Secur-Data Betriebsberatungsges.m.b.H.
1010 Wien, Fischerstiege 9
Tel. +43 (1) 533 42 07-0
Internet: www.secur-data.at E-Mail: office@secur-data.at

DSG-Info-Service

Juni 2009 Ausgabe Nr. 58/59/60

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

Der in der Ausgabe Nr. 56 unseres DSG-Info-Service vorgestellte Entwurf einer DSG-Novelle 2008, der am 11. April 2008 zur Begutachtung veröffentlicht wurde, hat zu einer noch nie dagewesenen Flut von Stellungnahmen geführt. Anschließend wurde es sehr still um die Materie.

Nun wurde am 20. Mail 2009 ein neuer Novellenentwurf zur Begutachtung veröffentlicht. Die Begutachtungsfrist läuft bis zum 17. Juni 2009.

Wir erwarten uns, dass diesmal die Verabschiedung durch das Parlament bis zum geplanten Inkrafttreten am 1. Jänner 2010 gelingen wird.

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 neuerlich eine Dreifachausgabe unseres DSG-Info in Händen.

Ministerialentwurf der DSG-Novelle 2010

Im Internet vollinhaltlich nachzulesen unter
http://www.parlinkom.gv.at/PG/DE/XXIV/ME/ME_00062/pmh.shtml

Kernpunkte des Novellierungsentwurfs

Die wesentlichen Kernaussagen des Gesetzesentwurfs sind zum Teil schon dem Pressematerial zu entnehmen:

- Bundeskompetenz für den gesamten Datenschutz und damit verbunden Entlastung der Länder;
- Regelung der Videoüberwachung;

- Entschärfung der Personalsituation insbesondere beim DVR.

Nicht Eingang in die Novelle fanden zwei 2008 noch vorgesehene Punkte:

- Einführung des betrieblichen Datenschutzbeauftragten;
- Auflassung des Datenschutzes für juristische Personen und Personengemeinschaften.

Novelle zum B-VG

In Artikel 10 und 102 der Bundesverfassung wird der Schutz personenbezogener Daten unter Bundeskompetenz gestellt.

Dies ist zu begrüßen, weil damit die 9 Landes-Datenschutzgesetze wieder entbehrlich werden. Da diese nur für gewisse manuell geführte Datenanwendungen überhaupt anwendbar waren, war die bestehende Rechtslage alles andere als zweckmäßig.

Gliederung

Die Gliederung des DSG in zwei Artikel, von denen der Artikel 1 eine Verfassungsbestimmung darstellt, wurde fallen gelassen. Dies war möglich, weil die Datenschutzkompetenz direkt in die Verfassung eingearbeitet wurde.

§ 1 Grundrecht auf Datenschutz (Verfassungsbestimmung)

Der Absatz 1 und der Anfang von Absatz 2 wurden neu formuliert und sollen folgenden Wortlaut erhalten:

> ***(1)*** *Jedermann hat Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten.*
>
> ***(2)*** *Der Anspruch besteht nicht, wenn Daten zulässigerweise allgemein verfügbar sind. Soweit ... (Rest unverändert)*

Es liegt also eine sprachliche Straffung vor, aber keine wesentliche inhaltliche Änderung.

§ 2 Zuständigkeit

Dieser Paragraph entfällt komplett, da er aufgrund der einheitlichen Datenschutzkompetenz des Bundes entbehrlich geworden ist.

§ 3 Räumlicher Anwendungsbereich

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 (dies wurde auch in § 12 und in § 34 Abs. 4 berücksichtigt).

§ 3 Abs. 4 wird gestrichen. Dies wird damit begründet, dass es keine Landesgesetzgebung mit einer möglicherweise anderen Sicht des Sitzstaatsprinzips geben wird.

§ 4 Definitionen und Regelungsgegenstand

Der Paragraph 4 enthält die bisherigen Bestimmungen als Absatz 1, die Regelungen der manuellen Datenarten treten als neuer Absatz 2 dazu.

