

ZENTRALER KREDITAUSSCHUSS

MITGLIEDER: BUNDESVERBAND DER DEUTSCHEN VOLKSBANKEN UND RAIFFEISENBANKEN E.V. BERLIN · BUNDESVERBAND DEUTSCHER BANKEN E.V. BERLIN
BUNDESVERBAND ÖFFENTLICHER BANKEN DEUTSCHLANDS E.V. BERLIN · DEUTSCHER SPARKASSEN- UND GIROVERBAND E.V. BERLIN-BONN
VERBAND DEUTSCHER PFANDBRIEFBANKEN E.V. BERLIN

29. Oktober 2008

Stellungnahme des Zentralen Kreditausschusses zum Referentenentwurf des Bundesministeriums des Innern vom 22. Oktober 2008 für ein „Gesetz zur Änderung des Bundesdatenschutzgesetzes und zur Regelung des Datenschutzaudits“

I. Allgemein

1. Beabsichtigte Maßnahmen gegen den Diebstahl und Missbrauch von personenbezogenen Daten sind nicht hinreichend zielgenau und können datenschutzkonform handelnde Unternehmen benachteiligen

Mit Artikel 1 des Gesetzesvorhabens möchte das Bundesministerium des Innern entsprechend der Datenschutzkonferenz innerhalb der Bundesregierung vom 4. September 2008 und der Stellungnahme des Bundesrates unter Nrn. 16 ff. vom 19. September 2008 (BR-Drs. 548/08) auf im August 2008 festgestellte Diebstähle von personenbezogenen Daten und deren Missbrauch reagieren.

Das Anliegen, solche kriminellen Machenschaften zu unterbinden, ist sehr zu begrüßen. Doch gilt es, hierbei zielgenau vorzugehen. Überzogene Maßnahmen mit breiter Streuwirkung sind abzulehnen, denn damit werden nicht nur die Täter getroffen, sondern auch Wirtschaftsunternehmen, die datenschutzkonform handeln.

Aus Sicht der Kreditwirtschaft ist zunächst festzustellen, dass die bekanntgewordenen Datendiebstähle nicht bei Kreditinstituten stattgefunden haben. Dies belegt, dass Kreditinstitute – wie auch die Mehrheit der Unternehmen aus anderen Wirtschaftskreisen - sehr sorgsam mit personenbezogenen Daten umgehen und die Datensicherheitsvorkehrungen gut funktionieren.

Jedoch sind von den Datendiebstählen in den betroffenen Unternehmen außerhalb der Kreditwirtschaft teilweise auch Kontoverbindungsdaten erfasst worden. Diese Informationen sind weiterverkauft und sodann für unberechtigte Lastschriftziehungen genutzt worden. Solche kriminellen Handlungen sind bereits nach geltendem (Datenschutz-)Recht strafbar. Da es keinen hundertprozentigen Präventivschutz durch Datensicherheitsmaßnahmen geben kann, kommt der Strafverfolgung nicht unerhebliche Bedeutung zu. Soweit in der öffentlichen Diskussion beklagt wird, dass solche Taten mangels Schwere von den Strafverfolgungsbehörden aufgrund begrenzter Ressourcen nicht ausreichend verfolgt werden, kann der Gesetzgeber durch Verschärfung der Strafanandrohung Prioritäten setzen. Eine effektive Aufklärung und strenge strafrechtliche Verfolgung dürfte erheblich dazu beitragen, Datendiebstähle und den Missbrauch dieser Daten zu bekämpfen.

