Österreichischer Rechtsanwaltskammertag | Die österreichischen Rechtsanwälte

Bundeskanzleramt

Ballhausplatz 2
1014 Wien
v@bka.gv.at

Zl. 13/1 09/94

GZ 810.026/0005-V/3/2009
BG, mit dem das B-VG, das Datenschutzgesetz 2000 und das Sicherheitspolizeigesetz geändert werden (DSG-Novelle 2010)

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 fortgesetzte Initiative, das österreichische Datenschutzgesetz zu novellieren und ist erfreut über den Umfang, mit dem dieses Projekt weiter betrieben wird. Der Österreichische Rechtsanwaltskammertag erlaubt sich, zu nachstehenden Passagen der DSG-Novelle 2010 Stellung zu nehmen wie folgt:

1. Natürliche Personen

Der Österreichische Rechtsanwaltskammertag hat positiv zur Kenntnis genommen, dass der im letztjährigen Entwurf einer DSG-Novelle 2008 enthaltene Vorschlag, den Grundrechtsschutz auf natürliche Personen einzuschränken, im Entwurf der DSG-Novelle 2010 nun wieder fallengelassen wurde, was der letztjährigen Forderung des Österreichischen Rechtsanwaltskammertages entspricht.

2. Präzisierung der Definition „Zustimmung“

Bereits zum Entwurf der DSG-Novelle 2008 hat der Österreichische Rechtsanwaltskammertag zu § 4 DSG 2000 angeregt, die Definition der datenschutzrechtlichen Zustimmung so zu präzisieren, dass bislang bestehende Rechtsunsicherheiten beseitigt werden, was mit dem Entwurf der Novelle 2010 durchgeführt werden könnte:

In einem – mittlerweile 24 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 zehn 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.

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.

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

3. 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.

4. Betrieblicher Datenschutzbeauftragter

Der Österreichische Rechtsanwaltskammertag stellt mit Erstaunen fest, dass der sehr begrüßenswerte Vorschlag des Entwurfes der DSG-Novelle 2008, im österreichische Datenschutzgesetz so wie in Deutschland den betrieblichen Datenschutzbeauftragten einzuführen, im Entwurf der Novelle des DSG 2010 nicht mehr enthalten ist. Der betriebliche Datenschutzbeauftragte würde die Befassung mit datenschutzrechtlichen Fragen fördern und Unternehmen motivieren, sich mehr mit der betrieblichen Datensicherheit und der Ausgestaltung der Unternehmens-EDV zu befassen, die heutzutage unabdingbare Themen für den Fortbestand der Unternehmen sind. Wie sich aus Gesprächen bei der heurigen Frühjahrstagung der Österreichischen Juristenkommission in Weissenbach am Attersee im Mai 2009 ergeben hat, ist der Vorschlag des betrieblichen Datenschutzbeauftragten offensichtlich aus rein politischen Gründen, nicht jedoch aus materiell-datenschutzrechtlichen Gründen – solche würden nämlich für diesen sprechen – wieder aus dem Entwurf der DSG-Novelle gestrichen worden. Der Österreichische Rechtsanwaltskammertag spricht sich für die Wiederaufnahme des Vorschlags, den betrieblichen Datenschutzbeauftragten im DSG zu verankern aus.

5. 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 die Identifizierung und Authentifizierung im elektronischen Meldeverfahren laut § 17 Abs 1a des Entwurfes wurde vom Österreichischen Rechtsanwaltskammertag bereits zum Entwurf 2008 mitgeteilt, dass seitens der Unternehmerschaft eine sehr deutliche Ablehnung der Bürgerkarte für diese Funktion besteht. Dies deshalb, weil es sich, wie der Name schon sagt, bei dieser um eine „Bürger“-Karte handelt, nicht jedoch um eine „Unternehmens“-Karte und es daher fraglich ist, ob ein Unternehmen seine Mitarbeiter dazu „zwingen“ kann, deren „private“ Bürgerkarte – etwa deren e-Card mit Bürgerkartenfunktion – für betriebliche Zwecke zum Einsatz zu bringen. Auch ist unklar, wie die Verbindung zwischen Mitarbeiter und Unternehmen im Hinblick auf

