DR. THOMAS SCHWEIGER, LL.M. (DUKE)

SCHWEIGER
MOHR &
PARTNER

RECHTSANWÄLTE

DR. DOMINIKUS SCHWEIGER*

DR. THOMAS SCHWEIGER
LL.M. (DUKE)* [1,2,3]

MAG. CHRISTOPH MOHR+

A-4020 LINZ
HUEMERSTRASSE 1 /
KAPLANHOFSTRASSE 2
TEL 0732/796900-0
FAX 0732/ 79 69 06

A-1190 WIEN
MUTHGASSE 36-40
BAUTEIL 4
(SPRECHSTELLE)

OFFICE@S-M-P.AT
WWW.S-M-P.AT

MITGLIED DER
ANWALTSKOOPERATION
ADVOCAT24

©
L|E|X|X
. . . mehr als nur
RECHT

KANZLEIKONTEN:

OBERBANK AG
Bankstelle Ottensheim
4041-0261.49
BLZ 15.013

ALLGEMEINE SPARKASSE
OBERÖSTERREICH BANK AG
0000-060161
BLZ 20.320

ANDERKONTEN:

VOLKSBANK
LINZ+MÜHLVIERTEL
KTO 541 0600 0000
BLZ 43.210

OBERBANK AG
Bankstelle Ottensheim
4041-0265.60
BLZ 15.013

[1] Mitglied der Treuhandrevision
[2] Mitglied des Deutschen Anwaltverein
[3] Mitglied der American Bar Association

ATU 40111204 / DVR: 2112439

*Dr. Schweiger & Partner Rechtsanwälte OG
FN 37294 w LG Linz
Rechnungsleger iSd UStG

in Kooperation mit
+ Mag. Christpoh Mohr, Rechtsanwalt

Bundeskanzleramt
Verfassungsdienst
Ballhausplatz 2
1014 Wien

via Emai: v@bka.gv.at
cc: begutachtungsverfahren@parlament.at

20.5.2008
t
SchwTh/Datenschutzno

Stellungnahme zum Entwurf der DSG-Novelle 2008
182/ME XIII. GP
Bundesgesetz mit dem Datenschutzgesetz 2000 geändert (DSG-Novelle 2008)
Unsere AZ: D/699/76
bitte anführen!

Sehr geehrte Damen und Herren!

Ich habe als Rechtsanwalt, der sich oftmals mit Angelegenheiten des Datenschutzes beschäftigt, auch erfahren, dass das DSG novelliert werden soll und dies im Kreis meiner Mandanten erörtert und besprochen.

Die Mitteilungen und Reaktionen meiner Mandanten sowie meine eigenen Überlegungen als Rechtsberater, der mit diesen Fragestellungen, die auf die Unternehmen und Unternehmer mit der Novelle zukommen, konfrontiert werden wird, haben mich veranlasst, eine Stellungnahme zu verfassen, welche ich Ihnen hiermit zusende:

zu § 1

Richtig ist, dass Österreich dem europaweiten Trend folgt, wenn es den Datenschutz bzw. das Grundrecht des Datenschutzes auf natürliche Personen einschränkt. Andererseits ist festzuhalten, dass in Österreich eine lange Tradition des Datenschutzes auch bei juristischen Personen besteht. Dies sollte beibehalten werden, da sich dieser Schutz durch Materiengesetze und das Datenschutzgesetz über lange Zeit bewährt hat.

Das Argument, dass sich schwerlich argumentieren lässt, dass die personenbezogenen Daten juristischer Personen nicht einer den natürlichen Personen vergleichbaren Schutzwürdigkeit unterliegen, kann nicht im vollen Umfang gelten. Diesbezüglich sei zum Beispiel darauf verwiesen, dass Datenanwendungen mit Vorabkontrolle insbesondere auch Datenanwendungen sind, die die Auskunftserteilung über die Kreditwürdigkeit der Betroffenen zum Zweck haben (§ 18 Z 3 DSG). Hier kann wohl eine Differenzierung zwischen natürlichen Personen und juristischen Personen nicht vorgenommen werden, da insbesondere betreffend die Kreditwürdigkeit von Unternehmen ein Informationsbedürfnis von Lieferanten und Kreditgebern oder Kunden – man denke an Konsumenten im Rahmen des Baunebengewerbe (z.B. Installateur, Küchenlieferant, Innenausstatter) – besteht. Durch die Regelungen des Datenschutzgesetzes wird gewährleistet, dass nur rechtskonform tätige und qualitativ hochwertig arbeitende Wirtschaftsauskunfteien Daten, die zur Beurteilung der Bonität von Unternehmern, juristischen Personen oder auch Privatpersonen ermitteln, verarbeiten und auch Dritten überlassen.