Der vorliegende Referentenentwurf verfolgt aber mit der Streichung des sogenannten Listenprivilegs in § 28 Abs. 3 BDSG und der Schaffung einer neuen Informationspflicht bei festgestellten „Datenpannen“ in § 44a BDSG-E eine generelle Verschärfung des materiellen Datenschutzrechts. Diese Vorgehensweise kann zwar auch die Täter treffen, wird sie aber nicht unbedingt von ihrem Vorhaben abhalten. In jedem Fall würden aber auch alle sich datenschutzkonform verhaltenden Unternehmen betroffen sein. Die Kreditwirtschaft hat deshalb schon vom Grundsatz her deutliche Zweifel, ob die beiden vorgeschlagenen Maßnahmen in dieser Weise wirklich sachgerecht und angemessen sind:

- **Streichung des Listenprivilegs**

Das Listenprivileg lässt nur für einen engen Kreis von Daten eine vereinfachte Übermittlung zum Zwecke des Datenhandels zu, wozu keinesfalls Kontoverbindungsdaten gehören. Das bedeutet, schon nach heutiger Rechtslage ist ein „Handel“ mit Kontoverbindungsdaten unzulässig, wenn nicht die Zulässigkeitsvoraussetzungen aus §§ 4 Abs. 1 und 28 Abs. 1 BDSG erfüllt sind. Mithin dürfte aus Sicht eines Bankkunden die Streichung des Listenprivilegs keine spürbare Verbesserung zur Folge haben. Vielmehr führt die Streichung des Listenprivilegs zur Austrocknung einer bislang legalen Übermittlung von bestimmten Daten zu Werbezwecken, die seit mehreren Jahrzehnten weitgehend problemlos praktiziert wird. Wirtschaftsunternehmen, darunter auch Kreditinstitute, würden damit zukünftig nicht mehr diejenigen Datenquellen zur Verfügung stehen, die sie brauchen, um zielgruppenorientiert sich mittels Werbeschreiben oder ähnlichen Maßnahmen neue Kundenkreise zu erschließen. Angesichts der gesamtwirtschaftlichen Bedeutung des – legalen – Adresshandels schießt die beabsichtigte

Streichung des Listenprivilegs weit über das Ziel hinaus.

- **Informationspflicht bei „Datenpannen“**

Die vorgesehene Informationspflicht beim Abhandenkommen von personenbezogenen Daten folgt einem Trend in den Rechtsordnungen einiger Bundesstaaten in den USA. Aber wird damit nicht das Opfer eines Datendiebstahls übermäßig in die Verantwortung genommen, weil man des Täters nicht habhaft werden kann? Zwar treffen die für die Speicherung der Daten verantwortliche Stelle gewisse Schutzpflichten gegenüber denjenigen, über deren Daten sie verfügt. Doch sollte die von einem Datendiebstahl betroffene Stelle mehr Wahlfreiheit eingeräumt werden, wie sie darauf reagiert. Auch sollte die betroffene Stelle in Bezug auf eine Unterrichtungspflicht von etwaigen Sanktionen bei Nichtbefolgung frei gestellt werden, wenn sie nachweisen kann, dass sie angemessene Datensicherungsmaßnahmen unternommen hat. Denn sie selber ist zuvorderst Opfer und nicht Täter des Datendiebstahls.

2. Koppelung von Missbrauchsbekämpfung und Etablierung eines Datenschutzaudits ist nicht sachgerecht

Das in Umsetzung von § 9a BDSG mit Artikel 2 des Gesetzentwurfs angestrebte Datenschutzauditgesetz wird seit geraumer Zeit kontrovers diskutiert. Dies nun in das Gesetzesvorhaben zur Bekämpfung des Datenmissbrauchs zu integrieren, dürfte aus Sicht der Audit-Befürworter ein willkommenes Vehikel sein. Doch wird mit einer Verknüpfung der Bekämpfung des Datenmissbrauchs mit dem Datenschutzaudit ein unzutreffendes Signal gesetzt. Denn auch ein noch so ausgefeiltes Datenschutzaudit kann es nicht mit hundertprozentiger Sicherheit verhindern, dass personenbezogene Daten gestohlen und missbräuchlich eingesetzt werden. Es wäre irreführend, zu suggerieren, dass nur solche Unternehmen, die sich einem – freiwilligen – Datenschutzaudit unterziehen, am Ehesten datenschutzkonform handeln. Ein solcher Eindruck eines Zwei-Klassen-Datenschutzes muss vermieden werden, denn es würde all diejenigen Unternehmen diskreditieren, die mittels eines guten internen Datenschutzmanagements unter Einsatz des betrieblichen Datenschutzbeauftragten rechtskonform handeln. Vielmehr ist das Datenschutzaudit einer von mehreren Wegen, Datenschutz und Datensicherheit zu gewährleisten.

