Secur-Data Betriebsberatungsges.m.b.H.
1010 Wien, Fischerstiege 9 Tel. (01) 533 42 07-0
Internet: www.secur-data.at E-Mail: office@secur-data.at

DSG-Info-Service

April 2008 Ausgabe Nr. 55/56/57

Sehr geehrter DSG-Paket-Kunde!
Sehr geehrter Leser!

Etwas überraschend und offensichtlich ohne vorherige Konsultation des Koalitionspartners oder des Datenschutzrates wurde am 11. April 2008 vom Bundeskanzleramt ein Begutachtungsentwurf für eine Novelle des Datenschutzgesetzes veröffentlicht. Die Begutachtungsfrist läuft bis zum 21. Mai 2008.

Der komplette Entwurf ist am besten über die Internetseite des Nationalrats nachzulesen. In dieser Ausgabe unseres DSG-Info-Service stellen wir die wesentlichen Neuerungen des Entwurfs vor und vor allem die wahrscheinlichen Diskussionspunkte sowie einige Schwachstellen aus unserer Sicht.

Wegen des Umfangs der Ausführungen, die wir aus Aktualitätsgründen nicht weiter kürzen wollen, haben Sie die erste Dreifachausgabe unseres DSG-Info in Händen.

Ministerialentwurf der DSG-Novelle 2008

Im Internet vollinhaltlich nachzulesen unter
http://www.parlinkom.gv.at/PG/DE/XXIII/ME/ME_00182/pmh.shtml

Presseaussagen

Frau Staatssekretärin Heidrun Silhavy hat auf ihrer Pressekonferenz bzw. in ihren Pressemitteilungen auf der Internetseite des Bundeskanzleramts die Novelle präsentiert. Wir zitieren auszugsweise aus ihren Aussagen, die Hervorhebungen wurden von uns angebracht:

*Zurzeit bestehen beim Einsatz von **Videoüberwachungen** durch Private, egal ob es sich um Hauseingänge, Geschäftslokale, Banken, Bahnhöfe oder U-Bahnen handelt, keine ausdrücklichen gesetzlichen Vorschriften. Genehmigungen werden im Einzelfall durch die Datenschutzkommission erteilt. Wir setzen uns nunmehr für eine eindeutige gesetzliche Regelung ein, wann*

der Einsatz von Videoüberwachung durch Private zulässig ist.

Die Novelle sieht weiters die Installierung eines ***betrieblichen Datenschutzbeauftragten*** *vor. Die jüngst bekannt gewordene Überwachung von Mitarbeiterinnen und Mitarbeiter eines deutschen Lebensmitteldiskonter zeigt, dass gesetzliche Regelungen in diesem Bereich unerlässlich sind. Um einen derartigen Missbrauch zu unterbinden soll in Betrieben mit mindestens 20 Bediensteten ein betrieblicher Datenschutzbeauftragter bestellt werden, der die Funktion eines Arbeitnehmervertreters hat. Gemeinsam mit dem Betriebsinhaber hat er für die Einhaltung der datenschutzrechtlichen Bestimmungen im Betrieb zu sorgen und ist vom Betriebsinhaber über neue Datenanwendungen rechtzeitig in Kenntnis zu setzen.*

Dem Datenschutzbeauftragten kommt dabei eine ähnliche Rolle wie einer Sicherheitsvertrauensperson zu. Mit dieser Regelung erfüllen wir eine langjährige Forderung der Gewerkschaften.

[**Anmerkung:** dem Gesetzesentwurf ist allerdings nicht zu entnehmen, dass diese Funktion in einer Rolle als Arbeitnehmervertreter wahrzunehmen ist.]

Weiters sieht die Novelle eine ***einheitliche Zuständigkeit des Bundes für Datenschutzangelegenheiten*** *vor. Derzeit existieren Datenschutzgesetze des Bundes und der Länder parallel nebeneinander. Um ein einheitliches Datenschutzniveau zu garantieren, wird nun eine einheitliche Zuständigkeit des Bundes vorgeschlagen.*

Kernpunkte des Novellierungsentwurfs

Drei Kernaussagen des Gesetzesentwurfs sind schon dem Pressematerial zu entnehmen:

- Bundeskompetenz für den gesamten Datenschutz, also auch für manuellen Datenanwendungen in Landeskompetenz;
- Einrichtung eines betrieblichen Datenschutzbeauftragten in Betrieben ab 20 Mitarbeitern;
- Regelungen für die Videoüberwachung.

Andere und mindestens ebenso gravierende Änderungen wurden in der Pressemitteilung nicht erwähnt:

- Auflassung des Datenschutzes für juristische Personen und Personengemeinschaften;
- Vereinfachung des Registrierungsverfahrens durch Selbstregistrierung in einer Datenbank;
- Datenschutzrechtliche Gleichstellung der Vertragsstaaten des Europäischen Wirtschaftsraums (EWR) anstatt bisher nur der EU.

