Z E N T R A L E R K R E D I T A U S S C H U S S

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

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
16(4)561 A

27. Februar 2009

Stellungnahme des Zentralen Kreditausschusses zum Gesetzentwurf der Bundesregierung für ein „Gesetz zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften“

(BT-Drucksache 16/12011 vom 18. Februar 2009)

I. Allgemein

1. Artikel 1 des Regierungsentwurfs: Datenschutzauditgesetz ist nicht erforderlich und würde den betrieblichen Datenschutzbeauftragten entwerten sowie Zwei-Klassen-Datenschutz begründen

Die in Artikel 1 mit dem Datenschutzauditgesetz-Entwurf beabsichtigte allgemeine Einführung eines Datenschutz-Gütesiegels für alle Arten von datenverarbeitenden Stellen ist nicht erforderlich. 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. Darüber hinaus könnte eine Verselbständigung der Richtlinien des Datenschutzauditausschusses auftreten, die sich auch auf das Verwaltungsermessen der Datenschutzaufsichtsbehörden auswirken könnte. Klare Zuständigkeiten im Bereich der Datenschutzaufsicht würden so verwässert und zu mehr Rechtsunsicherheit führen.

Zudem ist die Aussagekraft eines Datenschutz-Gütesiegels problematisch. 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. 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.

Überdies setzt eine Verknüpfung der Bekämpfung des Datenmissbrauchs mit dem Datenschutzaudit ein unzutreffendes Signal. Selbst ein noch so ausgefeiltes Datenschutzaudit kann nicht mit hundertprozentiger Sicherheit verhindern, dass personenbezogene Daten gestohlen und missbräuchlich eingesetzt werden. Es wäre fehlleitend, zu suggerieren, dass nur solche Unternehmen, die sich einem – freiwilligen – Datenschutzaudit unterziehen, am ehesten datenschutzkonform handeln. Der Eindruck eines solchen 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.

Ferner 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.

2. Artikel 2 des Regierungsentwurfs: Beabsichtigte Maßnahmen gegen den Diebstahl und Missbrauch von personenbezogenen Daten sind nicht hinreichend zielgenau und können datenschutzkonform handelnde Unternehmen benachteiligen

Mit Artikel 2 des Gesetzesvorhabens möchte die Bundesregierung 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, zumal durch den Diebstahl von Kontoverbindungsdaten bei Unternehmen, wie beispielsweise Call-

Centern, auch Bankkunden betroffen gewesen sind. Doch gilt es, bei der Verbesserung des Datenschutzrechts zielgenau vorzugehen. Überzogene Maßnahmen mit breiter Streuwirkung sind abzulehnen, denn damit werden nicht nur die Täter getroffen, sondern auch Wirtschaftsunternehmen, die datenschutzkonform handeln.

Zunächst ist festzustellen, dass Kreditinstitute – wie auch die Mehrheit der Unternehmen aus anderen Wirtschaftskreisen – in der Regel sehr sorgsam mit personenbezogenen Daten umgehen und die Datensicherheitsvorkehrungen gut funktionieren. Zu Tage getretene Schwachstellen bei der Datensicherheit in einzelnen Unternehmen dürfen nicht verallgemeinert werden. Auch darf nicht verkannt werden, dass nach geltendem Datenschutzrecht (§ 9 BDSG) geeignete Sicherheitsvorkehrungen zum Schutz personenbezogener Daten zu treffen sind und die festgestellten Datendiebstähle bereits nach geltendem (Datenschutz-)Recht strafbar sind. Folglich reicht das geltende Datenschutzrecht eigentlich aus. Da es keinen hundertprozentigen Präventivschutz durch Datensicherheitsmaßnahmen geben kann, kommt allerdings 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 Strafandrohung Prioritäten setzen. Eine effektive Aufklärung und strenge strafrechtliche Verfolgung dürfte erheblich dazu beitragen, Datendiebstähle und den Missbrauch dieser Daten zu bekämpfen.

Der vorliegende Gesetzentwurf verfolgt aber mit der Streichung des sogenannten Listenprivilegs in § 28 Abs. 3 BDSG und der Schaffung einer neuen Informationspflicht bei festgestellten „Datenpannen“ in § 42a 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 verhaltende 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 zu weitgehend**

  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 sich zielgruppenorientiert 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“ besser ausrichten**

  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 der von einem Datendiebstahl betroffenen Stelle mehr Wahlfreiheit eingeräumt werden, wie sie darauf reagiert. Auch sollte die betroffene Stelle in Bezug auf eine Unterrichtungspflicht von etwaigen Sanktionen bei Nichtbefolgung freigestellt werden, wenn sie nachweisen kann, dass sie angemessene Datensicherungsmaßnahmen unternommen hat. Denn sie selber ist zuvorderst Opfer und nicht Täter des Datendiebstahls.