Höchst aufklärungsbedürftig erscheint uns Z 3: Die Novelle enthält hier keine Änderung, sehr wohl kursiert auf der Parlamentsseite eine Textgegenüberstellung (bestehendes DSG ver-

glichen mit dem novellierten Gesetz), wo die juristischen Personen und die Personengemeinschaften nicht mehr als Betroffene anerkannt werden.

Da wesentliche Rechte aus dem DSG nur dem Betroffenen zustehen (insbesondere Auskunft, Richtigstellung, Löschung und Widerspruch), wird das noch zu beobachten sein.

Die Definition des Auftraggebers (Z 4) wurde gestrafft. Klargestellt wird, dass die Auftraggebereigenschaft auch dann erhalten bleibt, wenn der Dienstleister im Rahmen des ihm vom Auftraggeber erteilten Werkauftrages Daten bei Dritten ermittelt (sog. Ermittlungsdienstleister).

Die Definition des Dienstleisters (Z 5) wurde insofern verschärft, als der mit einer Werkherstellung Beauftragte nur dann Dienstleister ist, wenn er NUR die ihm vom Auftraggeber überlassenen Daten verwendet. So wird ein mit der Herstellung eines Werkes Beauftragter, der Daten verschiedener Auftraggeber verwendet, selbst zum Auftraggeber.

Die Begriffe „verwenden" (Z 9), „verarbeiten" (Z 10) und „übermitteln" (Z 12) umfassen nunmehr Daten in jeglicher Form, bisher ging es nur um Daten in einer Datenanwendung. Dafür verliert der Begriff „ermitteln" (Z 10) seine Definition. Andere Definitionen wurden nur leicht verändert.

§ 4 Abs. 2

Der neue Abs. 2 ersetzt sinngemäß den bisherigen § 58 und hat folgenden Wortlaut:

Dieses Gesetz gilt für Daten, die in einer Datenanwendung oder manuellen Datei verwendet werden. Wo in den folgenden Bestimmungen von Datenanwendungen die Rede ist, gelten sie auch für manuelle Dateien. Für alle übrigen manuellen Daten gelten § 6 Abs. 1 Z 1 bis 3 und Abs. 2, §§ 7 bis 9 und die Bestimmungen des 6. Abschnitts sinngemäß.

Im Klartext bedeutet das, dass das DSG für manuelle Daten in strukturierter Form vollinhaltlich gilt, für unstrukturierte Daten gelten nur:

- Datenverwendung nach Treu und Glauben (§ 6 Abs. 1 Z 1)
- Datenverwendung für festgelegte Zwecke (§ 6 Abs. 1 Z 2)
- Datenverwendung nur in jenem Umfang, der für den Zweck wesentlich ist (§ 6 Abs. 1 Z 3)
- Verantwortlichkeit des Auftraggebers (§ 6 Abs. 2)
- Zulässigkeit der Verwendung von Daten (§ 7)
- Schutzwürdige Geheimhaltungsinteressen bei der Verwendung von Daten (§§ 8 und 9)
- Rechtsschutz (§§ 30 bis 34)

Die Erleichterung, dass manuelle Dateien nur dann meldepflichtig sind, wenn sie der Vorabkontrolle unterliegen, besteht weiter, sie ist künftig in § 17 Abs. 1 geregelt.

§ 8 Schutzwürdige Geheimhaltungsinteressen bei nicht-sensiblen Daten

Zu den bisher geltenden Regelungen tritt ein neuer Umstand hinzu, der die Datenweitergabe erlaubt:

- *„Datenweitergabe zum Zweck der Erstattung einer Anzeige an eine zur Verfolgung der strafbaren Handlungen (Unterlassungen) zuständige Behörde"*

Diese Regelung dürfte unumstritten zu begrüßen sein, unseres Erachtens sollten in diesem Zusammenhang aber auch sensible Daten im notwendigen Ausmaß gedeckt sein. Hingegen wurde die im DSG-Entwurf aus 2008 enthaltene Zulässigkeit der Datenweitergabe für parlamentarische Kontrollzwecke nicht wieder aufgegriffen.