§ 1 Grundrecht auf Datenschutz (Verfassungsbestimmung)

Abweichend vom derzeitigen Gesetzeswortlaut soll der Datenschutz nur mehr für natürliche Personen verfassungsmäßig garantiert sein.

Daraus ergeben sich für **juristische Personen** weitestgehende Konsequenzen dadurch, dass ihnen Rechte wie

- Auskunftsrecht

- Richtigstellungsrecht
- Löschungsrecht
- Widerspruchsrecht

ersatzlos genommen werden.

Dadurch können einerseits geschäftsschädigende Falschaussagen nicht mit den Mitteln des Datenschutzes bekämpft werden, andererseits ergibt sich der kuriose Effekt, dass ein Unternehmen seine Kundendaten anders schützen muss, je nachdem, ob der Kunde eine juristische Person oder eine natürliche Person ist. Im Telekommunikationsgesetz (TKG 2003) wurde mit der Novelle 2005 eine vergleichbare Ungleichbehandlung eliminiert (Stichwort: unerbetene elektronische Nachrichten, § 107), nun entsteht sie im Datenschutzbereich von neuem.

Im Übrigen ist das TKG nur eines von vielen Gesetzen, die nur rudimentäre Datenschutzbestimmungen enthalten und darüber hinaus ausdrücklich auf das DSG 2000 verweisen. So verweist zB das TKG in § 96 Abs. 2 auf das Auskunftsrecht gem. DSG, das ein Teilnehmer („eine natürliche oder juristische Person, die mit einem Betreiber einen Vertrag über die Bereitstellung dieser Dienste geschlossen hat") gegenüber dem Anbieter hat. Somit widersprechen einander dann zwei Gesetze.

Im Übrigen enthält der § 1 einige sprachliche Verbesserungen, die zu begrüßen sind.

§ 2 Zuständigkeit (Verfassungsbestimmung)

Der Wechsel der Zuständigkeit für den gesamten Datenschutz zum Bund ist zu begrüßen. Bisher bestand bekanntlich die merkwürdige Konstellation, dass für manche manuelle Datenanwendungen die Zuständigkeit der Länder (mit ihren 9 Landes-Datenschutzgesetzen) bestand, wobei die Länder versucht haben, Teile dieser Zuständigkeit per Landesgesetz wieder der Datenschutzkommission zu übertragen.

§ 3 Räumlicher Anwendungsbereich (Verfassungsbestimmung)

Bei der Notwendigkeit einer Abgrenzung des Geltungsbereichs zwischen dem österreichischen DSG und einem ausländischen Datenschutzgesetz wird nunmehr auf das Recht des Sitzstaates im gesamten EWR und nicht nur in der EU Rücksicht genommen.

An dieser Stelle ist anzumerken, dass auch der Datenverkehr in den gesamten EWR genehmigungsfrei wird (siehe § 12).

§ 4 Definitionen und Regelungsgegenstand

Abgesehen vom Wegfall der juristischen Personen als „Betroffene" sind begrüßenswerte sprachliche Verbesserungen zu vermerken.

Neu ist aber ein 2. Absatz mit folgendem Wortlaut:

> *Die Regelungen des 2., 3., 5. und 8. Abschnitts dieses Bundesgesetzes gelten mit Ausnahme von § 6 Abs. 1 sowie § 7 Abs. 2 und 3 in Verbindung mit den §§ 8 und 9 nur für Daten, die einer Datenanwendung unterzogen oder in einer Datei verwendet werden. Der 4. Abschnitt gilt für Datenanwendungen und Dateien mit der*

Maßgabe, dass für ohne Automationsunterstützung geführte Dateien Meldepflicht nur besteht, wenn sie ihrem Inhalt nach gemäß § 18 Abs. 2 der Vorabkontrollpflicht unterliegen. Die Meldung solcher Dateien kann abweichend von § 17 Abs. 1a auch in nichtelektronischer Form erfolgen. Überall dort, wo in diesen Abschnitten bloß von Datenanwendungen die Rede ist, sind die Regelungen auf Dateien sinngemäß anzuwenden, es sei denn es ist ausdrücklich anderes bestimmt. Wo im 6. Abschnitt von Datenanwendungen die Rede ist, gelten die Bestimmungen sinngemäß für alle Daten. Der 9. und 9a. Abschnitt gilt nur für Datenanwendungen.

Haben Sie verstanden, worum es geht?

- Teile des DSG gelten für Daten aller Art,
- Teile nur für Dateien,
- Teile nur für Datenanwendungen,
- Teile nur bei Automationsunterstützung,
- Teile nur bei manuellen Datenanwendungen.

Eine verständliche Neuformulierung ist dringend erforderlich.

