bestimmung soll eine neue Beschwerdemöglichkeit betreffend Bekanntgabe des Ablaufs einer automatisierten Einzelentscheidung hinzugefügt werden. Diese Beschwerdemöglichkeit ist allerdings kritisch zu hinterfragen.

Völlig offen ist anhand des Entwurfstextes, wie detailreich diese Entscheidung offen gelegt werden muss. Muss nur generell aufgeklärt werden, wie diese Entscheidung getroffen wird/wurde oder müssen Betriebsgeheimnisse über die gesamte dahinterstehende Geschäftspolitik (wie z.B. Kreditpolitik) offen gelegt werden? Muss die (kreditgebende)

Wirtschaft generell ihre Entscheidungsfindung erläutern oder ihre gesamte Scorecard, die ein wesentlicher Teil des Betriebsgeheimnisses ist, offen gelegt werden?

Eine derartige Beschwerdemöglichkeit birgt auch die Gefahr einer unkontrollierten Flut von Anfragen in sich, die zu erheblichen Kosten für die Unternehmen führen können.

Diese Vorschrift birgt daher für die Wirtschaft zwei grundlegende Probleme in sich: zum einen kann diese Vorschrift zur Zwangsoffenlegung von Betriebsgeheimnissen wie Kreditpolitik oder Scorecard führen, zum anderen entstehen nicht vorhersehbare Kosten durch eine nicht abschätzbare Anzahl an Anfragen.

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. 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 der Versuch der Schaffung von Regelungen für die Zulässigkeit von Videoüberwachung begrüßt. Das Anliegen, vorhersehbare Regelungen dafür zu haben, wer unter welchen Voraussetzungen Videoüberwachung zulässigerweise einsetzen darf, ist vorhanden. Jedoch werden die vorgeschlagenen Regelungen diesem Anliegen nicht in ausreichendem Maße gerecht und darf insbesondere nicht der Fall eintreten, dass derzeit bereits von der Datenschutzkommission für zulässig erachtete Videoüberwachungen ihre Rechtsgrundlage verlieren und entsprechend den vorgeschlagenen Übergangsbestimmungen nach dem 1. Juli 2010 nicht mehr rechtmäßig wären. Bereits erfolgte Registrierungen von Videoüberwachungen müssen jedenfalls auch über den 1. Juli 2010 hinaus gültig bleiben (vgl. auch unten Bemerkungen zu Z 86 und 87).

Jedenfalls muss von der sich aus § 50 c Abs. 1 ergebenden Möglichkeit der Schaffung von Standardanwendungen für Videoüberwachung in ausreichendem Maße Gebrauch gemacht werden. Eine entsprechende Änderung der Standard- und Muster-Verordnung 2004 sollte daher zeitgleich mit gesetzlichen Regelungen betreffend die Videoüberwachung in Kraft treten.

<u>Zu § 50 a Abs. 1:</u>

Videoüberwachung wird definiert als „systematische, insbesondere fortlaufende Feststellung von Ereignissen, die ein bestimmtes Objekt („überwachtes Objekt“) betreffen, durch technische Bildaufnahmegeräte“. Diese Definition ist extrem weit und weicht auch von jener ab, die die Datenschutzkommission den Ausführungen zur Videoüberwachung im Anhang des Datenschutzberichts 2007 (Seite 64) zugrunde gelegt hat. Insbesondere fällt unter die vorgeschlagene Begriffsbestimmung wohl jede Videoanlage, z.B. also auch wenn sie Kundenstromanalysen, Statistik etc. dient.