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

die Kontrolle der „Zeichnungsberechtigung“ bzw „Signaturberechtigung“ hergestellt wird. Auch falls der Mitarbeiter nicht mehr im Unternehmen beschäftigt ist, kann zwar eventuell der Zugang hinsichtlich seiner Person gesperrt werden, der eigentliche Schlüssel, die Karte, ist aber im Eigentum des Mitarbeiters (Bürgers) und kann daher nicht einfach eingezogen werden. Der Österreichische Rechtsanwaltskammertag ist erfreut, dass seiner damaligen Stellungnahme insofern Rechnung getragen wurde, als im nunmehrigen Entwurf in § 17 Abs 1a die Bürgerkarte nur mehr als “insbesondere“ angeführt wird. In der dort vorgesehenen Verordnung sollte in der Folge darauf geachtet werden, dass es tatsächlich alternative Identifizierungs- und Authentifizierungsmöglichkeiten zur Bürgerkarte gibt.

6. Prüfungs- und Verbesserungsverfahren (§ 20)

Beim Studium des neu formulierten § 20 steht zu befürchten, dass sich dem durchschnittlich versierten Leser der Unterschied zwischen einer „Fehlerhaftigkeit“ im Sinne des § 20 Abs 1 und dem dadurch ausgelösten Verfahren nach § 20 Abs 2 und einer „Mangelhaftigkeit“ im Sinne des § 20 Abs 3 und dem dadurch nach § 20 Abs 4 ausgelösten Verfahren nicht erschließt. Insbesondere steht zu befürchten, dass dem Leser auch nicht ganz ersichtlich ist, was die Konsequenzen einer vorab kontrollpflichtigen Meldung in der praktischen Durchführung des Prüfungsverfahren sein werden. Es wird angeregt, diese Bestimmung allenfalls zu vereinfachen.

Zu § 20 und 21 des Entwurfes geht der Österreichische Rechtsanwaltskammertag davon aus, dass es auch künftig möglich sein wird, gesetzte Verbesserungsfristen mittels Antrag des meldenden Auftraggebers zu verlängern; sollte dies nicht so angedacht sein, schlägt der Österreichische Rechtsanwaltskammertag eine diesbezügliche explizite Möglichkeit zur Fristverlängerung vor.

7. Richtigstellung des Registers und Rechtsnachfolge

Zu § 22 erlaubt sich der Österreichische Rechtsanwaltskammertag die Anmerkung, dass bei der praktischen Umsetzung dieses Paragraphen darauf geachtet werden sollte, dass sämtliche rechtlichen Vorgaben in der EDV des DVR richtig umgesetzt werden können. Wie sich aus der Praxis der vergangenen Jahre gezeigt hat, ist es durch die mehrfache Systemumstellung im Datenverarbeitungsregister immer schwieriger geworden, rasch zu einem aktuelle und richtigen Registerstand zu gelangen. Besonders nach der letzten Systemumstellung Anfang 2009 ist technisch anscheinend nicht mehr sichergestellt, dass ein sachlich richtiger Registerstand vom EDV-System des Datenverarbeitungsregisters automatisch korrekt ausgegeben wird und erst durch sehr zeitaufwändiges, händisches Nachbearbeiten durch Sachbearbeiter des DVR der korrekte Registerstand sichergestellt werden kann. Allfällige weitere Systemanpassungen und Umstellungen sollten daher nur dann vorgenommen werden, wenn zunächst gesichert ist, dass das Register derzeit korrekte Ergebnisse liefert und dies auch künftig tun wird, wobei bei allfälligen EDV-Projekten ausreichend Personal und Budgetmittel seitens des Bundes zur Verfügung gestellt werden müssen, um weitere Unzulänglichkeiten der EDV des Datenverarbeitungsregisters hintanzuhalten.

