

Stellungnahme

zum „Bundesgesetz,
mit dem das Datenschutzgesetz 2000 geändert wird
(DSG-Novelle 2008)“

Zahl: BKA-810.026/0002-V/3/2008

ZTH Consulting Engineering
Dipl.-Ing. Thomas Hrdinka
Ocworkgasse 22
1210 Wien



Wien, am 25.5.2008

- Leerseite -

ZTH CONSULTING ENGINEERING

IT-Ziviltechniker Dipl.-Ing. Thomas Hrdinka, Staatlich befugter und beeideter Ingenieurkonsulent für Informatik
Ocwirkg. 22
1210 Wien



Email: office@zth.at
Web: www.zth.at



Sehr geehrte Damen und Herren,

als Ziviltechniker für Informatik, täglich mit dem Datenschutzgesetz konfrontiert, übermittle ich Ihnen dringend nötige Vorschläge zur Änderung zum gegenständlichen Entwurf.

Das Datenschutzgesetz ist eine wichtige Basis, auf dem Ziviltechniker für Informatik ihre tägliche Arbeit gründen. Ich sehe im vorliegenden Gesetzesentwurf gravierende Mängel an der Umsetzbarkeit und Zweckmäßigkeit, als auch sollten gerade Ziviltechniker für Informatik im Gesetz als externe Datenschutzbeauftragte erwähnt werden.

Diese Stellungnahme entstand durch freundliche Unterstützung von Dr. Thomas Schweiger (Schweiger · Mohr · Partner Rechtsanwälte, Linz).

Mit freundlichen Grüßen,

ZT Prof. Dipl.-Ing. Thomas Hrdinka

Staatlich befugter und beeideter Ziviltechniker für Informatik,
Allgemein beeideter und gerichtlich zertifizierter Sachverständiger



Erläuterungen zu den einzelnen Bestimmungen:

Ad § 1:

In Österreich besteht eine lange Tradition des Datenschutzes auch bei juristischen Personen. Dies muss beibehalten werden, da sich dieser Schutz durch Materiengesetze und das Datenschutzgesetz über lange Zeit bewährt hat.

Das Argument, dass die personenbezogenen Daten juristischer Personen nicht einer den natürlichen Personen vergleichbaren Schutzwürdigkeit unterliegen, kann nicht nachvollzogen werden. 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 der Kreditwürdigkeit von Unternehmen ein Informationsbedürfnis von Lieferanten und Kreditgebern oder Kunden – man denke z.B. an Konsumenten im Rahmen des Baunebengewerbes – 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 hier bietet das Datenschutzrecht eine wirksame Grundlage zum umfassenden Schutz von Daten von Unternehmen. Juristischen Personen würde auch das Recht auf Richtigstellung von Daten oder Löschung unzulässigerweise verarbeiteter Daten genommen, was vehement abgelehnt werden muss.

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.

ZTH CONSULTING ENGINEERING

IT-Ziviltechniker Dipl.-Ing. Thomas Hrdinka, Staatlich befugter und beeideter Ingenieurkonsulent für Informatik
Ocwirkg. 22
1210 Wien



Email: office@zth.at
Web: www.zth.at

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 grundrechtswidrig sind, da Art 8 EMRK nach der Judikatur (EGMR 16.12.1992, Niemietz gg. BRD) auch die juristische Person schützt.

Ad § 15a ff:

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

1. Betrieb

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 dreifacher Weise 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



Seite 6/12

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 auch einzelne Betriebsstätten von großen Unternehmen als „Betrieb“ im Sinne des § 15a Datenschutzgesetz beurteilt werden.

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 beschäftigten Mitarbeitern erscheint weder als zweckmäßig noch als praxisgerecht.

Hier sei lediglich auf die Regelung des Bundesdatenschutzgesetzes in Deutschland nämlich § 4 f. dBDStG 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 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

ZTH CONSULTING ENGINEERING

IT-Ziviltechniker Dipl.-Ing. Thomas Hrdinka, Staatlich befugter und beeideter Ingenieurkonsulent für Informatik
Ocwirkg. 22
1210 Wien



Email: office@zth.at
Web: www.zth.at

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.

Gemäß dieser Gesetzesnovelle müsste in diesem Betrieb, selbst wenn zum Beispiel nur in der Verwaltung personenbezogene Daten verarbeitet werden, ein eigener Datenschutzbeauftragter bestellt werden.

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

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 dieser ein 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. Schulung und Beratungszeit

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

Wenn eine „geeignete Person“ gemäß § 15a zum Datenschutzbeauftragten 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 von 20 Mitarbeitern 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 bestellen. Auch das spricht dafür, die Bestellung externer Experten bereits in § 15a (1) zuzulassen.