§ 8 und 9 Schutzwürdige Geheimhaltungsinteressen

Zu den bisher geltenden Regelungen treten zwei neue Umstände hinzu, die die Datenweitergabe erlauben:

- *„Unterstützung des Nationalrates, des Bundesrates oder eines Landtages bei der Ausübung parlamentarischer Kontrolltätigkeit nach Art. 52 bis 53 B–VG oder entsprechenden landesverfassungsrechtlichen Bestimmungen“*
- *„Datenweitergabe zum Zweck der Erstattung einer Anzeige an eine zur Verfolgung der strafbaren Handlungen (Unterlassungen) oder zumindest zur Entgegennahme derartiger Anzeigen zuständige Behörde“*

Damit werden einerseits parlamentarische Kontrollrechte erleichtert, andererseits können Strafanzeigen von vornherein mit Daten untermauert werden, sodass nicht auf einen Beschluss des Gerichts gewartet werden muss.

Auffällig ist nur, dass zwar die parlamentarische Kontrolle auch bei sensiblen Daten erlaubt sein soll, die Strafanzeige hingegen nicht. Das erscheint unausgewogen.

§ 15a Betrieblicher Datenschutzbeauftragter

Wir drucken diese Neueinführung im vollen Wortlaut ab:

§ 15a. (1) *Der Inhaber eines Betriebes (§ 34 Abs. 1 des Arbeitsverfassungsgesetzes – ArbVG, BGBl Nr. 22/1974, § 4 Abs. 1 des Post-Betriebsverfassungsgesetzes – PBVG, BGBl I Nr. 326/1996, § 5 Abs. 1 des Landarbeitsgesetzes 1984 – LAG, BGBl. Nr. 287/1984) mit mehr als 20 Mitarbeitern (wobei Mitarbeiter, die nicht zumindest 20 Stunden pro Woche im Betrieb tätig sind, außer Betracht bleiben) hat einen geeigneten Mitarbeiter zum betrieblichen Datenschutzbeauftragten zu bestellen.*

(2) *Der Inhaber hat mit dem Betriebsrat, wenn ein Betriebsausschuss errichtet ist, mit*

diesem, die beabsichtigte Bestellung oder Abberufung des Datenschutzbeauftragten zu beraten. Eine ohne Beratung vorgenommene Bestellung ist rechtsunwirksam. Die Bestellung bedarf auch der zivilrechtlichen Zustimmung des bestellten Mitarbeiters. Stimmt kein geeigneter Mitarbeiter der Bestellung zu, ist eine geeignete betriebsfremde Person oder ein geeignetes Unternehmen zu bestellen.

***(3)** Der betriebliche Datenschutzbeauftragte hat die Einhaltung der Vorschriften dieses Bundesgesetzes im Betrieb zu überwachen und den Betriebsinhaber, die Arbeitnehmer und den Betriebsrat in Belangen des Datenschutzes zu beraten. Er ist vom Inhaber über Vorhaben, neue Datenanwendungen einzusetzen, rechtzeitig zu unterrichten. Wird ihm ein Verdacht einer Verletzung datenschutzrechtlicher Vorschriften bekannt, hat er auf die Herstellung eines rechtmäßigen Zustandes hinzuwirken. Ist ihm dies aus Eigenem nicht möglich, hat er den Betriebsinhaber von dem Verdacht in Kenntnis zu setzen.*

***(4)** Für Beratungen durch den Datenschutzbeauftragten nach Abs. 3 hat der Inhaber Mitarbeitern, die mit der Verwendung von Daten betraut sind, im ersten Dienstjahr Arbeitszeit im Umfang von zumindest acht Stunden, in folgenden Dienstjahren im Ausmaß von zumindest vier Stunden pro Jahr zur Verfügung zu stellen. Dem betrieblichen Datenschutzbeauftragten selbst sind im ersten Jahr seiner ununterbrochenen Tätigkeit zumindest 40 Stunden und in jedem folgenden Jahr zumindest 20 Stunden an Arbeitszeit zum Erwerb von Fachkenntnissen und zur Weiterbildung auf dem Gebiet des Datenschutzes zur Verfügung zu stellen.*

***(5)** Der betriebliche Datenschutzbeauftragte ist in Ausübung dieser Funktion nicht an Weisungen gebunden. Er hat aber datenschutzbezogene Anregungen des Betriebsinhabers dennoch entgegenzunehmen und gegebenenfalls zu begründen, warum er diese nicht unterstützt. Im Hinblick auf den Kündigungs- und Entlassungsschutz ist der betriebliche Datenschutzbeauftragte einer Sicherheitsfachkraft (§ 73 Abs. 1 des ArbeitnehmerInnenschutzgesetzes, BGBl Nr. 450/1994) gleichgestellt.*

