Österreichischer Rechtsanwaltskammertag | Die österreichischen Rechtsanwälte

Bundeskanzleramt
Verfassungsdienst
Ballhausplatz 2
1014 Wien

E-Mail: v@bka.gv.at
begutachtensverfahren@parlament.gv.at

Zl. 13/1 08/69

GZ 810.026/0002-V/3/2008
BG, mit dem das Datenschutzgesetz 2000 geändert wird (DSG-Novelle 2008)

Referent: Dr. Rainer Knyrim, Rechtsanwalt in Wien

Sehr geehrte Damen und Herren!

Der Österreichische Rechtsanwaltskammertag dankt für die Übersendung des Entwurfes und erstattet dazu folgende

S t e l l u n g n a h m e :

Der Österreichische Rechtsanwaltskammertag begrüßt die Initiative, das österreichische Datenschutzgesetz zu novellieren, und ist erfreut über den Umfang, mit dem dieses Projekt sichtlich ernsthaft angegangen wurde. Von den verschiedenen innovativen Gedanken des Entwurfes greifen wir die nachstehenden heraus und erlauben uns zu diesen Folgendes mitzuteilen:

1. Einschränkung des Grundrechtschutzes auf natürliche Personen

Auch wenn der Gedanke hinter der in § 1 des Entwurfes vorgesehenen Einschränkung des Grundrechtschutzes auf natürliche Personen vielleicht die Entlastung von Unternehmen gewesen sein könnte, dürfte diese Einschränkung letztlich für Unternehmen negative Konsequenzen haben: Unternehmen ist es damit künftig unmöglich – insbesondere auch durch die nunmehr ausdrückliche Einschränkung des Auskunftsrechtes in § 26 Abs 1 DSG 2000 auf natürliche Personen –, ihre Rechtsposition im Hinblick auf die Verarbeitung ihrer Daten zu verteidigen. Wird der Grundrechtschutz tatsächlich auf natürliche Personen eingeschränkt, so ist es Unternehmen künftig etwa nicht mehr möglich, bei Werbezusendungen eine Auskunft nach § 26 DSG zu verlangen, woher das Werbung zusendende Unternehmen spezifische Informationen über das Unternehmen hat, die der Werbesendung zu Grunde liegen. Ebenso wenig haben sie ein Recht auf Richtigstellung, Löschung oder Widerspruch nach §§ 27 ff DSG 2000. Zwar könnte sich ein Unternehmen gegen einen unrechtmäßigen Anruf oder eine unrechtmäßige E-Mail nach § 107 TKG 2003 zur Wehr setzen, dies würde aber –

wenn überhaupt – bloß zu einem Stopp der Werbesendungen führen, aber für das Unternehmen nicht die vielleicht sehr wesentliche Frage lösen, woher das andere Unternehmen die Informationen über das eigene Unternehmen erhalten hat.

Dies gilt nicht nur für den Bereich von Werbezusendungen, sondern insbesondere auch für den gerade für Klein- und Mittelbetriebe immer wichtiger werdenden Bereich der Bonitätsbeurteilung. Möchte ein Klein- und Mittelbetrieb etwa wissen, wie ein anderes großes Unternehmen (etwa eine Bank, ein Telekommunikationsunternehmen oder eine Kreditratingagentur) zu seiner Bonitätsbeurteilung kommt und woher es die dafür erforderlichen Daten erhalten hat, so hätte es in Zukunft keine Möglichkeit mehr, diese Information zu erlangen, da § 26 DSG 2000 ja ausdrücklich nicht mehr anwendbar wäre. Ebenso wenig könnte es sich nach den §§ 27 ff DSG 2000 künftig gegen eine diesbezügliche Datenverarbeitung wehren.

Der Hinweis in den Erläuterungen zur Novelle, dass für Unternehmen künftig weiter der allgemeine Schutz des Berufs- und Geschäftsgeheimnisses bestehe, ist in diesen Fällen nicht hilfreich, da es sich bei den von einem dritten Unternehmen für Werbezwecke oder Bonitätsbeurteilung verwendeten Daten nicht unbedingt um Berufs- oder Geschäftsgeheimnisse handeln muss und sich umgekehrt umso mehr dritte Unternehmen gerade auf dieses Berufs- und Geschäftsgeheimnis berufen könnten, um Auskünfte zu der von ihnen durchgeführten Datenverwendung zu verweigern. Siehe zu den sehr eingeschränkten Möglichkeiten juristischer Personen, ihre Daten *ohne* Rückriff auf das DSG etwa bloß nach ABGB zu schützen, näher bei *Rebhahn,* Geheimnisschutz – Datenschutz – Informationsschutz: System und Prinzipien, in *Studiengesellschaft für Wirtschaft und Recht (Hrsg.),* Geheimnisschutz - Datenschutz - Informationsschutz (Linde 2007), 5 f, 17 f, 20 f und im selben Werk auf Seiten 140 f und 148 ff bei *Kramer,* Der zivilrechtliche Schutz von Geheimnissen, Daten und Informationen.

Der Österreichische Rechtsanwaltskammertag lehnt die Einschränkung des Grundrechtes auf Datenschutz auf natürliche Personen daher ab und erlaubt sich anzumerken, dass in Diskussionen mit verschiedensten Unternehmen im Vorfeld der Abgabe dieser Stellungnahme auch von diesen eine solche Einschränkung ausschließlich abgelehnt wurde.

Hingewiesen wird in diesem Zusammenhang auch auf ein kürzlich ergangenes Urteil des VG Wiesbaden (VG Wiesbaden, Urteil vom 7.12.2007, 6 E 928/07, online abrufbar unter http://www.jurpc.de/rechtspr/20080070.htm). In diesem Urteil wurde festgehalten, dass, obwohl im Bundesdatenschutzgesetz bzw dem Hessischen Landesdatenschutzgesetz juristische Personen an sich nicht unter datenschutzrechtlichen Schutz fallen, sich juristische Personen des Privatrechts in Form der GmbH bzw GmbH & Co BetriebsKG auf das Recht der informationellen Selbstbestimmung insofern berufen können, als ihren Trägern Schutz gegen unbegrenzte Erhebung, Speicherung, Verwendung oder Weitergabe der betreffenden individualisierten oder individualisierbaren Daten zusteht. Personenbezogene Daten sind laut diesem Urteil nämlich auch Daten, welche aus einer wirtschaftlichen Betätigung hervorgehen, und Wirtschaftsdaten einer juristischen Person personenbezogene Daten einer natürlichen Person, wenn diese einer Person als Alleinaktionär oder –gesellschafter zuzurechnen sind. Aus diesem