§§ 16 bis 22
Bestimmungen rund um das DVR

Ob das DVR künftig in Form einer Internetanwendung mit der Möglichkeit einer Online-Abfrage geführt wird, bleibt offen. Klar ist nur, dass die Einbringung der Meldungen mittels Internetanwendung zu erfolgen hat:

> ***§ 17 Abs. 1a**: Die Meldung ist in elektronischer Form im Wege der vom Bundeskanzler bereit zu stellenden Internetanwendung einzubringen. Die Identifizierung und Authentifizierung kann insbesondere durch die Bürgerkarte (§ 2 Z 10 des EGovernment-Gesetzes, BGBl. I Nr. 10/2004) erfolgen. Nähere Bestimmungen über die Identifizierung und Authentifizierung sind in die gemäß § 16 Abs. 3 zu erlassende Verordnung aufzunehmen. Eine Meldung in nicht-elektronischer Form ist für manuelle Dateien sowie bei einem längeren technischen Ausfall der Internetanwendung zulässig.*

Die Möglichkeit einer Papiermeldung bei Auftraggebern, die nur Papieranwendungen betreiben und möglicherweise gar keine elektronische Datenverarbeitung besitzen, ist vernünftig. Ob für andere Auftraggeber der Zwang, über einen Internetzugang verfügen zu müssen, verfassungsrechtlich hält, bleibt fraglich. Grundsätzlich ist der Weg in Richtung einer E-Government-Lösung zu begrüßen, wobei zu hoffen ist, dass die Internetanwendung einfach zu bedienen sein wird und jedenfalls das Einkopieren von vorhandenen tabellarischen Daten ermöglicht. Als unzumutbar würden wir ansehen, wenn man eine Liste der Datenarten Zeile für Zeile abtippen muss.

Ein völlig neuer Aspekt ist eine neue Befreiung von der Meldepflicht:

> ***§ 17 Abs. 4**: Weiters sind Datenanwendungen von der Meldepflicht ausgenommen, für die der Zweck, die betroffenen Personengruppen, Datenarten, Übermittlungen und Übermittlungsempfänger in einem Gesetz oder in einer Verordnung abschließend geregelt sind.*

Dies stellt unseres Erachtens eine eklatante Aushöhlung des mit dem Datenverarbeitungsregister zu erzielenden Zweckes dar. Künftig kann sich jeder Rechtsträger, der zur Erlassung einer Verordnung ermächtigt ist, seine Anwendungen per Verordnung registrierungsfrei stellen.

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):

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

trag auch die Registernummer des Rechtsvorgängers übertragen werden, wenn der Rechtsvorgänger jegliche Verarbeitung personenbezogener Daten in Auftraggebereigenschaft eingestellt hat.

§ 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 lt. § 20 Abs. 1 nur automationsunterstützt auf ihre Vollständigkeit und Plausibilität geprüft werden.

§ 24 Informationspflicht des Auftraggebers

Es wurde eine neue Informationsverpflichtung für den Fall eingeführt, dass ein Auftraggeber Kenntnis eines schweren Datenmissbrauchs erhält:

***§ 24 Abs. 2a**: Wird dem Auftraggeber bekannt, dass Daten aus einer seiner Datenanwendungen systematisch und schwerwiegend unrechtmäßig verwendet wurden, hat er darüber unverzüglich die Betroffenen zu informieren.*

Die Bestimmung ist grundsätzlich zu begrüßen, sollte aber einerseits erweitert werden um jene Fälle, wo Datenträger abhanden gekommen sind und noch keine unrechtmäßige Verwendung aufgefallen ist, andererseits sollte sie eingeschränkt werden auf Anwendungen mit Risikopotential. Ein gestohlenes Telefonverzeichnis rechtfertigt unseres Erachtens nicht den hohen Informationsaufwand.

§ 26 Auskunftsrecht

Das Auskunftsrecht wurde auf beliebige Auskunftswerber erweitert, bisher hatte nur der Betroffene ein Auskunftsrecht, was dazu führte, dass keine Negativauskunft (zu Ihrer Person sind keine Daten vorhanden) erhältlich war.