***(6)** Die Bestellung des betrieblichen Datenschutzbeauftragten lässt die Verantwortung des Betriebsinhabers für die Einhaltung der Bestimmungen dieses Bundesgesetzes unberührt.*

Abgesehen von dem Umstand, dass manches für und manches gegen den betrieblichen Datenschutzbeauftragten spricht, seien dazu folgende Anmerkungen erlaubt:

- Die Grenze von 20 Mitarbeitern ist wohl zu niedrig angesetzt.
- Bei Klein- und Mittelbetrieben wird in der Regel kein geeigneter Mitarbeiter vorhanden sein, sodass meistens die Auslagerung an einen externen Datenschutzbeauftragten erforderlich wird.
- In den Vorbemerkungen zum Gesetzesentwurf werden die Zusatzkosten für den betrieblichen Datenschutzbeauftragten dahingehend erläutert, dass nunmehr als Zusatzaufwand der Name des Datenschutzbeauftragten dem DVR mitgeteilt werden muss; also dürfte dem Planer des Gesetzesentwurfs der Blick für die betriebliche Praxis fehlen.

- Neben Betriebsrat und Sicherheitsfachkraft genießt nunmehr auch der betriebliche Datenschutzbeauftragte besonderen Kündigungs- und Entlassungsschutz.
- Trotz Bestellung eines betrieblichen Datenschutzbeauftragten haftet der Betriebsinhaber bei eventuellen Verstößen gegen die Bestimmungen des Datenschutzgesetzes.

Der Betriebsbegriff in § 34 ArbVG ist wie folgt definiert: *„Als Betrieb gilt jede Arbeitsstätte, die eine organisatorische Einheit bildet, innerhalb der eine physische oder juristische Person oder eine Personengemeinschaft mit technischen oder immateriellen Mitteln die Erzielung bestimmter Arbeitsergebnisse fortgesetzt verfolgt, ohne Rücksicht darauf, ob Erwerbsabsicht besteht oder nicht"*.

Mit dieser Definition ist es nun der Diskussion Tür und Tor geöffnet, ob ein Unternehmen mit vielen Betriebsstätten auch entsprechend viele betriebliche Datenschutzbeauftragte benötigt. Dabei bleibt völlig außer Acht, dass ein Betrieb ohne Datenanwendungen und ohne Dateien ganz offenkundig aus allen einfachgesetzlichen Regelungen des DSG herausfällt und daher keinesfalls einen Datenschutzbeauftragten bestellen muss.

Ein spezielles Kuriosum ergibt sich im Zusammenhang mit den weiter unten erläuterten Meldevorschriften. Bei der Meldung einer Datenanwendung ist die Person des Datenschutzbeauftragten zu benennen. Da die Meldepflicht aber den Auftraggeber betrifft (in der Regel ist das das Unternehmen als juristische Person), der Datenschutzbeauftragte aber vom Betrieb bestellt wird (da kann es mehrere in einem Unternehmen geben), wäre zu vermuten, dass eine Datenanwendung mehrfach zu melden ist. Ist dann die Anwendung des Unternehmens das Informationsverbundsystem der Anwendungen der Betriebe?

Im Übrigen würde die Neubesetzung eines Datenschutzbeauftragten auch eine Änderungsmeldung für sämtliche gemeldete Datenanwendungen nach sich ziehen.

§§ 16 bis 22
Bestimmungen rund um das DVR

Das DVR wird in Form einer Internetanwendung geführt, in die vom Auftraggeber die Meldungen direkt eingetragen werden sollen. Abweichend zum status quo, wo das DVR praktisch jede beliebige E-Mail-Meldung akzeptiert hat, wird eine Identifizierung des Einreichers mit der Bürgerkarte gefordert.

Bei einer Anwendung, die im Regelfall ja nicht der Vorabkontrolle unterliegen wird, soll die Meldung nach einer automatisierten Vollständigkeitsprüfung unmittelbar zur Registrierung führen. Es darf somit künftig eine Anwendung grundsätzlich erst nach erfolgter Registrierung in Betrieb gehen (bisher war nur die Abgabe der Meldung erforderlich).

Erleichtert wurde die Übernahme der Datenanwendungen durch einen Rechtsnachfolger (bisher waren Neumeldungen erforderlich).

§ 22a – Verfahren zur Überprüfung der Erfüllung der Meldepflicht

Der neugeschaffene § 22a ermächtigt die DSK, auch unabhängig vom Registrierungsverfahren jederzeit die Mangelhaftigkeit der Meldungen und die Erfüllung der Meldepflichten zu prüfen und in der Folge ein Verbesserungsverfahren durchzuführen, das in letzter Konsequenz auch bis zum Verbot des Betriebs einer Datenanwendung führen kann.