Tuchlauben 12 | A-1010 Wien | Tel. +43 (1) 535 12 75 | Fax +43 (1) 535 12 75-13 | rechtsanwaelte@oerak.at | www.rechtsanwaelte.at

Urteil ist zu ersehen, dass selbst dann, wenn das Grundrecht auf Datenschutz in Österreich auf natürliche Personen eingeschränkt würde, es durchaus zu erwarten ist, dass auch in Österreich im „Umweg“ der Judikatur der Grundrechtschutz auf bestimmte Arten von juristischen Personen – etwa GmbHs mit Alleinaktionären oder Alleingesellschaftern – ausgedehnt wird. Im Ergebnis käme es somit zu einem teilweisen Grundrechtschutz von juristischen Personen je nach Ausgestaltung der Gesellschafter- oder Kapitalstruktur. Somit würden nicht nur Rechtsanwälte je nach der Form ihres Tätigwerdens als Einzelanwalt (somit natürliche Person) oder in Form einer juristischen Person (GmbH) oder Personengemeinschaft (OG) einmal unter den Grundrechtschutz fallen und einmal nicht, sondern sämtliche andere Erwerbstätige in Österreich auch. Dass der Grundrechtschutz je nach – meist gesellschaftsrechtlich oder steuerrechtlich bedingter – Form des Tätigwerdens von Personen bzw Unternehmen vorliegt oder nicht, dürfte nicht das seitens des Gesetzgebers gewünschte Ergebnis einer Einschränkung des Grundrechtschutzes auf natürliche Personen sein. Die nunmehr plötzlich vorgeschlagene Einschränkung auf natürliche Personen ist auch insofern nicht nachvollziehbar, als juristische Personen ausdrücklich seit dem DSG 1978 bzw dessen In-Kraft-Treten am 1.1.1980, somit seit 28 Jahren, vom Grundrechtschutz umfasst sind und mittlerweile auch der Europäische Gerichtshof für Menschenrechte und der VfGH in ihrer Rechtsprechung anerkannt haben, dass auch juristische Personen den Schutz des Art 8 MRK genießen (EGMR, Niemitz/Bundesrepublik Deutschland, Urteil vom 16.12.1992; VfGH 28.11.2001, B 2271/00).

2. Präzisierung der Definition „Zustimmung“

Zu den Definitionen in § 4 des Entwurfes wird angeregt, die Definition der datenschutzrechtlichen Zustimmung so zu präszisieren, dass bislang bestehende Rechtsunsicherheiten beseitigt werden:

In einem – mittlerweile 23 Jahre alten – Rundschreiben des Verfassungsdienstes des Bundeskanzleramtes (BKA-VD, 810.008/1-V/1a/85 vom 10.8.1985) hat dieser zur Form einer ausdrücklichen Zustimmungserklärung festgehalten, dass eine Zustimmungserklärung deutlich vom übrigen Text eines Formulars abzusetzen ist und diese vom übrigen Formulartext derart zu trennen ist, dass eine gesonderte Unterfertigung der Zustimmungserklärung möglich ist. Diese Ansicht hat sich immer mehr auch auf „normale“ Zustimmungserklärungen übertragen. Der Oberste Gerichtshof hat allerdings parallel dazu in den letzten neun Jahren in einer Serie von Entscheidungen festgehalten, dass Zustimmungsklauseln zwar transparent sein müssen, aber dennoch in Allgemeinen Geschäftsbedingungen oder Vertragsformblättern enthalten sein können, sofern sie dort hervorgehoben sind. Eine gesonderte Unterfertigung fordert der Oberste Gerichtshof nur dann, wenn die datenschutzrechtliche Zustimmungserklärung gleichzeitig eine Entbindung vom Bankgeheimnis nach § 38 Abs 2 Z 5 BWG enthält (einen Überblick über die Judikatur enthält etwa *Knyrim,* Datenschutzrecht [Manz 2003], 170 ff; hinzuweisen ist auch auf die aktuellste Entscheidung des OGH zu dieser Frage, 4 Ob 221/06p vom 20.3.2007). In der Praxis führt dies zur Rechtsunsicherheit, ob nun Zustimmungserklärungen grundsätzlich oder nur bei geforderter Ausdrücklichkeit (§ 9 Z 6 idgF) vom übrigen Text der Allgemeinen Geschäftsbedingungen getrennt werden müssen.

Tuchlauben 12 | A-1010 Wien | Tel. +43 (1) 535 12 75 | Fax +43 (1) 535 12 75-13 | rechtsanwaelte@oerak.at | www.rechtsanwaelte.at

Weiters ist festzustellen, dass der Oberste Gerichtshof in seiner bisherigen, auf dem Transparenzgebot aufbauenden Judikatur einen mittlerweile kaum noch in die Praxis umsetzbaren strengen Maßstab an die Formulierung einer Zustimmungserklärung anlegt. Es ist gerade größeren Unternehmen mit einer Vielzahl von Konzerngesellschaften und Tätigkeitsbereichen kaum noch möglich, die vom Obersten Gerichtshof geforderten Kriterien einer transparenten Zustimmungserklärung zu erfüllen. Dies insbesondere im Hinblick auf die geforderte, möglichst abschließende Aufzählung aller datenempfangenden Konzerngesellschaften oder die genaue Beschreibung von vielleicht künftig erst stattfindenden Werbemaßnahmen oder Datenverwendungen und exakte Zuordnung zu verschiedenen Konzerngesellschaften (siehe etwa jüngst OGH 4 Ob 221/06p vom 20.3.2007). Würde den Forderungen des Obersten Gerichtshofes jeweils vollständig entsprochen, so bestünden datenschutzrechtliche Zustimmungserklärungen aus seitenlangen Aufzählungen von Übermittlungsempfängern, Datenverarbeitungszwecken, Datenarten und Werbeformen, was im Ergebnis für Konsumenten zu einer höchst unlesbaren bzw unzumutbaren Ausgestaltung führen würde. Dementsprechend ausführlich und abschließend formulierte Zustimmungserklärungen müssten überdies ständig überarbeitet und von den Konsumenten neu eingeholt werden, da sich deren Inhalt – entsprechend dem permanenten Umstrukturierungsprozess der globalen Wirtschaft – permanent ändern würde. Eine ständige Neueinholung der Zustimmungserklärung wäre für die Konsumenten ebenfalls unzumutbar.