II. Zu den einzelnen Regelungen des Gesetzentwurfs

1. Artikel 1 Nr. 5 a und b – Neufassung von § 28 Absätze 2 und 3 BDSG: Streichung des Listenprivilegs

a. Datenverarbeitung zu Werbezwecken (§ 28 Absatz 3 Nr. 1 BDSG-E) – Anknüpfung an „eigene Angebote“ zu eng

Zunächst fällt auf, dass der Anwendungsbereich des § 28 Abs. 3 BDSG-E nicht wie bisher nur die Übermittlung betrifft. Vielmehr soll mit der Vorschrift die gesamte Verarbeitung und Nutzung personenbezogener Daten zu den dort genannten Zwecken erfasst werden. Dies mag eine Konsequenz aus der Neuformulierung des § 28 Abs. 2 BDSG-E sein, doch wird damit eigentlich mehr materiellrechtlich verändert, als das Listenprivileg im Bereich der Werbung zu streichen. Schon aus systematischen Gründen ist es vorzugswürdig, in Absatz 3 weiterhin nur die Datenübermittlung zum Zweck des Adresshandels, der Werbung oder der Markt- und Meinungsforschung zu regeln und die Zulässigkeit aller anderen Formen der Verarbeitung zu diesen Zwecken weiterhin in § 28 Absatz 1 BDSG verortet zu lassen.

Sollte gleichwohl das vorliegende Konzept weiterverfolgt werden, ist zunächst sehr zu begrüßen, dass nach § 28 Abs. 3 Absatz 3 Nr. 1 BDSG-E eine Verarbeitung oder Nutzung personenbezogener Daten für Zwecke der Werbung für eigene Angebote oder der eigenen Markt- oder Meinungsforschung der verantwortlichen Stelle ohne eine gesonderte Einwilligung des Kunden zulässig sein soll. Doch greift die Formulierung „für eigene Angebote“ zu kurz. Denn Unternehmen verkaufen Waren und Dienstleistungen durchaus auch als Vermittler, das heißt sie unterbreiten Angebote für Produkte anderer Unternehmen. So ist es gerade das Geschäftskonzept in sogenannten Allfinanzkonzernen und -verbänden, dass das Unternehmen A auch die Produkte des Konzern- bzw. Verbundunternehmens B gegenüber ihren Kunden bewirbt. Zur Veranschaulichung folgende Beispiele:

- Das Kreditinstitut A bietet seinem Kunden die Kreditkarte eines Tochterunternehmens an.
- Das Kreditinstitut A vertreibt selber keine Hypothekarkredite an, möchte aber seine Kunden mit dem Kredit der Hypothekenbank im Konzern/Verbund bewerben.

Auch diese Datennutzung sollte von Nr. 1 erfasst sein, da ein generelles Einwilligungserfordernis nicht sachgerecht wäre. Bei Allfinanzkonzernen bzw. -verbänden ist es sowohl im Interesse von

Bank und Kunde, dass der Kunde Werbeinformationen zu Produkten im Konzern/Verbund erhält. Hierzu ist es aber nicht unbedingt notwendig, die Daten des Kunden an die anderen Unternehmen zu übermitteln, damit diese den Kunden dann ansprechen, womit auch die Einholung einer Einwilligung verbunden wäre. Auch ohne dass die Kundendaten das Kreditinstitut verlassen müssen, kann das Institut den Kunden als Vermittler ansprechen und ihn über die Produkte des Allfinanzkonzerns bzw. -verbunds unterrichten. Würde auch dieser Vorgang zukünftig generell dem Einwilligungserfordernis unterliegen, da es eine Werbung für ein „fremdes“ Produkt wäre, würde der Anreiz für das Unternehmen, die Daten besser im Hause zu halten, entfallen – faktisch würde die Zahl der Datenübermittlungen – legitimiert durch Einwilligungen – erheblich ansteigen.