3. Stellungnahme des Bundesrates vom 13. Februar 2009 enthält teilweise Änderungsvorschläge zum BDSG, die übermäßig sind, deren Folgen nicht abgeschätzt sind und auch nicht im Einklang mit der EU-Datenschutzrichtlinie stehen

Die Stellungnahme des Bundesrates vom 13. Februar 2009 (BR-Drs. 4/09) enthält zu Artikel 2 des Regierungsentwurfs in einzelnen Punkten Forderungen zu einer deutlichen Verschärfung des Datenschutzrechts, die unangemessen sind. Exemplarisch ist Nr. 4 der Stellungnahme zu nennen, wonach in der Unterrichtungsregelung bei Datenerhebung in § 4 Abs. 3 BDSG der Halbsatz „*sofern er nicht bereits auf andere Weise Kenntnis erlangt hat*“ gestrichen werden soll. Dies würde dazu führen, dass sowohl öffentliche als auch nicht-öffentliche Stellen die Betroffenen flächendeckend mit entsprechenden Hinweisblättern unterrichten müssten, obwohl

diese aus den Umständen oder den Vertragsunterlagen eigentlich ausreichend Kenntnis über die Identität der verarbeitenden Stelle, die Zweckbestimmung der Datenverarbeitung und die Kategorien von Empfängern haben. Überdies steht diese Änderung nicht im Einklang mit Art. 10 der Richtlinie 95/46/EG (EU-Datenschutzrichtlinie), der eine gesonderte Information nur fordert, wenn dem Betroffenen diese nicht schon vorliegt. Insgesamt darf das vorliegende Gesetzgebungsverfahren nicht dafür genutzt werden, an verschiedenen Stellen des BDSG vermeintlich kleine Änderungen mit großen Auswirkungen vorzunehmen, zu denen keine Folgenabschätzung vorliegt. Vielmehr müssten alle die vom Bundesrat zusätzlich angesprochenen Themen sorgsam im Rahmen der von ihm vorgeschlagenen Modernisierung des Datenschutzrechts im Gesamtkontext geprüft und abgewogen werden.

II. Zu den einzelnen Regelungen des Gesetzentwurfs

1. Artikel 1 – Datenschutzauditgesetz

Wie bereits unter I.1 ausgeführt, wird das Datenschutzauditgesetz abgelehnt, da es nicht erforderlich ist, die Stellung des betrieblichen Datenschutzbeauftragten schwächt und einen Zwei-Klassen-Datenschutz begründen würde. Zu einzelnen Regelungen ist Folgendes anzumerken:

a. § 1 DSAG-E - Datenschutzaudit: Begrenzung auf Produkt- und Dienstleisteraudit sowie Ungeeignetheit des Begriffs „Datenschutzkonzept“

Aus den bereits unter I.1. genannten Gründen ist ein Verfahrensaudit nicht notwendig. Vielmehr würde es reichen, ein - freiwilliges - Audit-Siegel-Verfahren nur für bestimmte Bereiche vorzusehen, nämlich für Softwareprodukte, Datenverarbeitungssysteme (Hardware) und Datenverarbeitungsdienstleistungen (z. B. Servicerechenzentrendienstleistungen). Ein Datenschutzsiegel für Produkte und Dienstleistungen könnte für den Nutzer (Unternehmen/Verbraucher) solcher Produkte/Dienstleistungen eine Bewertungs- und Entscheidungshilfe darstellen, um möglichst datenschutzfreundliche Technologien bzw. Dienstleistungen auswählen zu können.

<u>Formulierungsvorschlag</u> § 1 Satz 1 DSAG-E sollte besser wie folgt lauten:

„Nach Maßgabe dieses Gesetzes können
~~1. verantwortliche Stellen ihr Datenschutzkonzept und~~
*~~2.~~ Anbieter von Datenverarbeitungsanlagen, ~~und~~ -programmen **und –dienstleistungen** (informationstechnischen Einrichtungen **und Dienstleistungen**) die angebotenen informationstechnischen Einrichtungen kontrollieren lassen, sofern sie nichtöffentliche Stellen im Sinne des § 2 Absatz 4 des Bundesdatenschutzgesetzes sind. Sie dürfen ~~ihr Datenschutzkonzept oder~~ eine angebotene informationstechnische Einrichtung **und Dienstleistungen** mit einem Datenschutzauditsiegel kennzeichnen, wenn (…)“*

