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

Jänner 2010 Ausgabe Nr. 61/62

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

Der in der Ausgabe Nr. 58/59/60 unseres DSG-Info-Service vorgestellte Ministerialentwurf einer DSG-Novelle 2010 wurde im Zeitraum vom 20. Mai bis zum 17. Juni 2009 begutachtet. Tatsächlich langten – und zwar bis zum 14. Juli 2009 – 57 Stellungnahmen ein.

Es dauerte bis zum 17. November 2009, bis die Stellungnahmen gesichtet wurden. Den einzelnen Stellungnahmen wurde nur in geringem Ausmaß Rechnung getragen. Am 17. November 2009 wurde der Gesetzesentwurf als Regierungsvorlage dem Parlament vorgelegt. Der Beschluss im Nationalrat kam am 10. Dezember 2009 zustande, der Beschluss im Bundesrat am 18. Dezember 2009.

Aufgrund der bekannten parlamentarischen Querelen, die den Beschluss von Verfassungsgesetzen unmöglich machen, kamen letztlich nur die einfachgesetzlichen Regelungen zur Abstimmung.

Die DSG-Novelle 2010 wurde in BGBl. I Nr. 133 vom 30. Dezember 2009 publiziert und tritt am 1. Jänner 2010 in Kraft. Secur-Data hat den neuen Gesetzesstand bereits abrufbar, unter http://secur-data.at/?id=49 sind bereits alle Änderungen berücksichtigt.

DSG-Novelle 2010

BGBl. I Nr. 133/2009

Kernpunkte des Novellierungsentwurfs

Die wesentlichen Kernaussagen des Gesetzesentwurfs sind zum Teil schon dem Pressematerial zum Ministerialentwurf zu entnehmen (siehe DSG-Info Nr. 58/59/60):

- Regelung der Videoüberwachung;
- Entschärfung der Personalsituation insbesondere beim DVR.

In den folgenden Ausführungen wird primär auf Punkte eingegangen, die sich wesentlich

vom Ministerialentwurf (siehe DSG-Info Nr. 58/59/60) unterscheiden.

§ 8 Schutzwürdige Geheimhaltungsinteressen bei nicht-sensiblen Daten

Abs. 2 wurde durch eine Neuformulierung wesentlich verbessert, indem die Zweckbindung der Daten auch bei einer allfälligen Veröffentlichung gewahrt bleibt:

> ***§ 8 Abs. 2**: Schutzwürdige Geheimhaltungsinteressen gelten als nicht verletzt, wenn indirekt personenbezogene Daten verwendet werden oder zulässigerweise veröffentlichte Daten in einer mit dem ursprünglichen eindeutig erkennbaren Veröffentlichungszweck vereinbaren Weise verwendet wurden. Das Recht, gegen die Verwendung zulässigerweise veröffentlichter Daten gemäß § 28 Abs. 2 Widerspruch zu erheben, bleibt unberührt.*

Zu den bisher geltenden Regelungen tritt (§ 8 Abs. 4 Z 4) ein neuer Umstand hinzu, der die Datenweitergabe erlaubt:

> *Die Datenweitergabe zum Zweck der Erstattung einer Anzeige an eine zur Verfolgung der strafbaren Handlungen (Unterlassungen) zuständige Behörde*

Zu unserem Bedauern fehlt eine gleich lautende Ergänzung des § 9 (Verwendung sensibler Daten).

§ 13 Genehmigungspflichtiger Datenexport

§ 13 Abs 2 Z 2 erhält folgenden neuen Wortlaut:

> ***§ 13 Abs. 2 Z 2**: der Auftraggeber glaubhaft macht, daß die schutzwürdigen Geheimhaltungsinteressen der vom geplanten Datenverkehr Betroffenen auch im Ausland ausreichend gewahrt werden. Hiefür können insbesondere auch vertragliche Zusicherungen des Empfängers sowie einseitige Zusagen des Antragstellers (§ 19 Abs. 2) im Genehmigungsantrag über die näheren Umstände der Datenverwendung im Ausland von Bedeutung sein. Einseitige Zusagen des Antragstellers werden für diesen mit der Registrierung durch die Datenschutzkommission verbindlich.*

Interessant ist also der letzte Satz. Bisher wurden allfällige Zusagen des Antragstellers als Bedingungen in den Genehmigungsbescheid übernommen, mit der neuen Bestimmung könnte die DSK sich diese Arbeit ersparen.