6. Kündigungs- und Entlassungsbeschränkungen

§ 15 a Abs. 5 regelt die Kündigungs- und Entlassungsschutzbestimmung für den betrieblichen Datenschutzbeauftragten. Dies bewirkt, dass in Klein- und Mittelbetrieben ein erhöhter Finanzaufwand gegeben ist, da aufgrund von Kündigungsschutz- und

ZTH CONSULTING ENGINEERING

IT-Ziviltechniker Dipl.-Ing. Thomas Hrdinka, Staatlich befugter und beeideter Ingenieurkonsulent für Informatik
Ocwirkg. 22
1210 Wien



Email: office@zth.at
Web: www.zth.at

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.

7. 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 Wahlfreiheit gegeben werden, geeignete externe Personen oder geeignete Unternehmen als betriebliche Datenschutzbeauftragte zu bestellen und mit diesen entsprechende Verträge über die Betreuung abzuschließen. Beispielhaft wären Ziviltechniker mit einschlägiger Befugnis (wie Informatik) zu fordern.

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 beschäftigen, 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, welches Ziviltechniker gemäß ihrer gesetzlichen Verschwiegenheitsverpflichtung grundsätzlich erfüllen.

ZTH CONSULTING ENGINEERING



Seite 10/12

Ad § 17 Abs 1a:

Die in § 17 Abs 1a der vorgeschlagenen Fassung der DSG-Novelle 2008 ausschließliche Identifizierung und Authentifizierung mittels Bürgerkarte bei Meldungen von Datenanwendungen in elektronischer Form ist abzulehnen.

Gemäß E-GovG ist die Personenbindung einer Bürgerkarte auf natürliche Personen beschränkt. Die Personenbindung einer Bürgerkarte an eine juristische Person ist nicht geregelt. Die Ausstellung von Bürgerkarten an juristischen Personen scheint somit durch das E-GovG nicht gedeckt. Eine Identifizierung und Authentifizierung mit der Bürgerkarte ist juristischen Personen somit unmittelbar nicht möglich.

Zwar wird in § 5 Abs1 E-GovG das vertretungsweise Handeln durch einen mit einer Bürgerkarte ausgestatteten Vertreter (natürliche Person) behandelt, für den Fall, dass ein solcher Vertreter nicht existiert, ist es einer juristischen Person jedoch nicht mehr möglich, eine Meldung in elektronischer Form einzubringen.

Und es sind hauptsächlich gerade juristische Personen, die Datenanwendungen zu melden haben. Offen ist auch die Frage, ob ein in einem Unternehmen beschäftigter Inhaber einer Bürgerkarte überhaupt dazu verpflichtet werden kann, für diesen Zweck seine Bürgerkarte zur Verfügung zu stellen.

Die Vollziehbarkeit des § 17 Abs 1a der vorgeschlagenen Fassung der DSG-Novelle 2008 steht somit zur Gänze in Frage.

ZTH CONSULTING ENGINEERING

IT-Ziviltechniker Dipl.-Ing. Thomas Hrdinka, Staatlich befugter und beeideter Ingenieurkonsulent für Informatik
Ocwirkg. 22
1210 Wien



Email: office@zth.at
Web: www.zth.at

Ad 50 a ff:

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

Einige Kritikpunkte sind in diesem Zusammenhang jedoch aufzuzeigen:

Die in § 50 b festgelegte **Löschungsroutine** von 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 Räumlichkeiten einer Schule über ein möglicherweise verlängertes Wochenende. Die Löschungsroutine bzw. die Dauer der möglichen Speicherung mit 48 Stunden erscheint unter diesen Gesichtspunkten als zu kurz. Wenn man bereits legislativ 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.

ZTH CONSULTING ENGINEERING



Seite 12/12

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 Berechtigung oder Verpflichtung zur Weitergabe 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 verfassungsrechtlicher Normierung eingeschränkt bzw. untergraben.

Auch die Informationspflicht ist nicht ausreichend normiert, da sie z.B. entfallen kann, wenn die Beeinträchtigung der Rechte Betroffener 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 Eingriffsvorbehalt handelt, ist jede Ausnahme, die im Gesetz normiert ist, einschränkend auszulegen. 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.

ZTH CONSULTING ENGINEERING

IT-Ziviltechniker Dipl.-Ing. Thomas Hrdinka, Staatlich befugter und beeideter Ingenieurkonsulent für Informatik
Ocwirkg. 22
1210 Wien



Email: office@zth.at
Web: www.zth.at