Die Datenschutzkommission hat in ihrer Entscheidung vom 11. Oktober 2005, K 121.036/0014-DSK/2005 ausgeführt, dass eine Verwendung von personenbezogenen Daten im Sinne des § 4 Z 1 DSG 2000 bei Bildaufzeichnung nur dann vorliegt, „wenn sie in der Absicht geschieht, die darauf vorhandenen Personen zu identifizieren, wobei es genügt, wenn diese Absicht nur für bestimmte

Fälle und nicht durchgängig besteht; dies schließt neben den vom DSG 2000 (§ 45) ohnehin insgesamt weitestgehend ausgenommenen Bildaufnahmen für private z.B. touristische Zwecke etwa Bildaufnahmen für Zwecke von Verkehrsstromanalysen, also für statistische Zwecke, oder auch künstlerische oder kommerzielle Film- und Fotoherstellung ohne Absicht der Identifikation allenfalls abgelichteter Personen vom Begriff der Ermittlung personenbezogener Daten aus. Fehlt das Kriterium der Identifizierungsabsicht nach dem Zweck der Herstellung von Film- oder Fotoaufnahmen, ist dieser Vorgang - abgesehen von Datensicherheitsaspekten - nicht datenschutzrelevant".

Diese Judikatur findet in der vorgeschlagenen Regelung keine ausreichende Entsprechung; insbesondere auch nicht im Zulässigkeitstatbestand des Abs. 3 Z 2.

Die Definition der Videoüberwachung setzt offenbar auch nicht voraus, dass die Bilddaten aufgezeichnet werden. Vielmehr ergibt sich aus § 50 a Abs. 3 Z 4 ausdrücklich, dass auch bloße Echtzeitwiedergabe von der Regelung erfasst sein soll. Im Hinblick darauf, dass derartige Systeme nach aktueller Rechtslage und zutreffender Ansicht der Datenschutzkommission (vgl. Datenschutzbericht 2007, Seite 65) keine Datenanwendungen sind, erfolgt auch in dieser Hinsicht eine unangemessene Ausweitung; dies gilt insbesondere auch für die Meldepflicht, da gemäß § 50 c Abs. 1 Z 1 die nur Echtzeitüberwachungen gemäß § 50 a Abs. 3 Z 4 ausgenommen sind. Nach letzterer Bestimmung ist ein Betroffener durch eine Videoüberwachung nur dann nicht in seinen schutzwürdigen Geheimhaltungsinteressen verletzt, wenn sich die Überwachung in einer bloßen Echtzeitwiedergabe (ohne Speicherung) erschöpft und sie zum Zweck des Schutzes von Leib, Leben und 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.

Zu § 50 a Abs. 3:

Hinsichtlich der Z 2 und 3 vgl. die Bemerkungen oben zu § 50 a Abs.1.

Videoüberwachung kann auch dem Unfallschutz dienen. Hiezu ist z.B. an Betriebsanlagen mit relevanten Unfallquoten zu denken. Es wird angeregt, den Unfallschutz als zulässige Begründung für betriebliche Videoaufzeichnungen gesetzlich festzuhalten.

Zu Z 5:

Ein gefährlicher Angriff gemäß § 16 SPG liegt nur bei einer vorsätzlich begangenen Handlung vor. Daher wären z.B. fahrlässige Sachbeschädigungen nicht erfasst.

Die lit. a bindet die Zulässigkeit daran, dass das überwachte Objekt bereits einmal Ziel und Ort eines gefährlichen Angriffes war und eine Wiederholung wahrscheinlich ist. Welche gefährlichen Angriffe dabei zu berücksichtigen sind, wird ganz detailliert ausgeführt. Obwohl es sich in Z 5 nur um eine demonstrative Aufzählung handelt, wird durch diese detaillierte Anführung der Voraussetzungen eine sehr enge Grenze gezogen, die es für die Rechtsanwendung wohl sehr schwer machen würde, auch andere Fälle, die diesen engen Grenzen nicht gerecht werden, zu berücksichtigen. Die Regelung ist daher höchst bedenklich.