Verschärft wurde die Auskunftspflicht über die Herkunft der Daten, die Einschränkung auf die „verfügbaren Informationen“ besteht nicht mehr. Ob damit tatsächlich eine Verbesserung für den Betroffenen erwartet werden kann, bleibt abzuwarten.

§ 30 Kontrollbefugnisse der DSK

Die Kontrollbefugnisse der DSK wurden an das geänderte Registrierungsverfahren angepasst. Darüber hinaus gibt es eine neuen Option eines Eingriffs bei Gefahr im Verzug:

***§ 30 Abs. 6a**: 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.

§ 32 Anrufung der Gerichte

Es wurde eine neuer Absatz mit folgendem Wortlaut eingefügt:

***§ 32 Abs. 7**: Anlässlich einer zulässigen Klage nach Abs. 1, die sich auf eine nach Ansicht des Gerichts meldepflichtige Datenanwendung bezieht, hat das Gericht die Datenschutzkommission um Überprüfung nach den §§ 22 und 22a zu ersuchen. Die Datenschutzkommission hat das Gericht vom Ergebnis der Überprüfung zu verständigen. Dieses ist sodann vom Gericht auch den Parteien bekannt zu geben, sofern das Verfahren noch nicht rechtskräftig beendet ist.*

In der Begleitdokumentation wird dazu ausgeführt, dass dadurch eine Prüfung der Meldung durch die DSK auch bei Anwendungen erfolgen kann, die nicht der Vorabkontrolle unterliegen und daher im Meldeverfahren nicht mehr geprüft werden.

§§ 35 bis 44 Kontrollorgane

In § 36 Abs. 6 wurde nicht nur eine Altersgrenze von 65 Jahren für Mitglieder der DSK eingezogen, künftig endet die Mitgliedschaft für das richterliche Mitglied und für das Mitglied aus dem Kreis der rechtskundigen Bundesbediensteten (Beamtenstatus ist grundsätzlich nicht mehr erforderlich) auch dann, wenn die zugrundeliegende Funktion nicht mehr besteht (Ruhestand, Ausscheiden als Richter etc.).

Die Geschäftsordnung der DSK ist im Internet kundzumachen (§ 38 Abs. 1).

Der Bundekanzler hat das Recht, sich jederzeit über alle Gegenstände der Geschäftsführung der Datenschutzkommission beim Vorsitzenden und dem geschäftsführenden Mitglied zu unterrichten (§ 38 Abs. 2). Dies wird in der Begleitdokumentation als notwendig im Hinblick auf Art. 20 Abs. 2 letzter Satz B-VG begründet.

Der Datenschutzrat hat nunmehr das Recht, von der DSK Auskünfte und Berichte sowie Einsicht in Unterlagen zu verlangen (§ 41 Abs. 4a). In der Begleitdokumentation ist dazu klargestellt, dass sich dies auf den Aufgabenumfang des DSR zu beschränken hat und keinesfalls personenbezogene Daten von Beschwerdeführern zu übermitteln sind. Es wäre also zu begrüßen, diese Klarstellung auch in den Gesetzestext einfließen zu lassen.

§ 50 Informationsverbundsysteme

Es wurde ein vereinfachtes Meldeverfahren in analoger Form wie bei Musteranwendungen

für neue Teilnehmer an einem bereits bestehenden Informationsverbundsystem definiert:

***§ 50 Abs. 2a**: Wird ein Informationsverbundsystem auf Grund einer Meldung von zumindest zwei Auftraggebern registriert, so können Auftraggeber, die in der Folge die Teilnahme an dem Informationsverbundsystem anstreben, die Meldung im Umfang des § 19 Z 3 bis 8 auf einen Verweis auf den Inhalt der Meldung eines bereits registrierten Auftraggebers beschränken, wenn sie eine Teilnahme im genau gleichen Umfang anstreben. Soweit sich ein solcher weiterer Auftraggeber anlässlich der Meldung ausdrücklich den Auflagen unterwirft, die die Datenschutzkommission anlässlich der Meldung, auf die er verweist, ausgesprochen hat, werden diese für ihn mit der Registrierung in gleicher Weise und mit gleicher Wirkung (§ 52 Abs. 1 Z 3) verbindlich und ist die Erlassung eines gesonderten Auflagenbescheides durch die Datenschutzkommission nicht erforderlich.*

Durch einen Zusatz in § 50 Abs. 2 kann die Meldung des Verbundsystems dem Betreiber übertragen werden.