Sollte gleichwohl an dem weiteren Ansatz festgehalten werden, dann ist zu kritisieren, dass nach § 1 Satz 1 Nr. 1 des Gesetzentwurfs ein „Datenschutzkonzept“ der verantwortlichen Stelle auditierbar sein soll. Der Begriff „Datenschutzkonzept“ ist im Datenschutzrecht völlig neu und wird im Text des Datenschutzauditgesetzes nicht definiert. Damit ist der Gegenstand des Datenschutzaudits nach § 1 Satz 1 Nr. 1 des Gesetzentwurfs völlig unbestimmt. Eine solche Unschärfe ist keineswegs sachgerecht, da damit der Aussagegehalt eines Datenschutzsiegels zu einem Datenschutzkonzept unklar ist. Auch ist zu berücksichtigen, dass eine Auditierung nicht an ein gesamtes Unternehmen anknüpfen kann, sondern nur an dessen einzelne Datenverarbeitungen bzw. das von ihm angebotene Produkt oder die von ihm angebotene Dienstleistung. Es dürfte faktisch unmöglich sein, größere Unternehmen mit der Vielzahl im sogenannten Verfahrensverzeichnis nach § 4e BDSG dokumentierten Datenverarbeitungsverfahren vollumfänglich alljährlich zu auditieren. Sollte der Ansatz der Bundesregierung weiterverfolgt werden, generell Datenverarbeitungsverfahren in Unternehmen vom Datenschutzauditgesetz zu erfassen, dann müsste der Gegenstand des Audits auf einzelne, in sich abgeschlossene Teilbereiche der Datenverarbeitung (Beispiel: Datenverarbeitung beim Online Banking) eingegrenzt und eindeutig im Gesetzestext selber festgelegt werden. Das Datenschutzaudit sollte somit nicht auf ein „Datenschutzkonzept“, sondern auf „Datenverarbeitungen“ Bezug nehmen.

Vorschlag (hilfsweise)
In § 1 Satz 1 Nr. 1 DSAG-E sollte statt von „*Datenschutzkonzept*“ von „*Datenverarbeitungen*“ gesprochen werden.

b. §§ 2 bis 4 DSAG-E - Akkreditierung der Kontrollstellen: Verknüpfung von Datenschutzaufsicht mit Akkreditierungsfunktion vermeiden

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. Die Bestellung durch eine Datenschutzaufsichtsbehörde könnte dazu führen, dass der Auditor zum verlängerten Arm der staatlichen Datenschutzaufsicht wird, weil er faktisch in einem Abhängigkeitsverhältnis zur Datenschutzaufsichtsbehörde stände. Um dies zu vermeiden, sollte die Datenschutzaufsicht und die Akkreditierung von Kontrollstellen getrennt werden. So ist beispielsweise im Umweltauditgesetz auch eine Trennung von Aufsicht und „Zulassungsstelle“ vorgesehen (vgl. §§ 28 und 29 Umweltauditgesetz). Die Kreditwirtschaft schließt sich somit dem Vorschlag der Arbeitsgemeinschaft für wirtschaftliche Verwaltung (AWV) an, die Gutachterbestellung von der Datenschutzaufsicht zu entkoppeln und anderen Stellen zuzuweisen, beispielsweise wie bei der Bestellung von gerichtlichen Sachverständigen der Industrie- und Handelskammern.

Vorschlag Die Akkreditierung der Kontrollstellen sollte von anderen hierfür geeigneten Einrichtungen (z. B. Industrie- und Handelskammern) als Datenschutzaufsichtsbehörden wahrgenommen werden.

c. § 6 Abs. 3 Satz 2 DSAG-E – Anzeigepflicht der Kontrollstelle bei der Behörde: Anzeige nur, wenn datenverarbeitende Stelle trotz Aufforderung Verstoß nicht abgeholfen hat

Nach § 6 Abs. 3 Satz 2 DSAG-E soll von der Kontrollstelle jeder Verstoß der dem Audit unterliegenden datenverarbeitenden Stelle gegen § 1 Satz 2 Nummer 1 bis 3 DSAG-E der Aufsichtsbehörde angezeigt werden. Diese Anforderung ist überzogen und auch insgesamt nicht sachgerecht. Denn bei den bereits praktizierten Auditierungsverfahren ist es völlig üblich, dass bei festgestellten Verstößen das betreffende Unternehmen zunächst die Möglichkeit erhält, kurzfristig selber den Mangel abzustellen. Ein solcher Mechanismus trägt dazu bei, dass das Unternehmen den Auditor als sinnvolle und hilfreiche Überprüfungsinstanz wahrnimmt, der etwaige Defizite aufdeckt, aber auch die Möglichkeit der Selbstkorrektur erlaubt. Mithin muss die Anzeige bei der Aufsichtsbehörde eine „ultima ratio“ sein, wenn das Unternehmen den Mangel nicht abstellt.