Im Rahmen der Novellierung des DSG bietet sich daher die Gelegenheit, die Definition der „Zustimmung“ in § 4 so auszugestalten, dass ein ausgewogenes Maß zwischen den Transparenzinteressen der Konsumenten und einer möglichen Informationsüberflutung derselben sowie den Interessen der Unternehmen an administrierbaren datenschutzrechtlichen Zustimmungserklärungen hergestellt wird und der Umfang solcher Erklärungen auf ein vertretbares und lesbares Ausmaß eingeschränkt wird.

3. Parlamentarische Kontrolltätigkeit

Zu § 8 Abs 3 Z 2 lit b und § 9 Z 4 lit b des Entwurfes wird – im Hinblick auf die aktuelle Diskussion in Untersuchungsausschüssen etwa zur Frage, ob in Verwaltungsakten Daten über das Sexualleben von Bediensteten öffentlicher Dienststellen enthalten sind und die Akten daher unter Umständen geschwärzt vorzulegen sind – angemerkt, dass die absolute Ausnahme von Verwaltungsakten aus jeglicher Wertung und Interessensabwägung, die Kernbestandteil des Datenschutzgesetzes und auch der europäischen Datenschutzrichtlinie RL 95/46/EG sind, einen Bruch in der Datenschutzrechtsordnung darstellen würde. Auch wenn die Diskussion über personenbezogene Vorlage oder Nichtvorlage von Verwaltungsstellen gelegentlich etwas aufwendiger ist, so sollte doch überdacht werden, ob jeglicher Schutz von möglichen, in vorzulegenden Verwaltungsakten enthaltenen Daten von vielleicht unbeteiligten Personen aufgehoben wird oder ob es nicht doch zu einer Interessensabwägung kommen sollte. Für diese gibt es durchwegs greifbare Abwägungsrichtlinien (siehe dazu etwa *Knyrim,* Die Zulässigkeit

Tuchlauben 12 | A-1010 Wien | Tel. +43 (1) 535 12 75 | Fax +43 (1) 535 12 75-13 | rechtsanwaelte@oerak.at | www.rechtsanwaelte.at

der Bekanntgabe personenbezogener Daten an Untersuchungskommissionen am Beispiel der Stadt Wien, ZfV 2005, 694).

4. Ergänzung vorvertraglicher Daten

Zu § 8 DSG 2000 wird die Ergänzung angeregt, dass auch Daten, die im Vorfeld eines Vertragsverhältnisses verarbeitet werden müssen, um dieses zu Stande kommen zu lassen (vorvertragliche Maßnahmen, die auf Antrag der betroffenen Person erfolgen), ausdrücklich in dieser Bestimmung ergänzt werden, wie dies in Art 7 Abs 6 der Europäischen Datenschutzrichtlinie der Fall ist.

5. Betrieblicher Datenschutzbeauftragter

Der Österreichische Rechtsanwaltskammertag begrüßt die Einführung des betrieblichen Datenschutzbeauftragten, da dies der Befassung mit datenschutzrechtlichen Fragen sicher förderlich ist und dadurch Unternehmen motiviert werden, sich mehr mit der betrieblichen Datensicherheit und der Ausgestaltung der Unternehmens-EDV zu befassen, die heutzutage unabdingbare Themen für den Fortbestand der Unternehmen sind. Zu überlegen wäre, eine Definition für „Mitarbeiter“ in § 15a Abs 1 des Entwurfes einzufügen, um klarzustellen, ob es sich bei diesen um Vollzeit- oder Teilzeitkräfte oder auch freie Dienstnehmer handeln kann. Zu überlegen ist auch, warum unbedingt eigene Mitarbeiter des Betriebs für diese Funktion herangezogen werden müssen und nicht auch – wie etwa in Deutschland – externe Personen oder geeignete Unternehmen (die aufgrund bereits bestehender Fachkenntnisse weniger Schulungsbedarf im Sinne des § 15a Abs 4 des Entwurfes haben). Der Entwurf sieht dies bloß als „Notlösung“ vor, wenn kein geeigneter eigener Mitarbeiter zu finden ist.

Eine Erleichterung für Unternehmen, die mehrere Gesellschaften in Österreich haben, wäre auch, wenn für einzelne oder alle dieser Gesellschaften bloß ein und derselbe betriebliche (Konzern-)Datenschutzbeauftragte bestellt werden könnte. Dies ist sachlich rechtfertigbar, da heute in Konzernen in den verschiedenen Betrieben oft idente Software-Produkte mit identen Funktionalitäten implementiert werden, sodass die Themen und Fragen, die der betriebliche (Konzern-)Datenschutzbeauftragte zu erarbeiten hat, in allen Konzerngesellschaften dieselben oder sehr ähnlich sind und die mehrfache Befassung formal verschiedener Personen mit denselben materiellen Themen und Fragen daher eine Vergeudung von Personalressourcen wäre. Förderlicher wäre, wenn stattdessen einer einzigen Person mehr Zeit zur Verfügung steht, diese Themen und Fragen tiefgreifender aufzuarbeiten.

Im § 15a Abs 6 des Entwurfes bleibt unklar, ob es trotz dieser Bestimmung möglich ist, die Bereichsverantwortlichkeit nach § 9 Abs 2 VStG für den Bereich der Datenverarbeitung auf den betrieblichen Datenschutzbeauftragten zu delegieren. Wenn Unternehmen schon durch das Datenschutzgesetz angehalten sind, einen betrieblichen Datenschutzbeauftragten zu installieren, dann sollte es dem Unternehmen auch möglich sein, die entsprechende Verantwortlichkeit für diesen Bereich auch auf diese Person zu delegieren, was ein zusätzlicher Mehrwert für die Unternehmen wäre. Allenfalls müsste der betriebliche Datenschutzbeauftragte mit

Tuchlauben 12 | A-1010 Wien | Tel. +43 (1) 535 12 75 | Fax +43 (1) 535 12 75-13 | rechtsanwaelte@oerak.at | www.rechtsanwaelte.at

einer entsprechenden Anordnungsbefugnis im Sinne des § 9 Abs 4 VStG ausgestattet werden.