§§ 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“) oder eine bestimmte Person („überwachte Person“) betreffen, durch technische Bildaufnahme- oder Bildübertragungsgeräte. Für derartige Überwachungen gelten die folgenden Absätze, sofern nicht durch andere Gesetze Besonderes bestimmt ist. § 45 bleibt unberührt.*

***(2)** Für Videoüberwachung gelten die §§ 6 und 7, insbesondere der Verhältnismäßigkeitsgrundsatz (§ 7 Abs. 3). Rechtmäßige Zwecke einer Videoüberwachung, insbesondere der Auswertung und Übermittlung der dabei ermittelten Daten, sind jedoch vorbehaltlich des Abs. 5 nur der Schutz des überwachten Objekts oder der überwachten Person oder die Erfüllung gesetzlicher oder vergleichbarer rechtlicher Sorgfaltspflichten, jeweils einschließlich der Beweissicherung, im Hinblick auf Ereignisse nach Abs. 1.*

***(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.*

***(4)** Ein Betroffener ist darüber hinaus durch eine Videoüberwachung ausschließlich dann nicht in seinen schutzwürdigen Geheimhaltungsinteressen (§ 7 Abs. 2 Z 3) verletzt, wenn sie nicht im Rahmen der Vollziehung hoheitlicher Aufgaben erfolgt und*

***1.** bestimmte Tatsachen die Annahme rechtfertigen, das überwachte Objekt oder die überwachte Person könnte das Ziel oder der Ort eines gefährlichen Angriffs werden, oder*

***2.** unmittelbar anwendbare Rechtsvorschriften des Völker- oder des Gemeinschaftsrechts, Gesetze, Verordnungen, Bescheide oder*

gerichtliche Entscheidungen dem Auftraggeber spezielle Sorgfaltspflichten zum Schutz des überwachten Objekts oder der überwachten Person auferlegen, oder

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

***(5)** Mit einer Videoüberwachung nach Abs. 4 dürfen nicht Ereignisse an Orten festgestellt werden, die zum höchstpersönlichen Lebensbereich eines Betroffenen zählen. Weiters ist die Videoüberwachung zum Zweck der Mitarbeiterkontrolle an Arbeitsstätten untersagt.*

***(6)** Schutzwürdige Geheimhaltungsinteressen Betroffener sind auch dann nicht verletzt, wenn durch Videoüberwachung aufgezeichnete Daten über eine Verwendung entsprechend den Abs. 2 bis 4 hinaus in folgenden Fällen übermittelt werden:*

***1.** an die zuständige Behörde oder das zuständige Gericht, weil beim Auftraggeber der begründete Verdacht entstanden ist, die Daten könnten eine von Amts wegen zu verfolgende gerichtlich strafbare Handlung dokumentieren, oder*

***2.** an Sicherheitsbehörden zur Ausübung der diesen durch § 53 Abs. 5 des Sicherheitspolizeigesetzes – SPG, BGBl. Nr. 566/1991, eingeräumten Befugnisse,*

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.

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

Anmerkungen: § 50a regelt also in Abs. 2 die die Zulässigkeit von Videoüberwachungen im Hinblick auf den berechtigten Zweck und in Abs. 3 bis 6 die Zulässigkeit in Abwägung der schutzwürdigen Geheimhaltungsinteressen.

Abs. 7 enthält das Verbot eines automationsunterstützten Bildabgleichs. Damit würden folgende Anwendungen unzulässig werden:

- Zutrittskontrollsysteme mit Gesichtserkennung;
- Geschwindigkeitsüberwachung mittels Section Control;
- Gegenlaufkontrolle in Bereichen, die nur in einer Richtung begangen werden dürfen (Zu- und Abgänge sicherheitskritischer Objekte).