Diese Bestimmungen sind wohl im Hinblick darauf zu verstehen, dass künftig die meisten Meldungen im Selbstbedienungsverfahren eingebracht und im Regelfall von keinem Mitarbeiter der DSK auf formelle und materielle Mängel analysiert werden.

§ 30 Kontrollbefugnisse der DSK

Die Kontrollbefugnisse der DSK wurden dahingehend erweitert, dass sich der betriebliche Datenschutzbeauftragte wegen eines Verdachts der Verletzung datenschutzrechtlicher Vorschriften im Betrieb an die DSK wenden kann, worauf die DSK mit einem Prüfungsverfahren gem. § 22a vorgehen kann.

Mit dem neuen Abs. 6a hat die DSK auch die Option eines Eingriffs bei Gefahr im Verzug:

Liegt durch den Betrieb einer Datenanwendung eine wesentliche Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen (Gefahr im Verzug) vor, so hat die Datenschutzkommission die Weiterführung der Datenanwendung mit Bescheid gemäß § 57 Abs. 1 AVG zu untersagen. Wenn dies technisch möglich, im Hinblick auf den Zweck der Datenanwendung sinnvoll und zur Beseitigung der Gefährdung ausreichend scheint, kann die Weiterführung auch nur teilweise untersagt werden. Wird einer Untersagung nicht sogleich Folge geleistet, ist Strafanzeige wegen der Verwaltungsübertretung nach § 52 Abs. 1 Z 3 zu erstatten. Nach Rechtskraft einer Untersagung nach diesem Absatz ist ein Berichtigungsverfahren nach § 22a Abs. 2 formlos einzustellen. Die Datenanwendung ist im Umfang der Untersagung aus dem Register zu streichen.

Anmerkung: Diese Regelung bedeutet, dass eine einmal gemeldete und registrierte Anwendung jederzeit – auch nach mehreren Jahren – von der DSK untersagt werden kann.

§ 31 Beschwerde an die DSK
§ 31a Begleitende Maßnahmen im Beschwerdeverfahren

Die Bestimmungen über die Beschwerdeverfahren wurden wesentlich überarbeitet. Da es sich aber um reine Verfahrensvorschriften handelt – und da diese Verfahren bei einem korrekt arbeitenden Auftraggeber im Regelfall gar nicht auftreten sollten –, haben wir auf eine Erörterung im Rahmen des vorliegenden DSG-Info verzichtet.

§§ 50a bis 50e Videoüberwachung

Diese Bestimmungen werden ungekürzt abgedruckt:

§ *50a. Allgemeines*

(1) *Videoüberwachung bezeichnet die systematische, insbesondere fortlaufende Feststellung von Ereignissen, die ein bestimmtes Objekt („überwachtes Objekt") betreffen, durch technische Bildaufnahmegeräte. Für derartige Überwachungen gelten die folgenden Absätze, sofern nicht durch andere Gesetze Besonderes bestimmt ist.*

(2) *Videoüberwachung sowie die Auswertung und Übermittlung der dabei ermittelten Daten darf vorbehaltlich des Abs. 5 nur zum Schutz der überwachten Objekte oder zur Beweissicherung im Hinblick auf Ereignisse nach Abs. 1 erfolgen.*

(3) *Ein Betroffener ist durch eine Videoüberwachung dann nicht in seinen schutzwürdigen Geheimhaltungsinteressen (§ 7 Abs. 2 Z 3) verletzt, wenn*

1. *diese im lebenswichtigen Interesse einer Person erfolgt, oder*

2. *Daten über ein Verhalten verarbeitet werden, das ohne jeden Zweifel den Schluss zulässt, dass es darauf gerichtet war, öffentlich wahrgenommen zu werden, oder*

3. *er der Verwendung seiner Daten im Rahmen der Überwachung ausdrücklich zugestimmt hat, oder*

4. *sich die Überwachung in einer bloßen Echtzeitwiedergabe von das überwachte Objekt betreffenden Ereignisse erschöpft, diese also weder gespeichert (aufgezeichnet) noch in sonst einer anderen Form weiterverarbeitet werden, und sie zum Zweck des Schutzes von Leib, Leben oder Eigentum des Auftraggebers erfolgt, oder*