Die Videoüberwachung kann nicht von einem bereits verwirklichten Angriff abhängig gemacht, sondern muss vielmehr schon als Prävention eingesetzt werden können. Auch in der Stellungnahme 4/2004 der Art. 29 - Datenschutzgruppe vom 11.2.2004 zum Thema „Verarbeitung

personenbezogener Daten aus der Videoüberwachung“ wird die Videoüberwachung zur Verhütung von Straftaten, etwa zur Verhinderung von Überfällen, angesprochen (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp89_de.pdf; vgl. weiters auch den Datenschutzbericht 2007, S 64). Das Abwarten eines schädigenden Ereignisses, insbesondere das gesetzlich erzwungene Erdulden einer Straftat, als Voraussetzung für die legale Einrichtung einer Videoüberwachung ist nicht adäquat.

Beispielsweise wird darauf hingewiesen, dass bestimmte Branchen wie etwa Trafiken, Hotels, Taxifahrer und Juweliere erfahrungsgemäß und statistisch belegbar besonders häufig Opfer von Raubüberfällen werden. Es kann durchaus sein, dass z.B. die einzelne Trafik in den letzten 10 Jahren noch von keinem Überfall betroffen war, jedoch trotzdem ein extrem hohes Gefährdungsrisiko besteht. Dasselbe gilt z.B. auch für Überfälle auf Nachtportiere im Eingangsbereich und im Bereich von Hotelhallen oder bei sonstigen ähnlich disponierten Berufen. Auch z.B. die Tatsache, dass ein Schienenfahrzeug oder Bahnhof Ziel oder Ort eines gefährlichen Angriffes war, muss wohl die Annahme rechtfertigen, dass auch andere (und nicht nur die betroffenen) Schienenfahrzeuge oder Bahnhöfe Ziel oder Ort eines gefährlichen Angriffes sein könnten.

Notwendig ist daher jedenfalls die Aufnahme eines „vorausschauenden“ Tatbestandes, etwa in der Weise, dass es auch als bestimmte Tatsache anzusehen ist, wenn das überwachte Objekt, etwa aufgrund seiner Lage, seiner mangelnden Einsehbarkeit, seiner Umgebung nach oder (bei Personen) etwa dem Beruf nach, erfahrungsgemäß einer besonderen Gefährdung von Leib, Leben oder Eigentum ausgesetzt ist. Die Tatbestände der lit. b bis e decken das Spektrum der Gefährdungstatbestände bei weitem nicht ab.

Abgesehen vom grundsätzlichen Mangel der Zulässigkeit für Präventionszwecke ist die zeitliche Einschränkung in der lit. 5 auf 10 Jahre ebenso wie die Bezugnahme auf eine allfällige kürzere Verjährungsfrist (welche im Übrigen allein mit dem Strafbedürfnis und dem Präventionszweck im Hinblick auf den jeweiligen Täter zu tun hat) nicht nachvollziehbar.

Nicht nachvollziehbar ist, dass es sich nach Z 5 lit. b und c um Personen mit überdurchschnittlichem Bekanntheitsgrad oder um verfassungsmäßige Organe handeln muss, während der Schutz des Betroffenen selbst nirgends ausdrücklich erwähnt wird. Auch ist die Bezugnahme auf eine „Person mit überdurchschnittlichem Bekanntheitsgrad in der Öffentlichkeit“ unpräzise und auslegungsbedürftig.

In lit. d wird als bestimmte Tatsache angeführt, dass „das überwachte Objekt ein beweglicher Gegenstand mit Geldwert von mehr als € 100.000,- oder ein Aufenthaltsort derartiger Gegenstände ist“. Diese Wertgrenze scheint völlig willkürlich angesetzt, jedenfalls viel zu hoch gegriffen und auch nicht praxiskonform handhabbar. Gerade bei besonders gefährdeten Kleinbetrieben wie z.B. Trafiken würde eine solche Wertgrenze nicht erreicht; auch etwa die in letzter Zeit gehäuft auftretenden Diebstähle von Altmetall zeigen, dass gefährliche Angriffe oft Orte betreffen, wo die zu überwachenden Gegenstände einen geringeren Wert aufweisen. Dazu kommt, dass z.B. die Anschaffung neuer Busse die Grenze von € 100.000,- übersteigen kann, bei zunehmendem Alter die Wertgrenze jedoch unterschritten wird.