Wir regen daher an, dieses Verbot durch eine Genehmigungspflicht zu ersetzen. Für Videoüberwachungen ohne solche Kontrollen könnten hingegen Standard- oder Musteranwendungen vorgesehen werden. Da die DSK bereits jetzt nicht in der Lage ist, die Vorabkontrolle auszuführen, ergäbe sich eine empfehlenswerte Verwaltungsvereinfachung.

Folgende Passagen weichen von den derzeit bei der DSK gehandhabten Kriterien ab:

- Bescheide oder gerichtliche Entscheidungen, die dem Auftraggeber besondere Sorgfaltspflichten auferlegen,

stellen eine Rechtsgrundlage dar (Abs. 4 Z 2).

- Die Echtzeitüberwachung wird ausdrücklich zugelassen, bisher galt sie überhaupt nicht als Datenanwendung (Abs. 4 Z 3).
- Die Datenübermittlung an Sicherheitsbehörden zur Ausübung derer eigenen Befugnisse ist zulässig (Abs. 6 Z 2); in einem Bescheid der DSK an die Stadt Villach wurde früher eine Datenanwendung mit diesem Zweck untersagt.

§ 50b. Besondere Protokollierungs- und Löschungspflicht

(1) *Jeder Verwendungsvorgang einer Videoüberwachung ist zu protokollieren. Dies gilt nicht für Fälle der Echtzeitüberwachung.*

(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. 6 benötigt werden, spätestens nach 48 Stunden zu löschen. Die Datenschutzkommission kann eine längere Aufbewahrungsdauer festsetzen, wenn dies aus besonderen Gründen zur Zweckerreichung regelmäßig erforderlich ist. Ein Antrag auf Festsetzung einer längeren Aufbewahrungsdauer 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 schon allein aus Datenschutzgründen eine Einsatzform der Videoüberwachung zu bevorzugen, wo niemand regelmäßig in die Aufzeichnung Einsicht nehmen muss, sondern erst bei Bekanntwerden eines Vorfalls – dies kann aber Tage oder Wochen nach dem relevanten Ereignis sein – anlassbezogen analysiert wird.

Es sollten daher zwei Kategorien eingeführt werden: Die Videoüberwachung bei ständig besetzter Leitstelle – hier genügen 48 Stunden – einerseits und andererseits jene Varianten, wo im Regelfall gar kein Zugriff auf die Überwachungsdaten erfolgt – hier sind Zeiträume von mindestens 14 Tagen zu fordern.

§ 50c. Meldepflicht und Registrierungsverfahren

(1) *Videoüberwachungen unterliegen der Vorabkontrolle (§ 18 Abs. 2). Bestimmte Tatsachen im Sinn von § 50a Abs. 4 Z 1 müssen bei Erstattung der Meldung glaubhaft gemacht werden. Soweit gemäß § 96a des Arbeitsverfassungsgesetzes 1974, BGBl. Nr. 22, Betriebsvereinbarungen abzuschließen sind, sind diese im Registrierungsverfahren vorzulegen.*

(2) *Eine Videoüberwachung ist über § 17 Abs. 2 bis 4 hinaus von der Meldepflicht ausgenommen*

1. *in Fällen der Echtzeitüberwachung oder*

2. *wenn eine Speicherung (Aufzeichnung) nur auf einem analogen Speichermedium erfolgt.*

(3) *Mehrere überwachte Objekte oder überwachte Personen, für deren Videoüberwachung derselbe Auftraggeber eine gesetzliche Zuständigkeit oder rechtliche Befugnis (§ 7 Abs. 1) hat, können auf Grund ihrer gleichartigen Beschaffenheit oder ihrer räumlichen Ver-*

bundenheit in einer Meldung zusammengefasst werden, wenn sich diese auf die gleiche Rechtsgrundlage stützt.