5. *bestimmte Tatsachen die Annahme rechtfertigen, das überwachte Objekt könnte das Ziel oder der Ort eines gefährlichen Angriffes im Sinn von § 16 Abs. 1 Z 1 des Sicherheitspolizeigesetzes (SPG), BGBl. Nr. 566/1991 in der jeweils geltenden Fassung, werden. Als bestimmte Tatsache ist es insbesondere anzusehen, wenn*

a) *das überwachte Objekt bereits einmal Ziel oder Ort eines gefährlichen Angriffs war und eine Wiederholung wahrscheinlich ist. Zu berücksichtigen sind jedenfalls nur gefährliche Angriffe, die sich innerhalb der vergangenen zehn Jahre ereignet haben. Ist für die dem gefährlichen Angriff zu Grunde liegende gerichtlich strafbare Handlung (§ 16 Abs. 2 SPG) nach § 57 des Strafgesetzbuches (StGB), BGBl Nr. 60/1974 in der jeweils geltenden Fassung, eine kürzere Verjährungsfrist vorgesehen, so sind nur gefährliche Angriffe innerhalb dieser Frist relevant. § 58 StGB hat dabei außer Betracht zu bleiben, oder*

b) *das überwachte Objekt eine Person mit überdurchschnittlichem Bekanntheitsgrad in der Öffentlichkeit oder ein Aufenthaltsort einer derartigen Person ist, oder*

c) *das überwachte Objekt ein verfassungsmäßiges Organ oder dessen Aufenthaltsort ist, oder*

d) *das überwachte Objekt ein beweglicher Gegenstand mit Geldwert von mehr als EUR 100.000,– oder ein Aufenthaltsort derartiger Gegenstände ist, oder*

e) *das überwachte Objekt ein Gegenstand von überdurchschnittli-*

chem künstlerischem Wert ist,

oder

6. *unmittelbar anwendbare Rechtsvorschriften des Völker- oder des Gemeinschaftsrechts, Gesetze, Verordnungen, Bescheide oder gerichtliche Entscheidungen dem Auftraggeber spezielle Sorgfaltspflichten zum Schutz der überwachten Objekte auferlegen, oder*

7. *die Videoüberwachung zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche des Auftraggebers vor einem Gericht im Sinn von Art. 234 EGV erforderlich ist.*

(4) *Abs. 3 Z 4 bis 7 sind für Auftraggeber des öffentlichen Bereichs bei Wahrnehmung ihrer hoheitlichen Aufgaben nicht anwendbar. Außerdem dürfen mit einer Videoüberwachung nach Abs. 3 Z 4 bis 7 nicht Ereignisse an Orten festgestellt werden, die zum höchstpersönlichen Lebensbereich eines Betroffenen zählen.*

(5) *Schutzwürdige Geheimhaltungsinteressen Betroffener sind auch dann nicht verletzt, wenn durch Videoüberwachung aufgezeichnete Daten über eine Verwendung entsprechend den Abs. 2 und 3 hinaus an die zuständige Behörde oder das zuständige Gericht übermittelt werden, weil beim Auftraggeber der begründete Verdacht entstanden ist, die Daten könnten*

1. *eine von Amts wegen zu verfolgende gerichtlich strafbare Handlung dokumentieren, oder*

2. *der Abwehr oder Beendigung eines gefährlichen Angriffs dienen,*

auch wenn sich die Handlung oder der Angriff nicht gegen das überwachte Objekt richtet. Die Befugnisse von Behörden und Gerichten zur Durchsetzung der Herausgabe von Beweismaterial und zur Beweismittelsicherung sowie damit korrespondierende Verpflichtungen des Auftraggebers bleiben unberührt.

(6) *Mit einer Videoüberwachung gewonnene Daten von Betroffenen dürfen nicht automationsunterstützt mit anderen Bilddaten abgeglichen und nicht nach sensiblen Daten als Auswahlkriterium durchsucht werden.*

(7) *Im Übrigen gelten auch für Videoüberwachung die §§ 6 und 7, insbesondere der Verhältnismäßigkeitsgrundsatz (§ 7 Abs. 3).*

Anmerkungen: § 50a regelt also in Absatz 3 die Zulässigkeit von Videoüberwachungen, wobei im Wesentlichen die selben Kriterienkataloge angewendet werden, die schon in der Vergangenheit von der DSK im Registrierungsverfahren herangezogen wurden.

§ 50a Abs. 3 Z 2 betrifft zB die Bildübertragung mittels einer Webcam aus einer Diskothek in das Internet.

Die Anwendbarkeit von § 50a Abs. 3 Z 3 wird wohl nur extreme Ausnahmefälle betreffen, denn eine ausdrückliche Zustimmung kann ja nur von den regelmäßigen Nutzern eines Objektes eingeholt werden, hingegen nicht von zufälligen Besuchern.

Unzumutbar erscheint in § 50a Abs. 3 Z 5 lit. a die Forderung, dass im überwachten Objekt bereits eine Straftat erfolgt sein muss, damit man die Überwachung rechtfertigen kann. Hier werden verfassungsmäßig garantierte Rechtsgüter (Eigentum, körperliche Unversehrtheit, Hausrecht) völlig missachtet, weiters wird verkannt, dass der Hauptzweck einer jeden Videoüberwachung auch in der Prävention liegen kann. Desgleichen

stellt die Vermögensgrenze von 100.000 Euro eine nicht akzeptable und auch willkürliche Beschränkung dar. Darüber hinaus ist es eine überraschende Information, dass die DSK nunmehr auch in der Lage sein soll, den Wert von Kunstwerken zu schätzen.