§§ 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 E-Government-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 Form von E-Mail oder in nicht-elektronischer Form ist für manuelle Dateien sowie bei einem längeren technischen Ausfall der Internetanwendung zulässig.*

Ob für Auftraggeber der Zwang, über einen Internetzugang verfügen zu müssen, verfassungsrechtlich hält, bleibt fraglich. Grundsätzlich ist der Weg in Richtung einer E-Govern-

ment-Lösung zu begrüßen, wobei zu hoffen ist, dass die Internetanwendung einfach zu bedienen sein wird und jedenfalls das Einkopieren von vorhandenen tabellarischen Daten ermöglicht.

Eine im Ministerialentwurf noch enthaltene völlig neue Befreiung von der Meldepflicht (Wortlaut: 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.) wurde wieder fallen gelassen. Dies ist zu begrüßen, weil sonst jeder Rechtsträger, der zur Erlassung einer Verordnung ermächtigt ist, seine Anwendungen per Verordnung registrierungsfrei stellen könnte.

In § 19 wurde – bei Umnummerierung der bisherigen Abs. 2 und 3 – ein neuer Abs 2 eingefügt, der auch sehr interessant ist:

***§ 19 Abs. 2**: Der Auftraggeber kann bei Einbringung der Meldung oder danach bis zum Abschluss des Registrierungsverfahrens zusagen, dass er sich beim Betrieb der Datenanwendung bestimmten Auflagen oder Bedingungen unterwerfen oder die Datenanwendung nur befristet betreiben wird. Eine derartige Zusage wird für den Auftraggeber mit der Registrierung durch die Datenschutzkommission rechtsverbindlich. Eine Registrierung darf nur erfolgen, wenn die zugesagte Auflage, Bedingung oder Befristung derart bestimmt ist, dass sie auch von der Datenschutzkommission nach § 21 Abs. 2 ausgesprochen werden könnte.*

Auch hier wird also eine Bestimmung festgelegt, die der DSK eine Bescheiderlassung erspart, wenn der Bescheid ohnehin die vom Antragsteller beschriebenen Maßnahmen wiederholen würde.

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 sechs Monaten nach Wirksamkeit der Rechtsnachfolge eine entsprechend glaubhaft gemachte Erklärung gegenüber der Datenschutzkommission abgibt. Dem Rechtsnachfolger kann auf Antrag auch die Registernummer des Rechtsvorgängers übertragen werden, wenn der Rechtsvorgänger jegliche Verarbeitung personenbezogener Daten in Auftraggebereigenschaft eingestellt hat.*

Im Ministerialentwurf betrug die o.a. Frist noch 2 Monate. In Anbetracht des Zeitbedarfs für die Abwicklung einer Rechtsnachfolge ist diese Verlängerung ausdrücklich zu begrüßen.

§ 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 und den Betroffenen Schaden droht, hat er darüber unverzüglich die Betroffenen in geeigneter Form zu informieren. Diese Verpflichtung besteht nicht, wenn die Information angesichts der Drohung eines nur geringfügigen Schadens der Betroffenen einerseits oder der Kosten der In-*

formation aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert.

Im Vergleich zum Ministerialentwurf ist das eine vernünftige Reglung, da der Aufwand auf den möglichen Schaden abgestimmt wird.

§ 26 Auskunftsrecht

Das Auskunftsrecht wurde auch auf beliebige Personengemeinschaften erweitert, bisher hatte nur „der Betroffene" ein Auskunftsrecht, was zu zahlreichen Negativauskünften führte.