Anmerkungen: Die Meldepflicht entspricht den derzeitigen Gepflogenheiten beim DVR. Es wäre aber systematisch besser, die Vorabkontrolle von meldepflichtigen Videoüberwachungen bereits in § 18 abzuhandeln und nicht in § 50c sozusagen nachträglich hinein zu reklamieren.

Die Bestimmung, die eine analoge Aufzeichnung der Videoüberwachung von der Meldepflicht entbindet, entspricht zwar der gängigen Praxis bei der DSK, ist aber objektiv absurd. Die Begleitdokumentation begründet dies mit der fehlenden Strukturierbarkeit von VHS-Videokassetten und übersieht dabei, dass jede Videokamera grundsätzlich nur sequentielle Daten ohne weitere Strukturierung liefern kann. Der einzige Unterschied ist, dass auf der Kassette der gesuchte Zeitpunkt durch Spulen aufzusuchen ist, während dies digital direkt möglich ist. Erst wenn Informationen aus anderen Anwendungen, etwa eines elektronischen Schlosses, das den Benutzer identifizieren kann, zusammen mit den Videodaten protokolliert werden, entsteht eine Anwendung, die über die VHS-Kassette hinaus interessant ist.

§ 50d. Information durch Kennzeichnung

(1) *Der Auftraggeber einer Videoüberwachung hat diese geeignet zu kennzeichnen. Aus der Kennzeichnung hat jedenfalls der Auftraggeber eindeutig hervorzugehen, es sei denn dieser ist den Betroffenen nach den Umständen des Falles bereits bekannt. Die Kennzeichnung hat örtlich derart zu erfolgen, dass jeder potentiell Betroffene, der sich einem überwachten Objekt oder einer überwachten Person nähert, tunlichst die Möglichkeit hat, der Videoüberwachung auszuweichen.*

(2) *Keine Kennzeichnungsverpflichtung besteht bei Videoüberwachungen, die nach § 17 Abs. 2 Z 4 nicht meldepflichtig sind. Dies gilt auch für Videoüberwachungen im Rahmen der Vollziehung hoheitlicher Aufgaben, die nach § 17 Abs. 3 von der Meldepflicht ausgenommen sind.*

Anmerkungen: Die generelle Kennzeichnungspflicht von videoüberwachten Objekten ist grundsätzlich zu begrüßen, ebenso die Bekanntgabe des Auftraggebers.

§ 50e. Auskunftsrecht

(1) *Abweichend von § 26 Abs. 1 ist dem Auskunftswerber, nachdem dieser den Zeitraum, in dem er möglicherweise von der Überwachung betroffen war, und den Ort möglichst genau 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.

***(3)** In Fällen der Echtzeitüberwachung ist ein Auskunftsrecht ausgeschlossen.*

Anmerkungen: Wir halten die Bestimmungen über das Auskunftsrecht 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. Infolgedessen muss der Auftraggeber die genannte verbale Videobeschreibung verfassen.
- Da die Videoaufzeichnung eben nicht wie eine Datei im Sinne von § 4 Z 6 strukturiert ist, kann die Lokalisierung des Betroffenen auf den Aufzeichnungen nur durch einen langwierigen manuellen Suchprozess erfolgen, zumal sogar ein allenfalls möglicher automatischer Bildabgleich ausdrücklich untersagt ist. Die Begleitdokumentation spricht von einer zulässigen Abweichung bis zu einer Stunde, dh. der Auftraggeber hat für jede Anfrage die Daten von einer Stunde vor dem angegebenen Zeitpunkt bis zu einer Stunde danach zu durchsuchen. Dieser Umstand, in Verbindung mit der Tatsache, dass jedermann einmal im Jahr kostenlos diese Auskunft verlangen darf, kann dazu führen, dass Auftraggeber durch mutwillige Anfragen völlig lahmgelegt werden.
- Da ohnehin jeder Verwendungsvorgang der Videoüberwachungsdaten zu protokollieren ist (§ 50b Abs. 1), und da Videodaten nur indirekten Personenbezug haben, solange sie nicht gesichtet werden, sollten nach unserer Ansicht nur jene Teile der Videoaufzeichnung der Auskunftspflicht unterliegen, die über die reine Aufzeichnung hinaus verwendet wurden. Die große Masse der nur auf die Überschreibung wartenden Datenträger entfaltet keine Datenschutzrelevanz.