b. Weitgehende Streichung des Listenprivilegs schießt über das Ziel hinaus, gefährdet seriös und datenschutzkonform handelnde Adresshändler und entzieht Wirtschaftsunternehmen die Möglichkeit der zielgenauen Werbung

Wie oben bereits unter I.1. dargelegt, schießt die beabsichtigte Streichung des Listenprivilegs für Werbezwecke weit über das mit dem Gesetzentwurf verfolgte Ziel hinaus:

- Der „Handel“ mit – entwendeten – Kontoverbindungsdaten ist nicht durch § 28 Abs. 3 BDSG legitimiert. Folglich ist die Streichung des Listenprivilegs zur Missbrauchsbekämpfung zumindest bezüglich Kontoverbindungsdaten nicht erforderlich.
- Die Streichung des Listenprivilegs für Werbezwecke ist unverhältnismäßig. Denn damit würde der bislang legale Adresshandel ganz erheblich eingeschränkt, wenn nicht sogar beseitigt. Dies würde alle Wirtschaftsunternehmen hart betreffen, denn diese nutzen zur Neukundenacquire die Dienstleistungen des Adresshandels, um zielgruppenorientierte Werbung per Brief und anderen Übermittlungswegen betreiben zu können. Gerade für neue Marktteilnehmer wird mit der Austrocknung des bislang legalen Adresshandels eine erhebliche Markteintrittschanke geschaffen. Welche Auswirkungen dies für die gesamte Wirtschaft in Deutschland haben kann, haben bereits u.a. der Zentralverband der deutschen Werbewirtschaft anschaulich vorgetragen.

Am Beispiel der Kreditwirtschaft hat die Streichung des Listenprivilegs folgende

Konsequenzen: Kreditinstitute geben zwar keine Kundendaten zu Werbezwecken an Dritte ohne Einwilligung des Kunden weiter, weil das Bankgeheimnis zu beachten ist. Kreditinstitute nutzen aber zur zielgruppenorientierten Werbung von Neukunden im erheblichem Umfang die Dienstleistungen von legal und seriös arbeitenden Adresshändlern.

Sollten diese Dienstleister nur noch eine deutlich eingeschränkte Datenbasis haben, würde dies für Kreditinstitute bedeuten, dass sie ihre Neukundenwerbung nicht mehr zielgenau im heutigen Umfang fortführen könnten. Um weiter Neukunden gewinnen zu können, müssten sie - wie auch andere Wirtschaftsunternehmen – ihre Werbeaktivitäten im Grunde genommen mit flächendeckenden Postwurfsendungen fortsetzen. Eine solche Umstellung wäre mit deutlich höheren Kosten für das jeweilige Unternehmen verbunden und würde insgesamt zu einer Werbeflut für die Bürger führen. Dieser tiefe Eingriff in die Geschäftstätigkeit von Unternehmen ist auch nicht angemessen, denn es fehlt bislang der überzeugende Nachweis, dass durch Streichung des – seit Jahrzehnten geltenden – Listenprivilegs die Gefahr des illegalen Datenhandels erheblich gemindert würde.

2. Artikel 1 Nr. 5 c – § 28 Abs. 3a BDSG-E: Formelle Anforderungen an die Einwilligung für Datenverarbeitungen nach § 28 Abs. 3 Nr. 2 BDSG-E sind zu streng und nicht erforderlich