Geradezu überfällig ist die Ergänzung von § 26 Abs. 7 in Bezug auf das Löschungsverbot:

... Diese Frist gilt nicht, wenn einem Löschungsantrag des Auskunftswerbers nach § 27 Abs. 1 Z 2 oder § 28 zu entsprechen ist.

In § 26 Abs. 10 wird das Verfahren für den Fall präzisiert, dass Auskunftsbegehren statt beim richtigen Auftraggeber bei einem Dienstleister oder einem „Auftraggeber mit Dienstleistereigenschaft" eingebracht wird.

§ 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 Abs. 1 Z 3 bis 7 auf einen Verweis auf den Inhalt der Meldung eines bereits registrierten Auftraggebers beschränken, wenn sie eine Teilnahme im genau gleichen Umfang anstreben.*

§§ 50a bis 50e Videoüberwachung

Diese Bestimmungen werden ungekürzt abgedruckt:

§ 50a. Allgemeines

***(1)** Videoüberwachung im Sinne dieses Abschnittes 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.*

***(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 rechtlicher Sorgfaltspflichten, jeweils einschließlich der Beweissicherung, im Hinblick auf Ereignisse nach Abs. 1. Persönlichkeitsrechte nach § 16 ABGB bleiben unberührt.*

***(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 oder die überwachte Person 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.*

§ 50a regelt also in Abs. 2 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 werden folgende Anwendungen unzulässig:

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

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

- Bescheide oder gerichtliche Entscheidungen, die dem Auftraggeber beson-

dere 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).

§ 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 72 Stunden zu löschen. § 33 Abs. 2 AVG gilt. Eine beabsichtigte längere Aufbewahrungsdauer ist in der Meldung anzuführen und zu begründen. In diesem Fall darf die Datenschutzkommission die Videoüberwachung nur registrieren, wenn dies aus besonderen Gründen zur Zweckerreichung regelmäßig erforderlich ist.*

Auffällig ist die kurze Aufbewahrungsdauer von 72 Stunden (die Regierungsvorlage sah überhaupt nur 48 Stunden vor).

Gemildert wird diese relativ kurze Frist allerdings durch die Bezugnahme auf § 33 Abs. 3 AVG, der wie folgt lautet: *„Fällt das Ende einer Frist auf einen Samstag, Sonntag, gesetzlichen Feiertag oder den Karfreitag, so ist der nächste Werktag letzter Tag der Frist“*.

§ 50c. Meldepflicht und Registrierungsverfahren

(1) *Videoüberwachungen unterliegen der Meldepflicht gemäß den §§ 17 ff. Sofern der Auftraggeber nicht in der Meldung zusagt, die Videoüberwachungsdaten zu verschlüsseln und unter Hinterlegung des einzigen Schlüssels bei der Datenschutzkommission sicherzustellen, dass eine Auswertung der Videoaufzeichnungen nur im begründeten Anlassfall durch eine bestimmte Stelle stattfindet, unterliegen sie 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 – ArbVG, BGBl. Nr. 22, Betriebsvereinbarungen abzuschließen sind, sind diese im Registrierungsverfahren vorzulegen.*

(2) *Eine Videoüberwachung ist über § 17 Abs. 2 und 3 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 Verbundenheit in einer Meldung zusammengefasst werden, wenn sich diese auf die gleiche Rechtsgrundlage stützt.*

Auffällig ist vor allem die für den Regelfall vorgesehene Deponierung des Schlüssels bei der DSK. Es ist schwer vorstellbar, dass man bei Vorliegen eines Anlassfalls – das kann jederzeit rund um die Uhr sein – in kürzester Zeit

den Schlüssel von der DSK beschaffen kann. Eine verzögerte Auslieferung des Schlüssels wäre ein geradezu klassischer Amtshaftungsfall, etwa wenn dadurch die Aufklärung eines Einbruchs verhindert wird.