6. Online-Meldeverfahren – Verwendung der Bürgerkarte

Die beschleunigte Einbringung und Bearbeitung von DVR-Meldungen in elektronischer Form nach § 17 Abs 1a des Entwurfes ist grundsätzlich zu begrüßen. Bei der Gestaltung der Online-Applikation sollte aber darauf geachtet werden, dass nicht der Eindruck erweckt wird, dass die Befassung mit datenschutzrechtlichen Angelegenheiten durch das rasche und einfache Ausfüllen eines Online-Meldeformulares erledigt ist. Aus der täglichen Beratungspraxis der österreichischen Rechtsanwaltschaft zeigt sich, dass das Ausfüllen der Meldung oft nur ein geringer Teil bzw das Ergebnis einer davor wesentlich umfassenderen Beschäftigung mit der betrieblichen Datenverarbeitung eines Auftraggebers ist.

Zur vorgeschlagenen Verwendung der Bürgerkarte für Identifizierung und Authentifizierung im elektronischen Meldeverfahren laut § 17 Abs 1a des Entwurfes wurde dem Österreichischen Rechtsanwaltskammertag von verschiedenen Unternehmen eine sehr deutliche Ablehnung mitgeteilt. Dies deshalb, weil es sich, wie der Name schon sagt, bei dieser um eine „Bürger"-Karte handelt, nicht jedoch um eine „Unternehmens"-Karte. Fraglich ist daher, ob ein Unternehmen seine Mitarbeiter dazu „zwingen" kann, deren „private" Bürgerkarte – etwa deren eCard mit Bürgerkartenfunktion – für betriebliche Zwecke zum Einsatz zu bringen. Auch ist unklar, wie die Verbindung zwischen Mitarbeiter und Unternehmen im Hinblick auf die Kontrolle der „Zeichnungsberechtigung" bzw „Signaturberechtigung" hergestellt wird. Die Bürgerkarte stellt sich nicht als durchgängig sinnvolles Mittel zur Authentifizierung für Unternehmen dar. Ist der Mitarbeiter etwa nicht mehr im Unternehmen beschäftigt, so kann zwar eventuell der Zugang hinsichtlich seiner Person gesperrt werden, aber der eigentliche Schlüssel, die Karte, ist im Eigentum des Mitarbeiters (Bürgers) und kann daher nicht einfach eingezogen werden. Gerade bei komplexeren Systemen mit differenzierten Zugängen und Rechten würde die Bürgerkarte als Schlüssel zu Problemen führen. Besser wäre daher eine Karte mit einer qualifizierten Signatur, ausgestellt auf das Unternehmen oder einen Mitarbeiter in Verbindung mit einem Unternehmen. Seitens der Unternehmen wird daher eine Identifizierung und Authentifizierung unternehmerischen Handelns mit der Bürgerkarte einzelner Mitarbeiter äußerst kritisch gesehen; die Verwendung der Bürgerkarte in § 17 Abs 1a des Entwurfes ist daher abzulehnen. Stattdessen wird angeregt, in den Bestimmungen der §§ 4 und 5 E-Government-Gesetz eine Ausweitung der Bürgerkarte auf juristische Personen und Personengemeinschaften zu schaffen, um diesen den Rückgriff auf die Bürgerkarten ihrer Mitarbeiter zu ersparen.

7. Fehlerkorrektur

Der Österreichische Rechtsanwaltskammertag erlaubt sich höflich, auf zwei offensichtliche Tippfehler im Entwurf hinzuweisen: In § 21 Abs 1 Z 1 dürfte die Wortfolge „ergeben hat" überflüssig sein und in § 22a Abs 4 des Entwurfes dürfte

Tuchlauben 12 | A-1010 Wien | Tel. +43 (1) 535 12 75 | Fax +43 (1) 535 12 75-13 | rechtsanwaelte@oerak.at | www.rechtsanwaelte.at

nach der Wortfolge „zur Nachmeldung nicht entsprochen und ...“ das Wort „ist“ fehlen.

8. Stärkung der Position der Datenschutzkommission; Zentralisierung des Verwaltungsstrafverfahrens und Erhöhung der Transparenz im Verwaltungsstrafverfahren

Der Österreichische Rechtsanwaltskammertag begrüßt die Stärkung der Position der Datenschutzkommission durch § 30 Abs 6a des Entwurfes bei Gefahr im Verzug. Angeregt wird eine weitergehende Zentralisierung der Verwaltungsstrafverfahren weg von den Bezirksverwaltungsbehörden zu einer zentralisierten Verwaltungsbehörde oder zur Datenschutzkommission. Die tägliche Beratungspraxis der österreichischen Rechtsanwälte zeigt, dass die Bezirksverwaltungsbehörden auf das Thema Datenschutzrecht inhaltlich oft nicht vorbereitet sind und es dort teilweise nicht einmal vorgegebene Zuständigkeiten und geschulte Mitarbeiter gibt. „Zwangsbeglückte“ Verwaltungsbeamte ohne ausreichende Schulung und Zeit für das Anlernen datenschutzrechtlicher Themen scheinen in der Praxis mit Anzeigen zum Teil überfordert.

Die Verwaltungsstrafverfahren im Datenschutzrecht sind überdies vollkommen intransparent. Dies, da die Verwaltungsstrafbehörden sich aufgrund der mangelnden Parteistellung von Anzeigern auf das Datenschutzrecht der Angezeigten berufen und keinerlei Auskünfte über Einleitung, Fortgang oder wenigstens Abschluss des Verfahrens geben, was für anzeigende Personen – etwa auch Unternehmen, die mit derartigen Anzeigen gegen unzulässige Vorgangsweisen anderer Unternehmen vorgehen – äußerst frustrierend ist. Zwar wenden diese ihre Zeit und Kosten dafür auf, dass das Datenschutzrecht Beachtung findet, erhalten aber keineswegs das Gefühl, dass dies auch staatlicherseits der Fall ist, da Ihnen jegliche Information über den Ausgang ihrer Bemühung behördlicherseits verwehrt wird. Dementsprechend wird angeregt, den Anzeigern Parteistellung im Verfahren einzuräumen oder diese zumindest über den Verfahrensausgang – ähnlich § 30 Abs 7 DSG 2000 idgF – zu informieren und den Verwaltungsstrafbehörden auch eine Verpflichtung aufzuerlegen, dass Statistiken über Anzahl und Erledigung der Verfahren sowie über Höhe der Strafen erstellt und veröffentlicht werden. Letzteres etwa im Bericht der Datenschutzkommission nach § 38 Abs 4 DSG 2000 idgF aufgrund zentralisiert an die Datenschutzkommission gemeldeter Statistiken. Tatsache ist, dass keinerlei statistischen Informationen darüber in Österreich publik sind, ob Datenschutzrecht überhaupt (!) sanktioniert wird, was dazu führt, dass leider in Österreich „schwarze Schafe“ existieren, die ganz bewusst datenschutzwidriges Verhalten für ihren eigenen unternehmerischen Vorteil verwenden, da sie eine datenschutzrechtliche Sanktionierung nicht fürchten. Dieses Fehlen generalpräventiver Information führt letztlich zu einer Benachteiligung jener Unternehmen, die sich wohl verhalten, aber zusehen müssen, wie „schwarze Schafe“ staatlicherseits – vielleicht auch nur vermeintlich – ungestraft bleiben.