Jedenfalls muss klargestellt sein, dass sich eine Wertgrenze auf die Gesamtheit der Gegenstände bezieht, die im „überwachten Objekt“ vorhanden sind. Im Übrigen würde die Beschränkung auf bewegliche Gegenstände vor allem wertvolle Gegenstände vom Überwachungsschutz dann

ausschließen, wenn diese derartig mit einem unbeweglichen Gegenstand verbunden sind, dass sie als dessen Teil zu betrachten sind. Auch diese Konsequenz dürfte nicht eintreten.

Der Schwellenwert müsste jedenfalls auf einen wesentlich niederen Betrag herabgesetzt werden.

Die Bundessparte Information und Consulting führt zu Z 6 Folgendes aus:
In dieser Bestimmung werden Rechtsquellen aufgezählt, die als Rechtfertigung für eine Videoüberwachung gelten können. Dabei ist bemerkbar, dass in der Aufzählung die Rechtsquelle „*Vertrag*" nicht erwähnt wird. Da die Grundlagen für Sorgfaltspflichten zu Gunsten Dritten auch vertraglicher Natur sein können, wird eine derartige Ergänzung um „*Verträge*" dringend angeregt.

Die Bundessparte Bank und Versicherung führt zu Abs. 5 Folgendes aus:
Diese Regelung ist im Hinblick auf das Bankgeheimnis gemäß § 38 BWG für Banken problematisch, wenn die Herausgabe allfälliger Daten und Materialien nicht im Rahmen eines Ausnahmetatbestands des § 38 Abs. 2 BWG gefordert wird.
Wenn beispielsweise ein Zivilgericht in einer konkreten Rechtssache die Bank auffordert, vorhandene Videodaten herauszugeben, muss die Bank die Übermittlung der gewünschten Informationen verweigern, andernfalls verletzt sie das Bankgeheimnis.
Es muss daher eine klare Regelung geben, dass dadurch § 38 Abs. 2 BWG nicht berührt wird.

Nach Abs. 6 dürfen mit einer Videoüberwachung gewonnene Daten von Betroffenen nicht automationsunterstützt mit anderen Bilddaten abgeglichen und nicht nach sensiblen Daten als Auswahlkriterium durchsucht werden.
Dieses Verbot gilt ausnahmslos, da die Novelle keinen "Einzelgenehmigungsvorbehalt" durch die DSK vorsieht.
Damit wären viele der heute im Einsatz befindlichen, z.T. bereits mit (Gesichtserkennungs-) Software gekoppelten Videoüberwachungsanlagen künftig verboten. Das solcherart in der DSG-Novelle 2008 vorgesehene ausnahmslose Verbot des Abgleichs von Bilddaten einer Videoüberwachung erscheint daher problematisch; im Gesetz sollten daher geregelt werden, unter welchen Umständen die DSK Ausnahmen vom Bilddatenabgleich genehmigen kann.
Ebenso sollte dieses Verbot nicht für Fälle des Abs. 5 (Übermittlung von aufgezeichneten Daten an die zuständige Behörde oder das zuständige Gericht wegen des Verdachts auf eine von Amts wegen zu verfolgende gerichtlich strafbare Handlung oder zur Abwehr oder Beendigung eines gefährlichen Angriffs) gelten.

In Abs. 7 wird darauf hingewiesen, dass „im übrigen ... auch für Videoüberwachung die §§ 6 und 7, insbesondere der Verhältnismäßigkeitsgrundsatz (§ 7 Abs. 3)" gilt. Dieser Hinweis zeigt, dass auch die zuvor angeführten Zulässigkeitstatbestände keine abschließende Orientierung für die Rechtsunterworfenen bieten können, weil jeweils im Einzelfall auch noch die Verhältnismäßigkeit geprüft werden muss. Dem Anliegen einer vorhersehbaren Regelung kann daher auf diese Weise nicht in ausreichendem Ausmaß Rechnung getragen werden.