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

8. Verfahren zur Überprüfung der Erfüllung der Meldepflicht

Der Österreichische Rechtsanwaltskammertag begrüßt die Klarstellung und Stärkung der Position der Datenschutzkommission bei der selbständigen Überprüfung und Erfüllung der Meldepflicht in § 22 a des Entwurfes, erlaubt sich jedoch anzumerken, dass der Datenschutzkommission auch entsprechende Personalressourcen zur Verfügung gestellt werden müssen, damit diese – wie in allen anderen Ländern der Europäischen Union üblich – auch selbstständige „Stichprobenkontrollen“ durchführen kann. Bei der derzeitigen Personalausstattung der Datenschutzkommission scheint dies unmöglich, womit zu befürchten steht, dass insbesondere § 22 a Abs 1 des Entwurfes zu einer bloßen „Scheinregelung“ verkommt, die in der Praxis nicht umsetzbar ist. Gerade aufgrund der in Österreich vollkommen fehlenden Stichprobenkontrolle hat sich Österreich über die letzten zwei Jahrzehnte vom einstigen „Musterschüler“ im Datenschutzrecht zu einem der Schlusslichter in Sachen Einhaltung der Datenschutznormen entwickelt; die Stichprobenkontrolle gehört in den anderen Staaten der Europäischen Union als Selbstverständlichkeit zum Tätigkeitsfeld der Datenschutzkommission (siehe dazu etwa die einzelnen Länderberichte im 11. Jahresbericht der Art. 29 Datenschutzgruppe), um mögliche „schwarze Schafe“ dem stärkeren Risiko auszusetzen, bei einer derartigen Stichprobenkontrolle entdeckt zu werden.

9. Informationspflicht des Auftraggebers bei Datenschutzverstößen

Der Österreichische Rechtsanwaltskammertag nimmt erfreut zur Kenntnis, dass dem internationalen Trend zu Schaffung sogenannter „Data Breach Notification Laws“ in § 24 Abs 2 a der Novelle eine Informationspflicht des Auftraggebers bei Datenschutzverstößen eingeführt werden soll. Zu begrüßen wäre dabei, die dortige Wortfolge „systematisch und schwerwiegend unrechtmäßig verwendet wurden“ näher zu präzisieren, um damit Rechtssicherheit bei der Anwendung dieser Bestimmung zu schaffen. Zu überlegen wäre auch, diese Bestimmung dahingehend zu präzisieren, dass insbesondere dann, wenn den Betroffenen ein Schaden droht und durch die Information der Schaden abgewendet werden könnte, eine solche Informationspflicht jedenfalls besteht. Fraglich ist auch, ob diese Informationspflicht ihre Wirkung entfalten wird, wenn diese keinerlei Sanktion bei Nichterfüllung unterliegt, was nach dem vorliegenden Entwurf der Fall ist. Der internationale Trend sieht für die Nichtbefolgung der Informationspflichten klare rechtliche Konsequenzen vor, die hier leider vollkommen fehlen und daher Rechtsunsicherheit – insbesondere auch im Hinblick auf mögliche verschärfte Haftung aus nicht erfolgter Schadensminimierung nach allgemeinem Zivilrecht aufwirft.

10. Aufrundung von Eurobeträgen

Der Österreichische Rechtsanwaltskammertag schlägt vor, sämtliche im DSG vorkommenden Eurobeträge, die noch immer nach Kommastellen genau aus dem Schilling umgerechnet sind, auf runde Eurobeträge aufzurunden.

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. Widerspruchsrecht im Hinblick auf Bonitätsdaten

Mit Verwunderung nimmt der Österreichische Rechtsanwaltskammertag zur Kenntnis, dass zu § 28 Abs 1 und 2 nicht wie erwartet eine „Sanierung“ der derzeit aufgrund des OGH-Urteiles OGH 6 Ob 195/08g vom 1.10.2008 bestehenden Möglichkeit einer völlig widerspruchslosen Löschung von Bonitätsdaten durch die Betroffenen aus Bonitätsdatenbanken, obwohl diese einer Interessensabwägung zu unterwerfen sind (siehe dazu *Knyrim*, Widerspruch gegen die Datenverarbeitung in Wirtschaftsauskunfteien?, ecolex 2008, 1060), erfolgt. Der Österreichische Rechtsanwaltskammertag geht davon aus, dass falls eine derartige Sanierung nicht im Datenschutzgesetz erfolgt, diese in § 152 GewO ehestmöglich vorgenommen wird.

12. 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, die Anzeiger 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

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

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.

13. 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.“

14. Beschwerde an die Datenschutzkommission

Der Österreichische Rechtsanwaltskammertag erlaubt sich anzuregen, die in § 31 Abs 3 Z 6 bei einer Beschwerdeeinbringung vorgesehenen Angabe zur Rechtzeitigkeit der Beschwerdeeinbringung dahingehend zu überprüfen, ob diese zur Verwirrung bei den Beschwerdeführern führt. Bei den nach dem DSG typischen Beschwerden auf Auskunft, Widerspruch, Richtigstellung oder Löschung laufen jeweils keine Fristen, die eine Rechtzeitigkeit der Beschwerde fraglich machen, da jeweils von einem tagesaktuellen Ist-Datenbestand oder einem vermuteten Ist-Datenbestand ausgegangen wird, der beauskunftet und verändert werden soll.