Tuchlauben 12 | A-1010 Wien | Tel. +43 (1) 535 12 75 | Fax +43 (1) 535 12 75-13 | rechtsanwaelte@oerak.at | www.rechtsanwaelte.at

9. Erhöhung der Verwaltungsstrafen

Im Sinne des vorher Gesagten wird auch angeregt, die Verwaltungsstrafen des § 52 auf ein Niveau zu heben, dass die oben genannten „schwarzen Schafe“ stärker abschreckt. Eine Maximalstrafe von EUR 18.890,-- für das vorsätzliche Verschaffen eines widerrechtlichen Zuganges zu einer Datenanwendung oder das Aufrechterhalten eines erkennbar widerrechtlichen Zuganges oder für das vorsätzliche Verletzen des Datengeheimnisses hat heute wohl kaum mehr abschreckende Wirkung. Im europäischen Vergleich sind Verwaltungsstrafen mit einem deutlich höheren Strafrahmen daher mittlerweile durchwegs üblich. Siehe auch *Kotschy,* Verwaltungsbehördlicher Rechtsschutz in Datenschutzangelegenheiten, in *Studiengesellschaft für Wirtschaft und Recht (Hrsg.),* Geheimnisschutz – Datenschutz – Informationsschutz (Linde 2007), 131 f, die anmerkt, dass „die Strafbestimmungen im DSG hinsichtlich ihrer generalpräventiven Wirkung gelegentlich zu überdenken sein werden …. Weiters sind die Strafobergrenzen nicht hoch genug, um als Kostenfaktor ins Gewicht zu fallen, weshalb auch kein erheblicher Anreiz zur Berücksichtigung besteht.“

10. Klarstellungen in § 46 zur wissenschaftlichen Forschung und Statistik

Die Novelle könnte zum Anlass genommen werden, im bisherigen § 46 einige Klarstellungen zu machen: Die Vergangenheit hat gezeigt, dass viele Anträge nach § 46 ihre Wurzeln in dem Wunsch von Archivverwaltungen haben dürften, heikle Entscheidungen (zB zeitgeschichtlicher Forschungsprojekte) an die Datenschutzkommission zu delegieren (siehe etwa DSK 202.001/3-DSK/00). Mit der Schaffung des geplanten digitalen Langzeitarchivs des Bundes dürfte dieses Problem noch virulenter werden. Es ist jedoch nicht „Kernaufgabe“ der Datenschutzkommission, den Zugang zu Archiven (etwa Schriftgut oder historische Behördenakten) zu genehmigen. Vielmehr sollte in § 46 ein Stichtag bzw Schutzfristen für Datenanwendungen und Dateien festgesetzt werden, bei deren Anwendbarkeit eine präsumptio iuris (widerlegbare gesetzliche Vermutung) gilt, dass die vom Datenbestand der Datei Betroffenen bereits verstorben oder jedenfalls wegen des Zeitablaufs und des historischen Charakters der Daten nicht mehr schutzwürdig sind. Zum Beispiel sämtliche Dateien (Karteien), die seit 1945 nicht mehr aktualisiert worden sind. Oder nach dem Geburts- oder einem Eintragungsdatum geordnete Karteien und Register (zB Geburtenbücher, Vereins-Mitgliederverzeichnisse udgl) hinsichtlich der Eintragungen von vor mehr als hundert Jahren.

Weiters ist die Qualifikationsanforderung in § 46 Abs 3 Z 3 idgF zu hinterfragen. Gefragt ist vielleicht nicht oder nicht ausschließlich die fachliche Aneignung des Antragstellers, sondern vor allem eine datenschutzrechtliche Zuverlässigkeit auch im Sinne einer adäquaten technischen Sicherung der Daten. Überdies sollte klargestellt werden, dass auch juristische Personen, Institute etc Träger einer Genehmigung nach § 46 sein können.

Zudem sollte der Fall geregelt werden, dass ein ausländischer Forscher am Werk ist oder ein länderübergreifendes Projekt durchgeführt wird. Dies ist etwa nicht nur bei geschichtlichen Forschungsprojekten, sondern auch im medizinischen und

Tuchlauben 12 | A-1010 Wien | Tel. +43 (1) 535 12 75 | Fax +43 (1) 535 12 75-13 | rechtsanwaelte@oerak.at | www.rechtsanwaelte.at

pharmazeutischen Bereich an der Tagesordnung. Derzeit würde etwa ein australischer Forscher, der in einer österreichischen Datenbank Daten ermittelt und in Österreich – etwa auf seinem Laptop – personenbezogene Daten verarbeitet, sich nahezu unausweichlich wegen Übertretung insbesondere von § 52 Abs 2 Z 1 und 2 idgF strafbar machen, wenn er das Flugzeug retour nach Sydney besteigt (wegen Datenexports in ein Land ohne adäquaten Datenschutz ohne ausdrückliche Genehmigung der Datenschutzkommission für die auf seinem Notebook gespeicherten Daten). Dementsprechend sollte die Genehmigung nach § 46 Abs 3 eine allfällige Datenexportgenehmigung beinhalten und gleichzeitig als Erfüllung der Registrierungspflichten gelten, da eine Prüfung der Zulässigkeit des Verwendungsvorganges ohnehin Teil des Genehmigungsverfahrens ist und die DSK allenfalls weiterhin beschränkende Auflagen vorschreiben kann.