Das Grundrecht auf Datenschutz nach dem Datenschutz ist auch weitgehender als die angesprochenen in den Erläuterungen zur Novelle gesetzlichen Grundlagen zum Schutz von Betriebs- und Geschäftsgeheimnissen. Dieser ist in den Materiengesetzen nur unzureichend geregelt, und bietet das Datenschutzrecht eine wirksame Grundlage zum umfassenden Schutz von Daten von Unternehmen.

Auch kann wohl keine Unterscheidung getroffen werden zwischen Einzelunternehmen, die wohl eine natürliche Person darstellen, und Kapitalgesellschaften. Es sind

jedenfalls Abgrenzungsprobleme zu erwarten, wenn die Umsetzung in der vorgeschlagenen Form erfolgt.

Die bisherige Regelung, dass das Grundrecht auf Datenschutz für natürliche und juristische Personen gilt, sollte beibehalten werden, wobei dies auch andere Teile der Novelle und nicht nur § 1 betrifft.

Weiters bestehen Bedenken, dass die Einschränkung auf „natürliche Personen“ sowohl EU-rechtswidrig (DatenschutzRL 95/46/EG) sowie verfassungswidrig und grunrechtswidrig ist, da Art 8 EMRK nach der Judikatur (EGMR 16.12.1992, Niemietz gg. BRD) auch die juristische Person schützt.

zu § 2

Die Zuständigkeitsvereinfachung bringt sowohl in Gesetzgebung als auch Vollziehung Vorteile und sollte beibehalten werden.

zu § 4

Hier findet sich in der Ziffer 9 ein „Punkt“ anstelle eines „Strichpunktes“.

zu § 8

Hier wird in Absatz 4 eine Ziffer 4 angefügt; diese Bestimmung ermöglicht die Datenweitergabe zum Zwecke der Erstattung einer Anzeige.

Hier besteht die Befürchtung, dass auch widerrechtlich ermittelte Daten an Behörden zur Anzeigeerstattung weitergegeben werden, sodass hier eine Einschränkung jedenfalls notwendig erscheint und zwar in der Form, dass angefügt wird „sofern diese Daten zulässigerweise ermittelt wurden“.

zu § 15 a ff

In dieser Regelung wird der betriebliche Datenschutzbeauftragte normiert. Eine derartige Regelung ist grundsätzlich zu begrüßen. Es besteht jedoch Änderungsbedarf.

1. Betrieb als Anknüpfungspunkt

Die Anknüpfung an den Tatbestand des „**Betriebes**“ im Sinne des § 34 Abs. 1 Arbeitsverfassungsgesetz erscheint nicht zweckmäßig. Danach gilt als „Betrieb“ jede Arbeitsstätte, die eine organisatorische Einheit bildet, innerhalb deren 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 wesentliche Elemente eines Betriebes sind demnach der Betriebsinhaber, die Betriebsmittel, die Beschäftigten und das Vorliegen einer auf Dauer berechneten Tätigkeit, dabei müssen Betriebsmittel und Beschäftigte zu einer organisatorischen Einheit zusammengefasst sein, welcher der Hauptsache nach in dreifacherweise zum Ausdruck kommen muss:

Die Einheit des Betriebsinhabers, in der Einheit des Betriebszweckes und in der Einheit der Organisation (ARB 1881, 8545, 8674, 9453, 10.016; Strasser, Kommentar zum ArbVG 200 ff § 34 Anm. 2.1).

Um von einem “Betrieb“ – als Bestandteil eines Unternehmens – sprechen zu können, muss also der organisatorischen Einheit ein gewisses Mindestmaß an Selbstständigkeit, insbesondere in technischer Hinsicht, eingeräumt sein, und muss das Ergebnis ihres Arbeitsvorganges ein, wenn auch beschränkte, Abgeschlossenheit oder Unabhängigkeit von anderen Betriebsprüfungen aufweisen (ARB 9453, VwSlgNF 8342 a).

Aus dieser allgemeinen Definition im ArbVG sowie den Entscheidungen in der Judikatur ist zu befürchten, dass einzelne Betriebsstätten von großen Unternehmen als „Betrieb“ im Sinne des § 15a Datenschutzgesetz beurteilt werden, so z.B. ein McDonalds-Restaurant.

Sofern diese die festgelegte „**Mitarbeitergrenze**“ überschreiten, wäre für diese „Betriebe“ ein Datenschutzbeauftragter zu bestellen. So könnte zum Beispiel auch eine einzelne Niederlassung einer großen Lebensmitteleinzelhandelskette jeweils einen eigenen Betrieb im Sinne dieser Bestimmung darstellen.