§ 50b. Besondere Protokollierungs- und Löschungspflicht
(1) *Jeder Verwendungsvorgang einer Videoüberwachung ist zu protokollieren.*
(2) *Aufgezeichnete Daten sind, sofern sie nicht aus konkretem Anlass für die Verwirklichung der zu Grunde liegenden Schutz- oder Beweissicherungszwecke oder für Zwecke nach § 50a Abs. 5 benötigt werden, spätestens nach 48 Stunden zu löschen. Die Datenschutzkommission hat auf Antrag des Auftraggebers eine längere Aufbewahrung zu genehmigen, wenn dies aus besonderen Gründen zur Zweckerreichung regelmäßig erforderlich ist. Ein solcher Antrag ist bei meldepflichtigen Videoüberwachungen tunlichst mit der Meldung zu verbinden.*

Anmerkungen: Auffällig ist die kurze Aufbewahrungsdauer von 48 Stunden. Die mag zwar bei einer Videoüberwachung von Straßenbahn und Eisenbahn ausreichend sein, nicht aber in der betrieblichen Praxis, wenn man das Wochenende, unter Umständen mit anschließendem Feiertag, berücksichtigt.

Unseres Erachtens ist eine Einsatzform der Videoüberwachung zu bevorzugen, wo niemand regelmäßig in die Filme Einsicht nehmen muss, sondern erst bei Bekanntwerden eines Vorfalls – dies kann aber Tage oder Wochen nach dem relevanten Ereignis sein.

§ 50c. Meldepflicht und Registrierungsverfahren
(1) *Eine Videoüberwachung ist über § 17 Abs. 2 hinaus von der Meldepflicht ausgenommen, wenn* ***1.*** *§ 50a Abs. 3 Z 4 erfüllt ist oder* ***2.*** *eine Speicherung (Aufzeichnung) nur auf einem analogen Speichermedium erfolgt.*
(2) *Meldepflichtige Überwachungen unterliegen stets der Vorabkontrolle (§ 18 Abs. 2). Bestimmte Tatsachen im Sinn von § 50a Abs. 1 Z 5 und die Anspruchsverfolgung nach § 50a Abs. 1 Z 7 müssen bei Erstattung der Meldung glaubhaft gemacht werden.*
(3) *Mehrere überwachte Objekte, für deren Videoüberwachung derselbe Auftraggeber eine gesetzliche Zuständigkeit oder rechtliche Befugnis (§ 7 Abs. 1) hat, können auf Grund ihrer gleichartigen Beschaffenheit oder ihrer räumlichen Verbundenheit in einer Meldung zusammengefasst werden, wenn sich diese auf die gleiche Rechtsgrundlage stützt.*

Anmerkungen: Die Meldepflicht entspricht den derzeitigen Gepflogenheiten beim DVR. Es ist allerdings unklar, warum man die Vorabkontrolle nicht bereits in § 18 Abs. 2 festlegt, dort wäre das systematisch korrekt.

Die Bestimmung, die eine analoge Aufzeichnung der Videoüberwachung von der Meldepflicht entbindet, entspricht zwar der gängigen Praxis bei der DSK, ist aber objek-

tiv absurd. Im Übrigen befremdet der Verweis auf § 17 Abs. 2, denn nach § 17 Abs. 2 wäre die Videoüberwachung überhaupt nicht meldepflichtig, da sie ausschließlich veröffentlichte Daten (sofern die Aufzeichnung im öffentlichen Raum erfolgt) und indirekt personenbezogene Daten (da die Überwachungsanwendungen gem. § 50a Abs. 6 keinem automationsunterstützten Identifizierungsschritt unterworfen werden dürfen) enthält.

§ *50d. Information durch Kennzeichnung*

(1) *Der Auftraggeber einer Videoüberwachung hat diese geeignet zu kennzeichnen. Die Kennzeichnung hat jedenfalls den Auftraggeber zu benennen und hat örtlich derart zu erfolgen, dass jeder potentiell Betroffene, der sich einem überwachten Objekt nähert, tunlichst die Möglichkeit hat, der Videoüberwachung auszuweichen.*

(2) *Die Kennzeichnung kann entfallen,*

1. *wenn sie angesichts der Unwahrscheinlichkeit einer Beeinträchtigung der Betroffenenrechte oder der Beschaffenheit des überwachten Objekts, insbesondere dessen Mobilität, einerseits und der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordern würde, oder*

2. *im Fall einer Überwachung nach § 50a Abs. 3 Z 7, wenn dadurch die Gewinnung von Beweismitteln zur Anspruchsverfolgung vereitelt würde.*

(3) *Der beabsichtigte Entfall einer Kennzeichnung nach Abs. 2 ist bei meldepflichtigen Überwachungen in der Meldung an die Datenschutzkommission anzugeben. Wenn diese die Voraussetzungen nicht als gegeben erachtet, hat sie eine Kennzeichnung mit Bescheid anzuordnen.*

Anmerkungen: Die generelle Kennzeichnungspflicht von videoüberwachten Objekten ist grundsätzlich zu begrüßen.