Im Zuge der Behandlung der oben angeführten Punkte könnte im DSG auch explizit dargestellt werden, inwieweit der Datenschutz mit dem Tod einer Person endet. Als Ausfluss der Judikatur zu § 46 hat die Datenschutzkommission festgestellt (Bescheid DSK K 202.028/006-DSK/2003 vom 12.9.2003), dass das Grundrecht auf Datenschutz ein höchstpersönliches Recht sei, das mit dem Tod des Betroffenen erlösche und nicht auf Rechtsnachfolger übergehe. Träger dieses Grundrechtes könnten somit nur lebende Personen sein. Auch wenn diese Erkenntnis der DSK im Zusammenhang mit dem konkreten Bescheidhintergrund verständlich ist, so ist dennoch zu hinterfragen, ob das Datenschutzrecht nicht doch über den Tod hinausgeht und etwa in der Erbmasse des Verstorbenen eine – erhebliche – Rolle spielen kann. Aus der täglichen Beratung der Rechtsanwaltschaft sind dem Österreichischem Rechtsanwaltskammertag etwa Fälle bekannt, in denen Angehörige von Verstorbenen an den früheren Arbeitgeber des Verstorbenen die Aufforderung stellten, dessen E-Mail-Verkehr offen zu legen sowie allfällig auf dessen betrieblichen Computer abgespeicherte private Dateien herauszugeben, um Gewissheit darüber zu erlangen, ob der Verstorbene ein den Angehörigen unbekanntes, aber vermutetes außereheliches Verhältnis aus dem (allenfalls außereheliche Kinder entsprangen) hatte, was erhebliche Auswirkungen auf die Aufteilung der Erbmasse haben könnte.

Der vorher zitierten Entscheidung der Datenschutzkommission steht § 16 ABGB entgegen, der sich auch so interpretieren lässt, dass eine Fortwirkung von persönlichen Interessen – somit auch vom Interesse am Schutz von privaten oder sogar sensiblen Daten – über den Tod hinaus besteht. Nach herrschender Meinung erlischt etwa auch das Bankgeheimnis grundsätzlich nicht durch den Tod des Kunden (*Apathy* in *Apathy/Iro/Koziol* [Hrsg], Österreichisches Bankvertragsrecht, 2. Auflage 2007, Rz 2/61). Dies spielt insbesondere bei der sehr heiklen Frage eine Rolle, wer berechtigt ist, unter welchen Bedingungen von einer Bank über identifizierte und auch nicht identifizierte Einlagen des Verstorbenen Auskunft zu erlangen (siehe etwa OGH 15.5.1995, 7 Ob 610/95 oder *Sommer/Hirsch* in *Dellinger* [Hrsg], Bankwesengesetz, 1. Lfg, Dezember 2007, Rz 251 zu § 38 BWG). Warum das Datenschutzrecht zu einer völlig gegenteiligen Ansicht als das AGBG und das BWG kommen soll, ist daher nicht ganz verständlich und schafft entsprechende Rechtsunsicherheit. Eine gesetzliche Klarstellung würde hier Rechtssicherheit schaffen.

Tuchlauben 12 | A-1010 Wien | Tel. +43 (1) 535 12 75 | Fax +43 (1) 535 12 75-13 | rechtsanwaelte@oerak.at | www.rechtsanwaelte.at

11. „Entschärfung“ der Regelung zu Informationsverbundsystemen

Zu § 50 des Entwurfes wird angeregt, die Bestimmung zu den Informationsverbundsystemen zu „entschärfen“. Das Informationsverbundsystem des § 50 DSG 2000 stellt weltweit geradezu ein „Unikum“ im Datenschutzrecht dar und die Tatsache, dass heute vermutlich jeder größere Konzern über derartige Informationsverbundsysteme verfügt und vermutlich nur ein Bruchteil derselben entsprechend den gesetzlichen Bestimmungen des österreichischen Datenschutzgesetzes registriert oder, sofern notwendig, sogar bei der Datenschutzkommission vorab genehmigt sind, zeigt, dass hier Theorie und Praxis weit auseinanderklaffen. Zu überlegen wäre, ob der Tatbestand nicht auf ganz spezifische und bedeutende Anwendungen eingeschränkt wird (etwa die Informationsverbundsysteme im Bonitätsbereich oder im Sicherheitspolizeibereich, siehe zu Letzteren etwa *Wiederin,* Geheimnisschutz – Datenschutz – Informationsschutz im Sicherheitsrecht, in *Studiengesellschaft für Wirtschaft und Recht (Hrsg.),* Geheimnisschutz – Datenschutz – Informationsschutz (Linde 2007), 94 f). Damit könnten einfache Anwendungen wie etwa konzernweite Kontaktdaten oder Kundendatenbanken aus dessen Definition ausgenommen werden.

12. Videoüberwachung

Zu § 50a Abs 3 des Entwurfes wird angemerkt, dass seitens verschiedener Unternehmen in Diskussionen im Vorfeld zu dieser Stellungnahme der dort genannte Katalog als zu unpräzise und zu weitgehend kritisiert wurde. Eine Einschränkung und Präzisierung der Zulässigkeit von Videoüberwachung wird daher angeregt.

Zu § 50b Abs 2 wird vorgeschlagen, die grundsätzlich zulässige Speicherdauer auf 72 Stunden als absolutes Maximum auszudehnen. Anderenfalls müssten Aufzeichnungen von Einbrüchen oder Diebstählen in videoüberwachten Unternehmen, die am Freitag Abend nach Dienstschluss begangen werden, bereits am Sonntag Abend wieder automatisch gelöscht werden und wären somit bei Wiederaufsperren des Betriebes am Montag Morgen bereits nicht mehr einsehbar, was den Zweck einer solchen betrieblichen Überwachung zum Eigentumsschutz konterkarieren würde.

Zu § 50c Abs 1 Z 2 des Entwurfes ist – so die Rückmeldung verschiedener Unternehmen und Einzelpersonen an den Österreichischen Rechtsanwaltskammertag – diesen der dogmatisch-juristische Hintergrund für die Ausnahme analoger Speichermedien in dieser Bestimmung kaum nachvollziehbar. Sie betrachten die Einschränkung auf bloß digitale Speichermedien geradezu als Aufforderung, durch einen technologischen Rückschritt (Umstellung von Festplattenspeichermedien in Computern auf alte VHS-Videorekorder) möglichen datenschutzrechtlichen Problemen auf sehr einfache technische Weise aus dem Weg zu gehen, und daher als eine unbillige Möglichkeit, sich einer datenschutzrechtlichen Diskussion bzw Kontrolle zu entziehen. Umgekehrt wird die Aufnahme der Livebildübertragung in das Datenschutzrecht nicht verstanden. Eine für die Normadressaten verständlichere Lösung wäre daher zu bevorzugen.