Dies führt aber zu einem unbefriedigenden Ergebnis, wenn man bedenkt, dass die EDV-Systeme, in denen personenbezogene Daten verarbeitet werden, vorwiegend zentral von einer Stelle eines Rechtsträgers (Betriebsinhabers) verwaltet und geführt werden. Das Abstellen auf einen „Betrieb“ im Sinne des § 34 Abs. 1 ArbVG erscheint daher überschießend.

Die Abgrenzung sollte auf einen **Rechtsträger** abgeändert werden, anstelle dass auf den „Betrieb“ Bezug genommen wird.

2. Mitarbeitergrenze

Auch die **Mitarbeitergrenze von 20** (mehr als 20 Stunden beschäftigen) Mitarbeitern erscheint nicht zweckmäßig und praxisgerecht.

Hier sei lediglich auf die Regelung des Bundesdatenschutzgesetzes in Deutschland nämlich § 4 f. dBDSG verwiesen. Danach ist ein Datenschutzbeauftragter dann zu bestellen, wenn *10 oder mehr Personen ständig mit der Bearbeitung personenbezogener Daten mittels elektronischer Datenverarbeitung beschäftigt sind* bzw. 20 oder mehr Mitarbeiter, wenn die Daten manuell verarbeitet werden.

Die Bezugnahme auf eine Mindestanzahl von 20 (mehr als 20 Stunden beschäftigten Mitarbeitern) erscheint in diesem Zusammenhang nicht sachgerecht. Man denke nur an Klein- und Mittelbetriebe, die eine sehr schlanke Verwaltungsstruktur haben, und in denen zum Beispiel der Betriebsinhaber selbst mit ein oder zwei Angestellten die Verwaltung leitet und weitere 20 Personen als Arbeiter tätig sind, z.B. eine Tischlerei oder ein Autohaus oder eine große Fleischhauerei.

Nach dem Buchstaben der Gesetzesnovelle müsste in diesem Betrieb, selbst wenn zum Beispiel nur in der Verwaltung personenbezogene Daten verarbeitet werden, ein Datenschutzbeauftragter bestellt werden.

Die „Mitarbeitergrenze“ sollte sich daher auf Mitarbeiter, die mit der Ermittlung, Bearbeitung, Verarbeitung oder Speicherung beschäftigt sind, beziehen. Nur eine derartige Lösung erscheint auch sachgerecht. Nur die Anzahl der Mitarbeiter als Abgrenzungskriterium zu verwenden, ist in diesem Zusammenhang als nicht sachgerecht zu beurteilen.

3. Person des Datenschutzbeauftragten

Auch die Einschränkung auf „einen geeigneten Mitarbeiter“ erscheint unzweckmäßig.

Auch sei hier wiederum auf das deutsche BDSG verwiesen, wonach auch externe, fachlich qualifizierte Personen berechtigt sind, die Position des Datenschutzbeauftragten in einem Unternehmen wahrzunehmen. Es erscheint zweckmäßiger, hier die Qualifikation des Datenschutzbeauftragten in den Vordergrund zu rücken und dies nicht davon abhängig zu machen, ob er/sie Mitarbeiter im Betrieb ist. Im übrigen wird die Regelung durch den zweiten Absatz des § 15 a insofern eingeschränkt, als dann, wenn kein geeigneter Mitarbeiter der Bestellung zustimmt, eine geeignete betriebsfremde Person oder ein geeignetes Unternehmen bestellt werden kann.

Vorgeschlagen wird hier, die Formulierung in der Form zu ändern, dass diese lautet: *„……..hat eine geeignete Person oder ein geeignetes Unternehmen zum betrieblichen Datenschutzbeauftragten zu bestellen*“. Damit wäre die Wahlfreiheit für die Unternehmen gegeben, eine geeignete Person mit dem vom Gesetz auch geforderten Fachkenntnissen zu bestellen.

4. Betriebsrat und Beteiligung

Die Befassung des Betriebsrates mit der Frage Bestellung eines Datenschutzbeauftragten bzw. dessen Abberufung erscheint systemwidrig. Eine derartige Ausweitung der Kompetenzen des Betriebsrates in einem Materiengesetz ist nicht sachgerecht, da die Regelungen zur Beteiligung der Mitarbeitervertretung in Bezug auf die Organisationsstruktur eines Unternehmens ausschließlich im ArbVG zu finden sind.