a. Anforderungen nach § 4a BDSG reichen aus

Es nicht sachgerecht, mit § 28 Abs. 3a Satz 3 BDSG-E an die Form der Einwilligung für Vorgänge nach § 28 Abs. 3 Nr. 2 BDSG-E über das in § 4a BDSG beschriebene Maß strengere Anforderungen zu stellen. Zum Schutz des Betroffenen reicht es vollkommen aus, in Übereinstimmung mit der geltenden Rechtslage die Einwilligungserklärung bei Verwendung mit anderen Erklärungen besonders kenntlich zu machen. Nun noch zusätzliche Erfordernisse für ein „bewusstes“ Handeln des Betroffenen vorzugeben, ist auch angesichts der Vorkommnisse im August 2008 nicht notwendig. Ein Verstecken von Einwilligungserklärungen in langen Vertragstexten ist bislang schon nach geltendem Datenschutzrecht und auch den zivilrechtlichen Einbeziehungsvoraussetzungen für AGB-Klauseln nicht zulässig. Vielmehr besteht mit der geplanten Sonderregelung die Gefahr, dass der Betroffene durch unterschiedliche Formanforderungen an Einwilligungserklärungen eher verwirrt wird.

Es drängt sich auch der Eindruck auf, dass den Unternehmen die Datenweitergabe zu Werbezwecken mit besonders hohen Anforderungen so schwer gemacht werden soll, dass sie faktisch unterbleibt – also ein Übermittlungsverbot auf indirektem Weg.

b. Konzern- bzw. Verbundklauseln in der Kreditwirtschaft nicht gefährden

Die zusätzlichen Formvorgaben hätten auch erhebliche Auswirkungen auf Unternehmen, die heute schon Einwilligungserklärungen für Datenübermittlungen zu Werbezwecken verwenden, weil sie dies geschäftspolitisch wollen oder aufgrund besonderer Rahmenbedingungen müssen.

So setzen etliche Kreditinstitute heute schon – mit den Datenschutzaufsichtsbehörden im Jahre 1997 abgestimmte - „Konzern-/Verbundklauseln“ ein, wenn sie zu Werbezwecken Kundendaten zwischen selbständigen juristischen Personen im Finanzkonzern oder -verbund austauschen wollen. Um diese Datenübermittlungen im Einklang mit dem Bankgeheimnis zu tätigen, holen die Kreditinstitute von ihren Kunden Einwilligungserklärungen auf Basis der „Konzern-/Verbundklausel“ ein. Die bisherige Erfahrungen in der Kreditwirtschaft zeigen, dass die Kunden eine nach § 4a BDSG gesondert kenntlich gemachte „Konzern-/Verbundklausel“ gut wahrnehmen. Sie machen dabei durchaus von ihrem Recht Gebrauch, diese abzulehnen, wenn sie die Datenweitergabe nicht möchten.

Sollte gleichwohl an § 28 Abs. 3 Satz 3 BDSG-E festgehalten werden, dann müsste in jedem Fall durch eine diesbezügliche Überleitungsvorschrift sichergestellt werden, dass vor dem Inkrafttreten des neuen Gesetzes eingeholten Einwilligungsklärungen weiterhin rechtsgültig bleiben (Bestandschutz). Es wäre vollkommen unverhältnismäßig, wenn diese aufgrund von „Konzern-/Verbundklauseln“ eingeholten und mit den Formvorgaben des § 4a BDSG in Einklang stehenden Einwilligungserklärungen mit viel Aufwand nachträglich angepasst werden müssten, obwohl sie sich seit über 10 Jahren in der Praxis bewährt haben.

3. Artikel 1 Nr. 5 c – § 28 Abs. 3b BDSG-E: Koppelungsverbot greift in Vertragsabschlussfreiheit ein

Das in § 28 Abs. 3b BDSG-E vorgesehene Koppelungsverbot greift übermäßig in die Vertragsabschlussfreiheit ein. Lediglich in monopolähnlichen Situationen oder bei Dienstleistungen der Daseinsvorsorge wäre das Koppelungsverbot unter Abwägung aller Interessen rechtfertigbar.

4. Artikel 1 Nr. 8 b)bb) – § 43 Abs. 3b BDSG-E: Regelung zur Gewinnabschöpfung

Es ist nachvollziehbar, dass der Täter aus seinem Datenschutzverstoß keine Gewinne erwirtschaften soll. Ob dies mittels eines variablen Bußgeldrahmens geschehen kann, ist hinsichtlich der Bestimmtheiterfordernisses von Sanktionen aber fraglich, zumal gemäß § 10 UWG und § 34a GWB auch andere Lösungsmöglichkeiten zur Verfügung stehen.