Tuchlauben 12 | A-1010 Wien | Tel. +43 (1) 535 12 75 | Fax +43 (1) 535 12 75-13 | rechtsanwaelte@oerak.at | www.rechtsanwaelte.at

Der Österreichische Rechtsanwaltskammertag spricht sich weiters gegen das im Entwurf enthaltene, sehr umfangreiche und unbeschränkte Auskunftsrecht nach § 50e Abs 1 des Entwurfes aus. In der täglichen Beratung durch Rechtsanwälte zeigt sich bereits jetzt der Trend, dass das Auskunftsrecht des § 26 DSG 2000 immer mehr „missbraucht“ wird, um – statt ernsthafte persönliche datenschutzrechtliche Anliegen zu verfolgen – beim Gegenüber bloß Verwaltungsaufwand zu produzieren, um diesen zu „ärgern“. Besteht daher die Möglichkeit, unbeschränkt jederzeit Kopien der Videoaufzeichnung zu erhalten, so ist zu befürchten, dass es geradezu zum „Hobby“ von Personen wird, in den Aufnahmebereich von Videokameras zu treten, um danach eine Kopie der Aufzeichnung davon anzufordern. Im „Extremfall“ wäre es ein neues „Freizeitvergnügen“, etwa in einer Stadt durch möglichst viele Videokameras zu schreiten und sich danach von Dutzenden oder Hunderten Kameras die Videos schicken zu lassen, bloß um vielleicht mehr Aufzeichnungen „gesammelt“ zu haben als jemand anderer, ohne dass es diesen Personen dabei um ernsthafte datenschutzrechtliche Anliegen geht. Eine Einschränkung des Auskunftsrechtes auf Fälle, bei denen ein konkretes, wichtiges und überwiegendes Interesse an der Herausgabe einer Kopie der Aufzeichnung vom Antragsteller zu belegen oder zumindest zu behaupten ist, wird daher seitens des Österreichischen Rechtsanwaltskammertages angeregt.

Völlig unklar ist, wie es für ein größeres Unternehmen zu administrieren sein soll, wenn Videoaufzeichnungen zwar in äußerst kurzer Frist wieder zu löschen sind (etwa nach § 50b Abs 2 nach derzeitigem Entwurf binnen 48 Stunden), umgekehrt aber nach § 26 Abs 7 idgF, der im nachstehenden Sinn im Entwurf nicht angepasst wurde, ab dem Zeitpunkt der Kenntnis von einem Auskunftsverlangen die Daten über den Betroffenen in einem Zeitraum von 4 Monaten nicht mehr gelöscht werden dürfen. Stellt nämlich jemand in der 47. Stunde, nachdem er sich von einer Videokamera filmen hat lassen – vielleicht absichtlich, um jemanden zu „ärgern“ –, den Antrag beim „filmenden“ Unternehmen, ihm eine Kopie dieses Videos im Sinne des § 50e Abs 1 DSG 2000 zu übersenden, und richtet diesen Antrag an irgendeine „unbeteiligte“ Abteilung des Unternehmens, so ist von vornherein absehbar, dass das Unternehmen voraussichtlich organisatorisch nicht in der Lage sein wird, binnen bloß einer (!) Stunde eine derartige Anfrage so zu administrieren, dass genau jene Videoaufzeichnung genau jener Kamera binnen einer Stunde identifiziert und deren automatische Löschung technisch verhindert wird, auf der der Antragsteller zu sehen ist. In der derzeitigen Ausgestaltung des vorgeschlagenen Auskunftsrechtes des § 50e wäre es jedermann sehr leicht möglich, mit sehr einfachen Mitteln Unternehmer einer Verwaltungsstrafe nach § 52 Abs 1 Z 4 wegen der gesetzlich vorgeschriebenen Nichtlöschung der Videodaten, die vom Unternehmen nach Einlangen des Auskunftsantrages nicht rechtzeitig veranlasst wurde, in Höhe von EUR 18.890,-- auszusetzen.

13. In-Kraft-Treten

Zu den In-Kraft-Tretensbestimmungen des § 60 Abs 1 und Abs 4 wird vorgeschlagen, das In-Kraft-Treten auf 1.1.2009 zu verschieben, um den Unternehmen eine ausreichende Informations- und Reaktionsfrist auf die neuen Bestimmungen zu ermöglichen. Die Übergangsfrist für den betrieblichen Datenschutzbeauftragten in Abs 5 scheint mit 1.7.2009 angemessen lang.

Tuchlauben 12 | A-1010 Wien | Tel. +43 (1) 535 12 75 | Fax +43 (1) 535 12 75-13 | rechtsanwaelte@oerak.at | www.rechtsanwaelte.at

Umgekehrt wird zu § 61 Abs 9 angeregt, die Verordnung möglichst rasch zu erlassen, um Klarheit in diesem Bereich zu schaffen.

14. Ausstattung und Strukturierung der Datenschutzkommission

Die Datenschutzkommission selbst kritisiert in ihren Jahresberichten (online abrufbar unter www.dsk.gv.at) seit Jahren die untragbare Ressourcenausstattung insbesondere mit Personal. Wie die laufenden Jahresberichte zeigen, ist Österreich von einem datenschutzrechtlichen Vorzeigeland über die Jahre durch den dramatisch niedrigen Personalstand zu einem der Schlusslichter bei der Personalausstattung der Datenschutzkommissionen in ganz Europa geworden. Dies äußerst sich in entsprechend langen Verfahrensdauern, die insbesondere von internationalen Konzernen, die einen direkten internationalen Vergleich haben, regelmäßig sehr stark kritisiert werden und Negativpunkte des Wirtschaftsstandortes Österreich im internationalen Standortwettbewerb sind. Auch wenn die Mitarbeiter der Datenschutzkommission und des Datenverarbeitungsregisters ihr Bestes geben und, wie bekannt ist, regelmäßig auch an Sonn- und Feiertagen arbeiten, ist es nicht möglich, mit einer „Handvoll“ Mitarbeitern gleichzeitig die Datenschutzagenden der öffentlichen Hand zu kontrollieren, ein Datenverarbeitungsregister zu führen und die immer zahlreicheren Anträge von Konzernen auf Genehmigung des internationalen Datenverkehrs zu bearbeiten. Eine weitere Personalaufstockung ist daher dringend notwendig.