Es erscheint auch nicht ganz konsequent die Bestellung von der Beratung mit dem Betriebsrat abhängig zu machen, bei der Abberufung des Datenschutzbeauftragten jedoch keine Beteiligung des Betriebsrates vorzusehen.

5. Aufgabenbereich

Der Aufgabenbereich des betrieblichen Datenschutzbeauftragten, der im § 15 a Abs. 3 beschrieben ist, erscheint ausreichend.

6. Schulung und Beratungszeit

Problematisch erscheint jedoch in diesem Zusammenhang auch die Bestimmung des § 15 Abs. 4.

Wenn eine „geeignete Person“ gemäß § 15a zum Datenschutzbeauftragen zu bestellen ist, dann hat diese Person bereits die Kenntnisse und Fähigkeiten zu haben, die sie sich „im ersten Jahr seiner ununterbrochenen Tätigkeit“ im Rahmen von 40 Stunden bzw. in den Folgejahren 20 Stunden aneignen sollte. Ansonsten wäre die Person wohl nicht qualifiziert, diese Position auszuüben.

Derartige notwendige Fachkenntnisse erscheinen jeweils in Bezug auf die äußerst geringe Grenze (20 Mitarbeiter) als überschießend. Sie belasten die Unternehmen, insbesondere Klein- und Mittelbetriebe zu sehr. Auch ist es nicht möglich, in einem Betrieb, in dem derzeit kein Mitarbeiter über die notwendige Fachkenntnis verfügt, einem Mitarbeiter – der erst geschult werden muss – zum Datenschutzbeauftragten zu bestellten. Auch das spricht dafür, die Bestellung externer Experten bereits in § 15a (1) zuzulassen.

7. Kündigungs- und Entlassungsbeschränkungen

§ 15 a Abs. 5 regelt die Kündigungs- und Entlassungsschutzbestimmung für den betrieblichen Datenschutzbeauftragen. Dies bewirkt, dass in Klein- und Mittelbetrieben ein erhöhter Finanzaufwand gegeben ist, da aufgrund von Kündungsschutz- und Entlassungsschutzbestimmungen die Betriebsinhaber nicht über die Flexibilität verfügen, auf die Anforderungen des Marktes zu reagieren. Auch dies spricht dafür bei der Bestellung auf „eine geeignete Person“ abzustellen.

8. Änderungsbedarf

Übernimmt die Position des betrieblichen Datenschutzbeauftragten ein externer oder ein geeignetes externes Unternehmen, dann ist diese Bestimmung ohnehin hinfällig.

Auch aus diesem Grund sollte den betroffenen Unternehmen jeweils die Möglichkeit gegeben werden, **geeignete externe Personen oder geeignete Unternehmen als betriebliche Datenschutzbeauftragte zu bestellen und mit diesen entsprechende Verträge über die Betreuung abzuschließen**.

Es wäre wünschenswert, dass bezüglich des betrieblichen Datenschutzbeauftragten auch eine Regelung aufgenommen wird, dass **kein Interessenkonflikt** bestehen darf, sodass Personen aus der Geschäftsleitung, leitende Angestellte aus dem Personalwesen oder auch der Abteilung, welche sich mit Informationstechnologie beschäftigt, in der Regel nicht in Frage kommen. Auch hier ist auf die Erfahrung in Deutschland nach dem BDSG zu verweisen. In Deutschland ist der Datenschutzbeauftragte direkt der Geschäftsleitung zu unterstellen und in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden.

Ebenso wünschenswert in diesem Zusammenhang wäre eine Regelung, welche den § 4 f. Abs. 4 dBDSG vergleichbar ist, und zwar das der Beauftragte für den Datenschutz **zur Verschwiegenheit** über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, **verpflichtet** ist, soweit er nicht davon durch den Betroffenen befreit wird. Ebenso sollte eine Regelung betreffend ein **Aussageverweigerungsrecht bzw. Entschlagungsrecht** ähnlich des § 4 f Abs. 4 a dBDSG eingefügt werden.

zu § 16

Hier wird in Abs. 1 b eine Regelung aufgenommen, wonach eine meldepflichtige Datenanwendung erst nach Registrierung einen Betrieb aufnehmen darf. Die bisherige Regelung, nämlich das eine meldepflichtige Datenanwendung bereits nach Abgabe der Meldung aufgenommen werden kann, sollte beibehalten werden, wenn nicht gewährleistet ist, dass die Registrierung innerhalb weniger Tage geschieht.

zu § 19 Abs. 1 Z 8

Hier ist eine Änderung vorzunehmen, sofern in der Regelung des betrieblichen Datenschutzbeauftragten (§ 15 a) eine Änderung erfolgt.

zu 50 a ff - Videoüberwachung

In diesen Bestimmungen ist die Videoüberwachung geregelt. Es ist grundsätzlich begrüßenswert, dass dieses nunmehr in den Medien bereits vielfach diskutierte „Problem“ einer logistischen Lösung zugeführt wird.