5. Artikel 1 Nr. 9 – § 44a BDSG-E: Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Wie oben unter I.1. bereits dargelegt, ist die vorgesehene Pflicht des von einem Datendiebstahl oder sonstigen Datenmissbrauchs betroffenen Unternehmens, die hiervon tangierten Betroffenen und die Aufsichtsbehörde zu unterrichten, noch verbesserungsbedürftig:

- **Gleichbehandlung von „Datenpannen“ im öffentlichen und nicht-öffentlichen Bereich**

Irritierend ist zunächst, warum nur Wirtschaftsunternehmen und nicht auch öffentliche Stellen von der Vorschrift erfasst werden. Denn wie gerade beispielhaft Fälle im Vereinigten Königreich belegen (dort sind personenbezogene Daten bei Steuerbehörden, Rentenversicherungsträgern und sonstigen Verwaltungsbehörden abhandelt gekommen), können „Datenpannen“ auch im öffentlichen Bereich vorkommen. Wenn es wirklich für opportun erachtet wird, dem Verantwortlichen der Datenverarbeitung bei Datenverlust Handlungspflichten aufzuerlegen, dann kann es für den Schutz des Betroffenen keinen Unterschied machen, wo der Vorfall stattgefunden hat. Folglich muss die Vorschrift konsequenterweise „Datenpannen“ sowohl im öffentlichen als auch nicht-öffentlichen Bereich gleichermaßen erfassen.

- **Fokussierung auf Bankkontoverbindungsdaten und Kreditkartennummern**

Bei der Aufzählung der Datenarten in § 44a Satz 1 BDSG-E verwundert, dass „Daten zu Bank- oder Kreditkartenkonten“ (Nr. 4) mit besonders sensiblen Daten nach § 3 Abs. 9 BDSG (Nr. 1) oder sogar mit Daten, die einem Berufs- oder Amtsgeheimnis (Nr. 2), unterliegen, gleichgesetzt werden. Zunächst ist die Formulierung in Satz 1 Nr. 4 zu weit gefasst. Sie suggeriert, dass beispielsweise Kontoauszugsdaten von Kreditinstitutskunden

auch bei anderen Unternehmen als Banken vorhanden sind, was generell nicht der Fall ist. Zur Bekämpfung der im August 2008 bekannt gewordenen Missbrauchsfälle würde es völlig ausreichen, den Tatbestand auf „Bankkontoverbindungsdaten und Kreditkartennummern“ zu begrenzen. Bei diesen Daten handelt es sich aber nicht um besonders sensible oder geheimhaltungsbedürftige Daten, denn sie dienen der Abwicklung des Zahlungsverkehrs und werden daher zwischen Gläubiger und Schuldner offen ausgetauscht. Dies müsste zumindest bei der Evidenzschwelle berücksichtigt werden, wann eine Informationspflicht wirklich opportun sein sollte.

- **Evidenzschwelle und Reaktionsmöglichkeiten**

Mit der Vorschrift wird nicht der Datenmissbrauch erschwert oder unterbunden, sondern dem Unternehmen als Opfer einer solcher kriminellen Handlung werden besondere Pflichten zur Schadensbegrenzung auferlegt. Anstatt zwingend in jedem Fall eine Unterrichtung vorzusehen, sollte dem Unternehmen ein Ermessen eingeräumt werden, ob und wie es unterrichtet. Denn die Unterrichtung kann eine von mehreren geeigneten Maßnahmen zur Schadensbegrenzung oder -abwehr darstellen.

Auch kommt der Evidenzschwelle entscheidende Bedeutung zu, wann das Unternehmen zu unterrichten hat. Hierbei sind auch die Erfahrungen aus den USA einzubeziehen: Dort haben Unterrichtungen bei jeder noch so kleinen Datenpanne teilweise dazu geführt, dass die Wahrnehmungsbereitschaft der Betroffenen gesunken ist. Folglich sollte die Unterrichtungspflicht als „ultima ratio“ nur bei schwerwiegenden Sachverhalten greifen.