Auch die Struktur der Datenschutzkommission an sich, die im aktuellen Bericht 2007 der Datenschutzkommission von ihr selbst kritisiert wird, bei der die Mitglieder der Datenschutzkommission den österreichischen Datenschutz nach wie vor bloß als „Nebenjob“ betreiben, scheint nicht mehr zeitgemäß. Gerade internationale Konzerne kritisieren am Standort Österreich immer mehr, dass dieser bei den für große Konzerne essentiell notwendigen Datenverarbeitungsprojekten und IT-Reorganisationen immer mehr zum „Flaschenhals“ für ganz Europa wird, da aufgrund der Arbeitsweise der Datenschutzkommission (nur unregelmäßig alle paar Wochen oder Monate stattfindende Arbeitssitzungen) eine kontinuierliche und rasche Abarbeitung der meist sehr dringlichen Anliegen der Konzerne ebenso wenig möglich ist wie ein fruchtbringender regelmäßiger wechselseitiger Dialog mit den Mitgliedern der Datenschutzkommission, die ja ihre Agenden – bis auf das geschäftsführende Mitglied – alle nur als „Nebenjob“ ausführen. Bevor diese Situation zum wirklichen Schaden für den Wirtschaftsstandort Österreich wird, sollte daher dringend die Struktur der Österreichischen Datenschutzkommission grundlegend überdacht werden.

Einem Rechtsanwalt wurde bereits von einem Vorstand eines internationalen Konzerns angedroht, den österreichischen Standort schlicht aus datenschutzrechtlichen (!) Gründen zu schließen, wenn es nicht möglich sei, in Österreich vom Konzern geforderte und überall anders umsetzbare IT-Projekte datenschutzrechtlich in vertretbarer Zeit und mit vertretbarem Aufwand zu legalisieren. Die Schaffung hauptberuflich tätiger Mitglieder in einem permanent und nicht nur in sporadischen Sitzungen entscheidungsbefugten Gremium dürfte daher zur absoluten Notwendigkeit für den Wirtschaftsstandort Österreich im computerisierten 21. Jahrhundert werden.

Tuchlauben 12 | A-1010 Wien | Tel. +43 (1) 535 12 75 | Fax +43 (1) 535 12 75-13 | rechtsanwaelte@oerak.at | www.rechtsanwaelte.at

15. Verbesserter Zugang zum Datenschutzrecht

Da das Datenschutzrecht an sich eine sehr komplexe und „sperrige“ Rechtsmaterie ist, wird angeregt, § 6 über die Grundsätze des Datenschutzgesetzes so zu erweitern und umzuformulieren, dass dieser etwa nach dem Vorbild der „Eight Data Protection Principles“ im englischen Datenschutzgesetz (siehe www.ico.gov.uk) dem Datenschutzgesetz voran- oder nachgestellt werden kann. Damit hätten die Normadressaten einen schnellen und einfachen Zugang zu den wichtigsten Punkten und Prinzipien des österreichischen Datenschutzrechts.

16. Datenschutz-Gütesiegel

Im Schreiben des Bundeskanzleramtes vom 4. März 2008 wird ausdrücklich um Stellungnahme dazu ersucht, ob die Einführung eines „österreichischen Datenschutz-Gütesiegels“ für sinnvoll und zweckmäßig erachtet wird. Der Österreichische Rechtsanwaltskammertag erachtet ein solches Datenschutz-Gütesiegel für sinnvoll und zweckmäßig, ebenso wie verschiedenste Unternehmen, die im Vorfeld dieser Stellungnahme ein solches Gütesiegel für einen positiven Ansatz zur Selbstregulierung befunden haben. Eine Aufnahme desselben in den Entwurf wird daher angeregt, wobei auf das im Schreiben des Bundeskanzleramtes selbst zitierte Modell des European Privacy Seal als positives Beispiel hingewiesen wird.

17. Anpassung des Arbeitsverfassungsgesetzes

Der Österreichische Rechtsanwaltskammertag ersucht das Bundeskanzleramt überdies, bei den zuständigen Stellen anzuregen, dass begleitend zur Novellierung des Datenschutzgesetzes auch die Bestimmungen des Arbeitsverfassungsgesetzes, insbesondere dessen §§ 96 und 96a, novelliert werden. Aus der täglichen Beratung wissen die österreichischen Rechtsanwälte zu berichten, dass im Bereich der Verwendung von Mitarbeiterdaten und des Einsatzes von modernen Informationstechnologien im Betrieb (E-Mail, Internet, Internetapplikationen) äußerst große Rechtsunsicherheit sowohl auf Seiten der Arbeitgeber – als auch der Arbeitnehmervertretungen herrscht. Die Katalogisierung in §§ 96 und 96a Arbeitsverfassungsgesetz ist zu unpräzise und teilweise nicht mehr zeitgemäß, die bestehende Judikatur ist äußerst spärlich, zum Teil ebenfalls überholt oder im Ergebnis problematisch. Wichtige Bereiche, wie etwa die Überwachung des E-Mail- und Internetverkehrs, die Strukturierung und Auswertung von Mitarbeiterdaten in den verschiedensten Formen und zu den verschiedensten Zwecken, wie sie heute im Unternehmen an der Tagesordnung stehen, sind im Arbeitsverfassungsgesetz bis heute vollkommen ungeregelt. Siehe dazu auch *Brodil,* Geheimnisschutz – Informationsschutz – Datenschutz im Arbeitsrecht, in *Studiengesellschaft für Wirtschaft und Recht (Hrsg.),* Geheimnisschutz – Datenschutz – Informationsschutz (Linde 2007), 299, der anmerkt, dass „die Regelungen des Kollektivarbeitsrechts im Lichte moderner Technologien aus rechtspolitischer Sicht unvollständig erscheinen“, und weiters festhält, dass „aus rechtspolitischer Sicht eine nähere Determinierung

Tuchlauben 12 | A-1010 Wien | Tel. +43 (1) 535 12 75 | Fax +43 (1) 535 12 75-13 | rechtsanwaelte@oerak.at | www.rechtsanwaelte.at

von Vorschriften im Zusammenhang mit dem Geheimnis-, Informations- und Datenschutz im Arbeitsleben sinnvoll und angebracht erscheint“.

Wien, am 13. Mai 2008

DER ÖSTERREICHISCHE RECHTSANWALTSKAMMERTAG

Dr. Gerhard Benn-Ibler
Präsident

Tuchlauben 12 | A-1010 Wien | Tel. +43 (1) 535 12 75 | Fax +43 (1) 535 12 75-13 | rechtsanwaelte@oerak.at | www.rechtsanwaelte.at