15. Ineinandergreifen von Zivilgerichts- und Verwaltungsverfahren

Der Österreichische Rechtsanwaltskammertag regt an, in § 32 Abs 7 des Entwurfes klarzustellen, dass das Gericht die Datenschutzkommission nur dann um Überprüfung ersuchen muss, wenn sich die Klage auf eine meldepflichtige Datenanwendung bezieht, die derzeit offensichtlich noch nicht gemeldet ist. Nach dem Wortlaut der derzeitigen Formulierung könnte diese auch so verstanden werden, dass, auch wenn eine Datenanwendung bereits gemeldet ist, wenn sich die Klage auf eine solche bezieht, das Gericht die Datenschutzkommission um Überprüfung ersuchen muss (selbst wenn die Datenanwendung an sich nicht strittig ist sondern zB nur ein Datensatz in dieser richtiggestellt werden soll).

Weiters regt der Österreichische Rechtsanwaltskammertag an, eine Frist für die Mitteilung des Ergebnisses der Überprüfung durch die Datenschutzkommission an das Gericht festzusetzen um die zeitliche Verzögerung im Zivilprozess kalkulierbar zu machen.

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

16. Ausstattung der Datenschutzkommission; Berichtspflicht der Datenschutzkommission

Zu § 38 Abs 2 des Entwurfes wird festgehalten, dass der 1. Satz der Regelung, der auch bislang schon bestand, vom Bundeskanzler endlich so umgesetzt werden sollte und der Datenschutzkommission tatsächlich die notwendige Personalausstattung bereitgestellt werden sollte.

Zum im Entwurf neu vorgeschlagenen Recht des Bundeskanzlers, sich jederzeit über alle Gegenstände der Geschäftsführung der Datenschutzkommission beim Vorsitzenden und dem geschäftsführenden Mitglied zu unterrichten, äußert der Österreichische Rechtsanwaltskammertag erhebliche Bedenken: Ein solches Unterrichtsrecht verläuft auf einen Rechtfertigungsdruck und letztlich auf eine indirekte Abhängigkeit der Datenschutzkommission vom Bundeskanzler hinaus, was sich diametral zum Vertragsverletzungsverfahren der Europäischen Union gegen Österreich im Hinblick auf die Unabhängigkeit der Datenschutzkommission verhält. Der Österreichische Rechtsanwaltskammertag spricht sich klar für eine vollständig unabhängige Datenschutzkommission aus; eine solche darf selbst durch ein „Unterrichtungsrecht“ des Bundeskanzleramtes in ihrer Unabhängigkeit auch nur im Ansatz eingeschränkt werden.

Sehr bedenklich ist in diesem Zusammenhang, dass die erläuternden Bemerkungen zu dieser Bestimmung festhalten, dass diese Regelung lediglich die bisherige Praxis gesetzlich festschreibe. Dies bestätigt die nicht nur seitens der EU-Kommission, sondern verschiedenster österreichischer Institution seit Längerem vorgetragene Beschwerde, dass die Datenschutzkommission nicht vollständig unabhängig, sondern zu sehr in den Geschäftsbetrieb des Bundeskanzleramtes eingegliedert sei. Eine vollständig unabhängige Datenschutzkommission sollte – wie in den anderen Mitgliedstaaten der Europäischen Union – eine Selbstverständlichkeit sein.

17. „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.

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

18. Videoüberwachung

Zu § 50 a Abs 4 wird vorgeschlagen, „öffentliche“ Eingriffe unter einen ähnlichen generellen Eingriffsvorbehalt zu stellen, wie er in § 1 Abs 2 formuliert ist.

Zu § 50 a Abs 6 wäre zu überdenken, ob durch diese Bestimmung nicht die Vorlage unzulässigerweise durch Grundrechtsverletzungen erlangte Videobeweismittel gefördert bzw deren Vorlage bei Gerichten und Sicherheitsbehörden begünstigt wird.

Zu § 50 b Abs 2 wird vorgeschlagen, die grundsätzlich zulässige Speicherdauer auf 72 Stunden als Normdauer auszudehnen. Andernfalls müssten Aufzeichnungen von Einbrüchen oder Diebstählen in videoüberwachten Unternehmen, die am Freitag Abend nach Dienstschluss begangen werden, bereits am Sonntag Abend automatisch gelöscht werden, was den Zweck einer solchen betrieblichen Überwachung zum Eigentumsschutz konterkarieren würde. Somit müsste in jedem Fall einer Videoüberwachung zum Eigentumsschutz extra ein Antrag gestellt werden, die Speicherdauer zu verlängern.