- **Keine Informationspflicht bei zugriffsgesicherten Daten**

In Bezug auf die Evidenzschwelle der „schwerwiegenden Beeinträchtigung für den Betroffenen“ sollte im Gesetz selber geregelt werden, dass diese nicht vorliegt, wenn zwar die maßgeblichen Daten abhanden gekommen sind, diese aber nach dem Stand der Technik gegen den Zugriff Unberechtigter ausreichend geschützt sind. Dies kann durch Verschlüsselung der Daten und/oder durch Schutzvorkehrungen am betreffenden Datenträger oder Rechner (z.B. Notebook) erfolgen. Denn der Täter hat zwar die Daten, den Datenträger oder den Rechner in den Händen, er kann aber wegen der Schutzmaßnahmen nichts mit diesen anfangen. Eine Informationspflicht ist dann mangels einer Gefährdungslage für die Betroffenen entbehrlich.

- **Keine „Selbstanzeige“**

Wie bereits betont, ist das Unternehmen zunächst selber Opfer eines Datenmissbrauchs. Es sollte daher darauf geachtet werden, dass es zur Schadensbegrenzung mittels der Informationspflicht wirklich motiviert und nicht abgeschreckt wird. Dazu muss sichergestellt sein, dass die Information der zuständigen Aufsichtsbehörde nicht in eine „Selbstanzeige“ mit der automatischen Folge der Sanktionierung mündet. Denn dann könnte ein geschädigtes Unternehmen eher dazu tendieren, die Angelegenheit zu verschweigen, was dem Ziel der Schadensbegrenzung zuwider liefe.

In der Regelung muss daher zum Ausdruck kommen, dass ein Unternehmen sanktionslos bleibt, wenn es nachweisen kann, die Datensicherungsmaßnahmen nach § 9 BDSG im wirtschaftlich vertretbaren Umfang erfüllt zu haben. Dies ist insbesondere dann anzuerkennen, wenn das Unternehmen beispielsweise durch ein sachgerechtes Datenzugriffsmanagement und Einsatz geeigneter Datenverschlüsselungstechniken alles wirtschaftlich und technisch Vertretbare unternommen hat, um der niemals mit letzter Sicherheit auszuschließenden Gefahr des Datendiebstahls zu begegnen. Ein solch datenschutzkonformes Handeln sollte dabei nicht zwingend von einem externen Datenschutzaudit abhängig gemacht werden. Dies würde dem Freiwilligkeitsprinzip des Datenschutzauditgesetzes in Artikel 2 des Gesetzentwurfs zuwiderlaufen. Das Datenschutzaudit kann nicht zum Junktim datenschutzkonformen Unternehmerhandelns gemacht werden.

6. Artikel 2 – Datenschutzauditgesetz

Wie bereits unter I.2 ausgeführt ist eine Koppelung des Datenschutzauditgesetzes (Artikel 2) mit den Regelungen zur Bekämpfung des Datenmissbrauchs (Artikel 1) abzulehnen. Überdies wird das vorliegende Datenschutzauditgesetz sehr kritisch bewertet:

- **Datenschutzsiegel ist nicht generell erforderlich, Gefahr der Schwächung der Institution des betrieblichen Datenschutzbeauftragten**

Die allgemeine Einführung eines Datenschutz-Gütesiegels für alle Arten von datenverarbeitenden Stellen wird als nicht erforderlich abgelehnt. Denn jede

datenverarbeitende Stelle ist verpflichtet, die Datenschutzvorschriften einzuhalten. Der interne Datenschutzbeauftragte und die behördliche Datenschutzaufsicht üben hierzu die notwendige Kontrolle aus. Mit dem Datenschutzauditgesetz besteht die Gefahr, dass die Institution und Bedeutung des betrieblichen Datenschutzbeauftragten erheblich gemindert wird und dies sowohl innerhalb des Unternehmens als auch gegenüber der Datenschutzaufsicht.