Zu § 50 b:

Die grundsätzliche Speicherfrist von maximal 48 Stunden ist für die Praxis viel zu kurz. Videoaufzeichnungen von Freitagabend müssten Sonntagabend bereits wieder gelöscht werden. Angesichts der Tatsache, dass nicht alle Unternehmen am Wochenende tätig sind, ist diese Frist praxisfremd. Es wird daher eine grundsätzlich zulässige Speicherdauer von zumindest ca. 1 Woche angeregt.

Unklar ist auch, wie der nach § 50 b Abs. 2 geforderte Nachweis für die Erforderlichkeit einer längeren Aufbewahrungsfrist als die grundsätzlich vorgesehenen 48 Stunden zu erbringen sein wird. Es ist davon auszugehen, dass auf Basis einer derart kurzen Speicherfrist der ursprünglich verfolgte Überwachungszweck nicht mehr verfolgt werden kann. Es muss jedenfalls sichergestellt werden, dass eine aus Präventions-, Schutz- und Strafverfolgungsgründen erforderliche erheblich längere Speicherdauer ermöglicht wird.

Eine Löschung nach bereits 48 Stunden kann z.B. für die Kreditwirtschaft nicht in Frage kommen können.

In diesem Konnex ist auch darauf hinzuweisen, dass eine betroffene Person innerhalb dieser kurzen Frist das Auskunftsrecht gemäß § 50e geltend machen müsste, andernfalls kann es sein, dass der Auftraggeber, sofern er keine längere Aufbewahrungsdauer beantragte und diese auch seitens der DSK genehmigt bekam, gar nicht mehr in der Lage ist, dem Begehren auf Auskunft im Sinne des § 50e seitens des Betroffenen nachzukommen, da die Löschung des Bildmaterials in Befolgung des Gesetzes bereits durchgeführt wurde (vgl. dazu die Bemerkungen unten zu § 50 e).

Zu § 50 c:
An dieser Stelle darf nochmals auf das Anliegen der Schaffung von ausreichenden Standardanwendungen für Videoüberwachung hingewiesen werden.

Das aufwändige Verfahren der Vorabkontrolle führt, wie die bisherigen Erfahrungen gezeigt haben, oft zu großen Verzögerungen und sollte daher hinterfragt werden.

Hinsichtlich Abs. 1 Z 1 wird auf die Bemerkungen zu § 50 a Abs. 1 hingewiesen.

Zu § 50 d:

Nach der derzeitigen Regelung ist der Auftraggeber gemäß § 24 DSG verpflichtet, über den Zweck der Datenanwendung sowie Namen und Adresse des Auftraggebers in geeigneter Weise zu informieren. Diese Verpflichtung besteht nicht, sofern diese Informationen dem Betroffenen nach den Umständen des Falles ohnehin bereits vorliegen.

Diese Ausnahme ist nur konsequent, sollen damit doch unnötige Informations- und Kennzeichnungspflichten in jenen Fällen vermieden werden, in denen z.B. aufgrund des Anbringungsortes kein Zweifel an der Identität des Auftraggebers bestehen kann.

Eine gleichartige Ausnahmebestimmung wäre auch in § 50d Abs. 2 der Novelle aufzunehmen. Einerseits um auch aus Sicht der Betroffenen nicht erforderliche (erweiterte) Kennzeichnungen in jenen Fällen hintanzuhalten, in denen ohnehin kein Zweifel an der Identität des Auftraggebers besteht. Andererseits um die damit für Unternehmen verbundenen Verwaltungskosten zu reduzieren, die im Falle einer Auswechslung der bestehenden Informationen anfallen würden.

Abs. 2 sollte um eine Z 3 ergänzt 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 § 50 e:

§ 50 e normiert ein Auskunftsrecht aus Videoüberwachungen. Ein solches wird in der vorgeschlagenen generellen Ausformung abgelehnt.