§ *50e. Auskunftsrecht*

(1) *Abweichend von § 26 Abs. 1 ist dem Auskunftswerber, nachdem dieser den Zeitraum, in dem er möglicherweise von der Überwachung betroffen war, möglichst präzise benannt und seine Identität in geeigneter Form nachgewiesen hat, Auskunft über die zu seiner Person verarbeiteten Daten durch Übersendung einer Kopie der zu seiner Person verarbeiteten Daten in einem üblichen technischen Format zu gewähren. Alternativ kann der Auskunftswerber eine Einsichtnahme auf Lesegeräten des Auftraggebers verlangen, wobei ihm auch in diesem Fall die Ausfolgung einer Kopie zusteht. Die übrigen Bestandteile der Auskunft (verfügbare Informationen über die Herkunft, Empfänger oder Empfängerkreise von Übermittlungen, Zweck, Rechtsgrundlagen sowie allenfalls Dienstleister) sind auch im Fall der Überwachung schriftlich zu erteilen, wenn nicht der Auskunftswerber einer mündlichen Auskunftserteilung zustimmt.*

(2) *§ 26 Abs. 2 ist mit der Maßgabe anzuwenden, dass in dem Fall, dass eine Auskunft wegen überwiegender berechtigter Interessen Dritter nicht in der in Abs. 1 geregelten Form erteilt werden kann, der Auskunftswerber Anspruch auf eine schriftliche Beschreibung seines von der Überwachung verarbeiteten Verhaltens hat.*

Anmerkungen: Wir halten diese Bestimmungen für völlig undurchführbar, und zwar aus folgenden Gründen:

- Die maximal zulässige Aufbewahrungsdauer von 48 Stunden beschränkt den Zeitraum, in dem überhaupt eine Auskunft erteilt werden könnte, auf ein Minimum.
- Der Nachweis der Identität des Auskunftswerbers kann nicht zum gewünschten Ziel führen, nämlich den Auskunftswerber tatsächlich auf den Videos zu erkennen, da die Daten auf der Videoaufzeichnung aus Sicht des Auftraggebers im Regelfall den Charakter von indirekt personenbezogenen Daten haben.
- Die Einsichtnahme in die Aufzeichnungen bzw. die Ausfolgung einer Kopie kann überhaupt nur in jenen Fällen zulässig sein, in denen sich der Auskunftswerber ***allein*** im videoüberwachten Bereich aufgehalten hat. Andernfalls würden die Betroffenenrechte weiterer Personen unzulässigerweise beeinträchtigt.

§ 60 Inkrafttreten
§ 61 Übergangsbestimmungen

Vorgesehen ist, dass die Verfassungsbestimmungen der Novelle am 1. Juli 2008 in Kraft treten, die meisten einfachgesetzlichen Bestimmungen und insbesondere die Videoüberwachung am 1. März 2008 (das ist wohl zu bezweifeln), der betriebliche Datenschutzbeauftragte am 1. Juli 2009.

Für Videoüberwachungen ist eine Übergangsbestimmung vorgesehen: *Videoüberwachungen, die vor dem Inkrafttreten der §§ 50a bis 50e registriert wurden, sind bis zum 1. Juli 2010 auch dann rechtmäßig, wenn sie den am 30. Juni 2008 geltenden datenschutzrechtlichen Bestimmungen genügen.*

Das ist aus mehreren Gründen nicht akzeptabel. Erstens bedarf es der Rechtssicherheit, dass ein einmal erteilter Bescheid auch weiterhin Gültigkeit behält, zweitens gibt es relativ wenige ***registrierte*** Videoüberwachungen, hingegen eine große Zahl an ***eingereichten und nicht fristgerecht registrierten*** Anwendungen.

Für die Meldung des Datenschutzbeauftragten lautet die Übergangsbestimmung: *Die Angaben zum betrieblichen Datenschutzbeauftragten (§ 19 Abs. 1 Z 8) sind der Datenschutzkommission bei vor dem 1. Juli 2009 registrierten Datenanwendungen anlässlich der ersten über eine Streichung hinausgehenden Änderungsmeldung zu melden, die ab diesem Datum erstattet wird. Eine Meldung allein im Hinblick auf § 19 Abs. 1 Z 8 ist nicht erforderlich.*

••••

Hinweis: Unser Datenschutzseminar am 6. Mai 2008 ist bereits ausgebucht.
Der nächste Termin im Herbst wird noch festgelegt.