- **Ungleichbehandlung von öffentlichem und nicht-öffentlichen Stellen**

Es ist nicht nachvollziehbar, warum nur der nicht-öffentliche Bereich in den Anwendungsbereich des Datenschutzauditgesetzes fallen soll. Wenn diesem Instrument wirklich eine solche Bedeutung zugemessen und auch noch eine Koppelung zur Bekämpfung des Datenmissbrauchs hergestellt wird, wäre es nur konsequent, gleichermaßen den öffentlichen Bereich von dem Gesetz zu erfassen, denn „Datenpannen“ – so die Beispiele im Vereinigten Königreich - können genauso im öffentlichen Bereich vorkommen.

- **Gefahr der fehlleitenden Wirkung**

Die Aussagekraft eines Datenschutz-Gütesiegels ist nicht unproblematisch. Denn es könnte dem Verbraucher den unzutreffenden Eindruck vermitteln, dass eine datenverarbeitende Stelle ohne Siegel sich nicht datenschutzkonform verhält. Insofern birgt ein Gütesiegel die Gefahr der Irreführung und der Schaffung eines Zwei-Klassen-Datenschutzes. Auch ordnungspolitisch stellt sich die Frage, worin der Mehrwert des Gütesiegels bestehen könnte. Denn für Unternehmen könnte dies einen zusätzlichen bürokratischen Aufwand darstellen, der gerade kleinere und mittlere Unternehmen stark belasten würde.

- **Produkt- und Dienstleisteraudit**

Es könnte allenfalls akzeptabel sein, in Umsetzung von § 9a BDSG ein - freiwilliges - Audit-Siegel-Verfahren für bestimmte Bereiche vorzusehen, nämlich für Softwareprodukte, Datenverarbeitungssysteme (Hardware) und Datenverarbeitungsdienstleistungen (z. B. Servicerechenzentrendienstleistungen). Dies könnte für den Nutzer (Unternehmen/Verbraucher) solcher Produkte/Dienstleistungen eine Bewertungs- und Entscheidungshilfe darstellen, um möglichst datenschutzfreundliche Technologien bzw. Dienstleistungen zu nutzen.

- **Unternehmensaudit unrealistisch**

Die Auditierung kann nicht an ein gesamtes Unternehmen anknüpfen, sondern nur an dessen einzelne Prozesse bzw. das von ihm angebotene Produkt oder die von ihm angebotene Dienstleistung. Es dürfte faktisch unmöglich sein, größere Unternehmen mit der Vielzahl der Datenverarbeitungsverfahren alljährlich zu auditieren. Auch muss eine Irreführung verhindert werden, dass ein für ein konkretes Produkt erteiltes Gütesiegel insgesamt den Hersteller als besonders datenschutzfreundlich erscheinen lässt.

- **Akkreditierung der Kontrollstellen**

Die Akkreditierung der Kontrollstelle soll nach dem vorliegenden Entwurf den zuständigen Landesbehörden obliegen. Es bestehen Zweifel, ob die Datenschutzaufsichtsbehörden der Länder die Akkreditierung vornehmen sollten. Zum Einen ist dieser föderalistische Ansatz nicht sachgerecht für bundesweit agierende Unternehmen, denn diese müssen sich darauf verlassen können, dass eine zugelassene Kontrollstelle auch bundesweit von allen Aufsichtsbehörden akzeptiert wird. Zum Anderen könnte die Bestellung durch eine Datenschutzaufsichtsbehörde dazu führen, dass der Auditor zum verlängerten Arm der staatlichen Datenschutzaufsicht wird, weil er faktisch in einem Abhängigkeitsverhältnis zur Datenschutzaufsichtsbehörde stände. Vielmehr sollte der Vorschlag der Arbeitsgemeinschaft für wirtschaftliche Verwaltung (AWV) weiterverfolgt werden, die Gutachterbestellung von der Datenschutzaufsicht zu entkoppeln und anderen Stellen zuzuweisen, beispielweise wie bei der Bestellung von gerichtlichen Sachverständigen den Industrie- und Handelskammern.