§§ 51 bis 52 Strafbestimmungen

In § 51 entfällt der Abs. 2, wodurch die Datenverwendung in Gewinn- und Schädigungsabsicht zum Offizialdelikt wird. Der Tatbestand ist auch dann schon erfüllt, wenn der Betroffene in seinen Geheimhaltungsinteressen gem. § 1 Abs. 1 geschädigt werden soll. Damit liegt eine wesentliche Verschärfung der strafrechtlichen Sanktionierungsmöglichkeiten vor.

Die Verwaltungsstrafen können nunmehr bis zu 25.000 Euro (§ 52 Abs. 1) oder 10.000 Euro (Abs. 2) betragen.

§ 60 Inkrafttreten
§ 61 Übergangsbestimmungen

Vorgesehen ist, dass die Novelle am 1. Jänner 2010 in Kraft tritt. Für Videoüberwachungen ist eine Übergangsbestimmung vorgesehen:

> ***§ 61 Abs. 6**: Videoüberwachungen, die vor dem Inkrafttreten der §§ 50a bis 50e registriert wurden, bleiben in ihrer registrierten Form rechtmäßig, wenn sie den am 31. Dezember 2009 geltenden datenschutzrechtlichen Bestimmungen genügen und die Datenschutzkommission keine Befristung verfügt hat. Hat die Datenschutzkommission hingegen eine Befristung einer solchen Videoüberwachung verfügt, bleibt diese bis zum Ablauf der Befristung, längstens aber bis zum 31. Dezember 2012 rechtmäßig.*

In Bezug auf die befristeten Anwendungen ist diese Bestimmung sinnvoll. Unklar ist allerdings, ob auch die große Zahl der zwar ***eingereichten, aber nicht fristgerecht registrierten*** Anwendungen im Hinblick auf diese Bestimmung Rechtssicherheit genießt.

Zusammenfassende Stellungnahme

Im Vergleich zum Entwurf 2008 ist die Novelle in vielen wesentlichen Punkten wirtschaftsfreundlicher geworden.

Größter Schwachpunkt des Entwurfs 2008 aus Sicht der Wirtschaft war die verpflichtende Einführung eines betrieblichen Datenschutzbeauftragten in jedem einzelnen Betrieb mit mehr als 20 Mitarbeitern (das könnte auch schon eine Einzelhandelsfiliale sein). Diese Forderung wurde nicht aufrecht gehalten.

Zweiter großer Schwachpunkt des Entwurfs 2008 waren die Bestimmungen zur Videoüberwachung, auch wenn die Tatsache, dass überhaupt eine gesetzliche Regelung dafür geplant wird, vorbehaltlos zu begrüßen war. Der Entwurf 2010 enthält gegenüber 2008 folgende Verbesserungen:

- Die Überwachung umfasst nicht nur Objekte, sondern auch Personen.
- Die Überwachung darf auch schon vorgenommen werden, wenn sich noch keine strafrechtlich relevanten Vorfälle ereignet haben.
- Die Überwachung zugunsten prominenter Personen oder Amtsträger ist nicht mehr leichter als bei Normalbürgern.
- Das überwachte Objekt muss nicht einen Mindestgeldwert von 100.000 Euro darstellen.

Bei Interesse verfolgen Sie bitte auf der Internetseite des Parlaments die einlangenden Stellungnahmen zu der Novelle. Am 8. Juni 2009 (Redaktionsschluss des vorliegenden DSG-Info) waren bereits drei Stellungnahmen publiziert.

••••

Hinweis: Unser Datenschutzseminar findet wieder im Herbst 2009 statt.
Der genaue Termin wird noch festgelegt.

Sofern die DSG-Novelle vor dem Seminartermin beschlossen wird, wird das Seminar die Rechtslage ab 2010 behandeln, andernfalls wird die Novelle nur als Zusatzpunkt behandelt.