Gemäß § 50 e soll dem Auskunftswerber eine Kopie der zu seiner Person verarbeiteten Daten übersendet werden bzw. kann er Einsichtnahme auf Lesegeräten verlangen bzw. sind gewisse Auskünfte schriftlich zu erteilen. Bei einem derartigen Auskunftsverlangen müssten sämtliche Bänder (z.B. über sämtliche Bahnhöfe bzw. Fahrzeuge eines Verkehrsunternehmens) durchgesehen werden. Dies würde einen unzumutbaren Arbeitsaufwand und damit verbundene Kosten verursachen.

Abgesehen von der grundsätzlichen Ablehnung eines Auskunftsrechts in der vorgeschlagenen generellen Form dürfte jedenfalls kein Auskunftsrecht in den Fällen des § 50a Abs. 3 Z 2 (auf öffentliche Wahrnehmung gerichtetes Verhalten) und in den Fällen des § 50a Abs. 3 Z 7 (Videoüberwachung zur Geltendmachung von Ansprüchen vor Gericht) und Abs. 5 (Verdacht auf gerichtlich strafbare Handlung oder Abwehr oder Beendigung eines gefährlichen Angriffs) bestehen, wobei für die beiden letzten Fälle auf die Bestimmungen der ZPO und der StPO über die Akteneinsicht verwiesen werden kann.

Die Kosten sollten auf keinen Fall vom Auftraggeber getragen werden müssen; die vorherige Leistung eines angemessenen Kostenersatzes wäre jedenfalls erforderlich. Ferner wird die Erteilung der verlangten Auskunft auch faktisch zum Großteil nicht möglich sein, da die Daten gemäß § 50 b schon nach 48 Stunden zu löschen sind (vgl. dazu auch die Bemerkung oben zu § 50 b).

Zu bedenken ist weiters, dass mit diesem Auskunftsrecht die Gefahr von Missbrauch verbunden wäre. Bei Videoaufnahmen werden natürlich immer auch andere Personen mit auf der Aufzeichnung zu sehen sein. Bei einer Einsichtnahme/Übermittlung der Aufzeichnung an den Auskunftswerber werden somit immer gleichzeitig auch schutzwürdige Interessen Dritter verletzt - dies kann nicht im Sinne des Gesetzes sein und auch durch den vorgeschlagenen Abs. 2 wird für diese Problematik keine adäquate Abhilfe geschaffen.

Auch in die Interessen des Auftraggebers selbst, wie insbesondere dessen Betriebs- und Geschäftsgeheimnisse dürfte durch ein Auskunftsrecht keinesfalls eingegriffen werden.

Im Übrigen ist auch unklar, wann ein Zeitraum im Sinne des Abs. 1 „möglichst präzise“ benannt ist.

Zu Z 86 und 87:

Gemäß § 60 Abs. 4 soll der 9a. Abschnitt am 1.3.2008 (also rückwirkend) in Kraft treten. Demgegenüber regelt § 61 Abs. 6, dass Videoüberwachungen, die vor dem Inkrafttreten der §§ 50a bis 50e registriert wurden, bis zum 1.7.2010 dann rechtmäßig sind, wenn sie den am 30.6.2008 geltenden datenschutzrechtlichen Bestimmungen genügen. Hier handelt es sich offenbar um ein Redaktionsversehen.

Im Übrigen ist der Zeitpunkt für das Inkrafttreten der Regelungen viel zu früh angesetzt. Wie bereits eingangs erwähnt besteht zur Novelle insgesamt und auch zum Bereich der Videoüberwachung im Speziellen erheblicher Diskussionsbedarf. Weiters müsste auch genug Zeit für die Umsetzung der Regelungen bleiben, sodass ein Inkrafttreten der Regelungen wohl frühestens am 1.7.2009 denkbar sein kann.