Einige Kritikpunkte sind in diesem Zusammenhang jedoch jedenfalls aufzuzeigen.

Die in **§ 50 b** festgelegte **Löschungsroutine** (48 Stunden) entspricht den bisherigen Vorgaben der Datenschutzkommission. Diese sind jedoch zu überdenken, da sie aus Sicht der Praxis zu kurz greift.

Man denke nur zum Beispiel an die Überwachung eines Schalterraumes einer Bank oder wie derzeit vielfach diskutiert der Räumlichkeiten einer Schule über ein möglichweise auch noch verlängertes Wochenende. Die Löschungsroutine bzw. die Dauer der möglichen Speicherung mit 48 Stunden erscheint unter diesen Gesichtspunkten als zu kurz. Wenn man bereits legistisch gestattet, die Videoüberwachung unter bestimmten gesetzlich definierten Voraussetzungen durchzuführen, dann sollte – im Hinblick auf die Protokollierung von Verwendungsvorgängen (§ 50 b Abs. 1) - eine längere Frist definiert werden.

Videoüberwachung von Verhalten, welches darauf gerichtet ist, öffentlich wahrgenommen zu werden, ist genehmigungsfrei zulässig und gewissermaßen aufgrund einer fehlenden Interessensabwägung außerhalb des Rahmens des DSG (neu). Hier sollten Einschränkungen erfolgen, denn dies würde bedeuten, dass derartige Überwachungen ohne Einschränkungen möglich wären, sodass dies sogar hinter den Entscheidungen des OGH 6Ob2401/96y (Überwachung einer Wohnhausanlage) und 7Ob89/97g (Nachbargrundstück mit Kameraattrappen) und den darin festgelegten

Kriterien zurückbleiben würde. In diesem Punkt geht die Novelle in der Regelung der Zulässigkeit von Videoüberwachung zu weit.

Hier sollte z.B. eine Einschränkung in der Form gemacht werden, dass es genehmigungsfrei und ohne Einschränkungen möglich ist, öffentlich zugängliche Bereiche von Geschäfts- und Büroräumlichkeiten mittels Videoüberwachung automationsunterstützt zu überwachen.

Alternativ dazu bestünde die Möglichkeit, derartige Verhaltensweise, die öffentlich wahrgenommen werden können, unter einen geringeren Schutz iSd Datenschutzes zu stellen, ähnlich der Unterscheidung zwischen „normalen personenbezogenen Daten“ und „sensiblen Daten“ oder z.B. die Löschungsroutine bei diesen „Datenarten“ zu verlängern.

Auch die **generelle Weitergabeberechtigung oder –verpflichtung** an die Sicherheitsbehörden, die nunmehr in der Novelle normiert wird, erscheint bedenklich. Bisher ist das DSG davon ausgegangen, dass jede Datenermittlung zweckgebunden ist und die Verwendung für einen anderen Zweck unzulässig ist. Dies wird dadurch massiv und ohne verfassungsrechtliche Normierung eingeschränkt bzw. untergraben.

Auch die **Informationspflicht** ist nicht ausreichend normiert, da sie z.B. entfallen kann, wenn die Beeinträchtigung der Betroffenenrechte unwahrscheinlich ist. Diese Formulierung ist zu vage und entspricht nicht dem bisherigen Standard des DSG, welches mit sehr genauen Definitionen und strikten Formulierungen auskommt. Da es sich beim Datengeheimnis um ein Grundrecht mit gesetzlichen Eingriffvorbehalt hatndelt, ist jede Ausnahme, die im Gesetz normiert ist, einschränkend auszulgen. Unbestimmte Gesetzesbegriffe wie beim Entfall der Informationsverpflichtung, sind daher eher kontraproduktiv, da damit zu rechnen ist, dass diese sehr einschränkend ausgelegt werden könnten. Im Hinblick auf die sehr weitreichenden Befugnisse zur Videoüberwachung erscheint es geboten, jedenfalls die Zulässigkeit auch von einer angemessenen Information der möglichen Betroffenen abhängig zu machen; dies würde den Betroffenen ermöglichen, der Überwachung durch Video zu entgehen, da

sie sich gewissermaßen bewusst entscheiden, „überwacht“ ihren Angelegenheiten z.B. beim Einkauf oder in der Bank nachzugehen.

mit freundlichen Grüßen
Dr. Thomas Schweiger, LL.M. (Duke)