Schon zum Entwurf der Novelle 2008 wurde seitens des Österreichischen Rechtsanwaltskammertages zu § 50 c Abs 2 Z 2 festgestellt, dass der dogmatisch-juristische Hintergrund für die Ausnahme analoger Speichermedien in dieser Bestimmung kaum nachvollziehbar ist. Schon damals haben Gespräche mit verschiedenen Unternehmen und Einzelpersonen ergeben, dass dies ein Aufruf zu einem technologischen Rückschritt zur Umgehung von Datenschutzbestimmungen ist, da diesfalls einfach an Stelle eines Festplattenspeichermediums in einem Computer auf einem alten VHS-Videorekorder zurückgegriffen werden könnte, um die Regelungen hinsichtlich Videoaufzeichnung der DSG-Novelle auszuheben. Dementsprechend wird die Streichung der Ausnahme analoger Speichermedien von der Meldepflicht angeregt. Dies insbesondere auch im Hinblick darauf, dass nach dem Entwurf künftig auch manuelle Dateien künftig dem Datenschutzgesetz und zumindest in Teilbereichen auch einer Meldepflicht unterliegen sollen.

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

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

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.

19. In-Kraft-Treten

Zu den In-Kraft-Treten-Bestimmungen des § 60 wird vorgeschlagen, das In-Kraft-Treten auf den 30.6.2010 zu verschieben, um den Unternehmen eine ausreichende Informations- und Reaktionsfrist auf die neuen Bestimmungen zu ermöglichen, damit einer Beschlussfassung der Novelle und Publikation derselben nicht vor Spätherbst 2009 zu rechnen ist, also äußerst knapp vor dem derzeit vorgesehenen Inkrafttreten zum Jahreswechsel.

20. 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 gegenüber Mitgliedern des Österreichischen Rechtsanwaltskammertages 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 Rechtsanwälten vielfach bekannt ist, regelmäßig auch an Sonn- und Feiertagen arbeiten, ist es nicht möglich, mit einer „Handvoll" Mitarbeitern gleichzeitig die

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

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.

Zur Illustration darf angeführt werden, dass einem Rechtsanwalt bereits von einem Vorstand eines internationalen Konzerns angedroht wurde, 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.

21. 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.

22. Datenschutz-Gütesiegel

Im Schreiben des Bundeskanzleramtes vom 14. März 2008 zum Entwurf der Novelle 2008 wurde ausdrücklich um Stellungnahme dazu ersucht, ob die Einführung eines „österreichischen Datenschutz-Gütesiegels" für sinnvoll und zweckmäßig erachtet wird. Der Österreichische Rechtsanwaltskammertag erachtet ein solches

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

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.

23. Anpassung des Arbeitsverfassungsgesetzes; Arbeitnehmerdatenschutzgesetz

Bereits in der Stellungnahme zum Entwurf der Novelle 2008 hat der Österreichische Rechtsanwaltskammertag das Bundeskanzleramt ersucht, bei den zuständigen Stellen anzuregen, dass begleitet zur Novellierung des Datenschutzgesetzes auch die Bestimmung eines Arbeitsverfassungsgesetzes, insbesondere dessen § 96 und § 96 a novelliert werden. In Gesprächen auf der Frühjahrstagung der Österreichischen Juristenkommission in Weissenbach am Attersee im Mai 2009 zeigte sich, dass tatsächlich angedacht ist, dass eine solche Novellierung unter den Titel „Arbeitnehmerdatenschutzgesetz“ vorzunehmen. Der Österreichische Rechtsanwaltskammertag unterstützt dieses Vorhaben zur Schaffung von Rechtssicherheit und fordert eine möglichst rasche Erstellung eines derartigen „Arbeitnehmerdatenschutzgesetzes“. Dies, da aus der täglichen Beratung Rechtsanwälte zu berichten wissen, 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 Arbeitnehmervertretung 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 von Vorschriften im Zusammenhang mit dem Geheimnis-, Informations- und Datenschutz im Arbeitsleben sinnvoll und angebracht erscheint“.

Wien, am 16. Juni 2009

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