§ 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 im Rahmen der Vollziehung hoheitlicher Aufgaben, die nach § 17 Abs. 3 von der Meldepflicht ausgenommen sind.*

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 oder des Auftraggebers nicht in der in Abs. 1 geregelten Form erteilt werden kann, der Auskunftswerber Anspruch auf eine schriftliche Beschreibung seines von der Überwachung verarbeiteten Verhaltens oder auf eine Auskunft unter Unkenntlichmachung der anderen Personen hat.*

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

Wir halten die Bestimmungen über das Auskunftsrecht für völlig undurchführbar, und zwar aus folgenden Gründen:

- maximal zulässige Aufbewahrungsdauer von 72 Stunden;
- Nachweis der Identität des unbekannten Auskunftswerbers;
- Lokalisierung des Betroffenen auf den Aufzeichnungen.

Vollends absurd wird das Auskunftsrecht dann, wenn nur die DSK den Schlüssel zu den Videoüberwachungsdaten besitzt.

§ 60 Inkrafttreten
§ 61 Übergangsbestimmungen

Die Novelle tritt am 1. Jänner 2010 in Kraft. 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.*

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

Für die Neuorganisation des Datenverarbeitungsregisters (insbesondere in Bezug auf die Online-Meldung) gibt es ebenfalls eine Übergangsbestimmung:

> ***§ 61 Abs. 8**: Die Verordnung nach § 16 Abs. 3 ist vom Bundeskanzler nach Maßgabe der technischen Möglichkeiten des Datenverarbeitungsregisters bis spätestens 1. Jänner 2012 neu zu erlassen. Bis zum Inkrafttreten dieser Verordnung sind die §§ 16 bis 22, § 30 Abs. 3 und 6 sowie § 40 Abs. 1 (letzterer mit Ausnahme des Verweises auf § 31a Abs. 3) in der Fassung vor dem Bundesgesetz BGBl. I Nr. 133/2009 anzuwenden; § 22a, § 30 Abs. 2a und 6a, § 31a Abs. 1 und 2 sowie § 32 Abs. 7 sind bis dahin nicht anzuwenden. § 31 Abs. 3 in der Fassung vor dem Bundesgesetz BGBl. I Nr. 133/2009 ist bis dahin zusätzlich weiter anzuwenden. Die Erklärung, ob eine Datenanwendung einen oder mehrere der in § 18 Abs. 2 Z 1 bis 4 genannten Tatbestände erfüllt (§ 19 Abs. 1 Z 3a), ist der Datenschutzkommission bei im Zeitpunkt des Inkrafttretens der neuen Verordnung nach § 16 Abs. 3 registrierten Datenanwendungen anlässlich der ersten über eine Streichung hinausgehenden Änderungsmeldung zu melden, die nach diesem Zeitpunkt erstattet wird. Eine Meldung allein im Hinblick auf § 19 Abs. 1 Z 3a ist nicht erforderlich.*

Verständlich ist dieser Text natürlich nicht. Es geht hier darum, dass im Registrierungsverfahren die derzeitigen Verfahren weiter verwendet werden, bist das Online-Register funktionsfähig ist und mittels Verordnung eingesetzt werden kann.

Zusammenfassende Stellungnahme

Bedauerlicherweise konnte die verfassungsrechtliche Kompetenzbereinigung im Datenschutzbereich nicht erzielt werden.

Ebenso bedauerlich ist die lange Übergangsfrist für die Erlassung einer neuen DVRV, es ist zu hoffen, dass die zulässigen 2 Jahre nicht ausgeschöpft werden.

••••

Hinweis: Unser Datenschutzseminar findet wieder im Frühjahr 2010 statt.
Der genaue Termin wird noch festgelegt.

Wir wünschen unseren Kunden, Interessenten und sonstigen Lesern
ein erfolgreiches Jahr 2010