Unbedingt müsste gewährleistet sein, dass bereits derzeit genehmigte Videoüberwachungen auch nach der neuen Rechtslage als genehmigt gelten. In etlichen Bereichen wurden nach langen Gesprächen und Verhandlungen mit der Datenschutzkommission Modalitäten für die Videoüberwachung gewisser Berufsgruppen erreicht. Ein Erlöschen der Genehmigungen mit 1. Juli 2010 würde einen enormen Bürokratismus nach sich ziehen und wäre auch keinesfalls gerechtfertigt.

Das Vertrauen der Auftraggeber in die Rechtslage und die Qualifikation der DSK sind nur dann geschützt, wenn bereits registrierte Videoüberwachungen auch über den 1. Juli 2010 hinaus gültig bleiben, da jedenfalls davon auszugehen ist, dass bisherige Registrierungen dem gültigen Schutzniveau entsprechen.

Wir fordern daher nachdrücklich, dass schon erfolgte Registrierungen von Videoüberwachungen weiterhin aufrecht bleiben und ihre Geltung behalten.

Ergänzender Vorschlag:

Ergänzend übermitteln wir folgenden Vorschlag des FV der Finanzdienstleister betreffend der Bestimmung des § 28 Abs. 2 DSG:

„Seit einiger Zeit wird teilweise eine nicht nachvollziehbare Argumentation betreffend der angeblichen Möglichkeit sich aus Bonitätsdatenbanken gem. § 28 Abs. 2 DSG herausreklamieren zu können, vertreten, wenn die Daten einem „von vornherein nicht bestimmten Personenkreis“ zugänglich seien (zit nach LGZ Wien - nicht rechtskräftige E aus 2007). Diese Interpretation des Gesetzes ist extrem auf die Wortinterpretation gestützt und übersieht sowohl Praxis als auch rechtlichen Rahmen der Kredit- und Wirtschaftsauskunfteien vollkommen. Durch diese Interpretation bekommt der § 28 Abs. 2 eine niemals intendierte und in der Realität nicht akzeptable Anwendung. Diese Ideen haben keine Basis im geltenden Recht und stehen im Übrigen mit der klaren Intention des Gesetzgebers zu § 28 Abs. 2 DSG in Widerspruch (vgl. EB dazu): dort ist von Dateien die Rede, die bei Durchschnittsbetrachtung keine Gefährdung erzeugen. Das muss im Hinblick auf § 18 DSG für Bonitätsdaten kategorisch ausgeschlossen werden. Diese können keinesfalls unter § 28 Abs. 2 subsumiert werden, da diese Dateien keinesfalls als öffentlich zugängliche Datenanwendungen (iS des § 28 Abs. 2 DSG) angesehen werden können. Zum Unterschied zum § 28 Abs. 1 DSG, der hier nicht bestritten wird, ist der § 28 Abs. 2 DSG europarechtlich nicht vorgegeben. Der Sinn dieses Paragraph war in den Erläuterungen zum DSG 2000 hinlänglich diskutiert und wurde erst durch die übermäßige Interpretation durch einzelne Gerichte ein Problem. Um dieser übertriebenen Interpretation Vorschub zu leisten und Rechtssicherheit für alle Betroffenen herzustellen, sollte hier eine gesetzliche Klarstellung des § 28 Abs. 2 DSG vorgenommen werden oder dieser Paragraph gänzlich gestrichen werden.

Es wird daher folgender, ergänzender Formulierungsvorschlag zu § 28 Abs. 2 DSG 2000 gemacht: „Dateien, welche für Übermittlungen eine Bescheinigung gem. § 7 Abs. 2 benötigen oder eine solche tatsächlich vorsehen, sind schon aus diesem Grund nicht öffentlich zugänglich“.“

Zur Frage eines Datenschutz-Gütesiegels:

Zu der im Begleitschreiben des Bundeskanzleramts-Verfassungsdienst zur gegenständlichen Novelle aufgeworfenen Frage der Einführung eines „österreichischen Datenschutz-Gütesiegels“ wird mitgeteilt, dass kein Bedarf für ein derartiges Gütesiegel gesehen wird.

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

Dr. Reinhold Mitterlehner
Generalsekretär-Stv.