Formulierungsvorschlag
§ 6 Abs. 3 Satz 2 DSAG-E sollte wie folgt ergänzt werden:
„Stellt eine Kontrollstelle bei ihrer Tätigkeit Verstöße gegen § 1 Satz 2 Nummer 1 bis 3 fest und stellt die kontrollierte Stelle diesen Verstoß trotz schriftlicher Aufforderung nicht binnen einer Frist von drei Monaten ab, unterrichtet sie die zuständige Behörde.“

d. § 8 DSAG-E - Überwachung: Keine hoheitlichen Befugnisse für Kontrollstellen

Mit dem Verweis in § 8 Abs. 5 DSAG-E auf die Überwachungsmöglichkeiten nach § 8 Abs. 1 bis Abs. 4 DSAG-E werden den Kontrollstellen hoheitliche Befugnisse übertragen, wonach ihnen die gleichen Kontrollrechte wie staatlichen Aufsichtsbehörden zugewiesen werden. Es ist verfassungsrechtlich äußerst bedenklich, den Kontrollstellen u. a. nach Abs. 5 i.V.m. Abs. 2 ein Durchsuchungsrecht bei den von ihnen betreuten Unternehmen einzuräumen, denn sie sind keine Hoheitsträger. Auch würde von vornherein das Verhältnis zwischen Auditor und Unternehmen in ein falsches Licht gerückt, was den Zweck eines freiwilligen Auditierungsverfahrens konterkarieren würde. Welches Unternehmen möchte sich schon von einer Kontrollstelle auditieren lassen, die mit Auskunfts- und Durchsuchungsrechten ausgestattet ist, die es ansonsten nur aus der Strafverfolgung und staatlichen Beaufsichtigung kennt.

Vorschlag
§ 8 Abs. 5 DSAG-E sollte gestrichen werden.

2. Artikel 2 des Gesetzentwurfs - Änderung des Bundesdatenschutzgesetzes

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

aa. 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.2. 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 in den im August 2008 bekannt gewordenen Fällen 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 treffen, denn diese nutzen zur Neukundenakquise die Dienstleistungen des Adresshandels, um zielgruppenorientierte Werbung per Brief und auf anderen Übermittlungswegen betreiben zu können. Gerade für neue Marktteilnehmer wird mit der Austrocknung des bislang legalen Adresshandels eine erhebliche Markteintrittsschranke geschaffen. Welche Auswirkungen dies für die gesamte Wirtschaft in Deutschland haben kann, hat 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, da das Bankgeheimnis zu beachten ist. Kreditinstitute nutzen aber zur zielgruppenorientierten Werbung von Neukunden 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.

Vorschlag
§ 28 Abs. 3 BDSG sollte in seiner heutigen Fassung unverändert gelassen werden.

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

Sollte gleichwohl an der Änderung des § 28 Abs. 3 BDSG festgehalten werden, dann sollte Folgendes beachtet werden:

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 Abs. 1 BDSG verortet zu lassen.

Sollte gleichwohl der Ansatz weiterverfolgt werden, mit § 28 Abs. 3 BDSG-E alle Arten der Datenverarbeitung zu erfassen, ist zunächst sehr zu begrüßen, dass nach § 28 Abs. 3 Satz 2 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. Von großer wirtschaftlicher Bedeutung ist aber auch, dass die Daten zudem für fremde Angebote genutzt werden dürfen. 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 -verbünden, dass das Unternehmen A neben eigenen Produkten auch die Produkte des Konzern- bzw. Verbundunternehmens B gegenüber seinen Kunden bewirbt. Zur Veranschaulichung folgende Beispiele:

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

In diesen Fällen wäre ein generelles Einwilligungserfordernis nicht sachgerecht. Bei Allfinanzkonzernen bzw. -verbünden 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.

Um diese Geschäftsmodelle nicht zu gefährden und die Zahl der Datenübermittlungen zukünftig nicht übermäßig zu erhöhen, sollte die bereits im Regierungsentwurf mit § 28 Abs. 3 Satz 4 BDSG-E angelegte Legitimierung der Nutzung von Daten für Werbung auch für Fremdprodukte („Beipackwerbung", vgl. S. 29 der Gesetzesbegründung) zusätzlich in § 28 Abs. 3 Satz 2 Nr. 1 BDSG-E selber verankert werden.

Formulierungsvorschlag

§ 28 Abs. 3 Satz 2 Nr. 1 BDSG-E sollte wie folgt ergänzt werden:
„... für Zwecke der Werbung für eigene und fremde Angebote oder der eigenen Markt- oder Meinungsforschung der verantwortlichen Stelle erforderlich ist, die diese Daten mit Ausnahme der Angabe zur Gruppenzugehörigkeit beim Betroffenen nach § 28 Absatz 1 Satz 1 Nummer 1 erhoben hat, ..."

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

aa. Anforderungen nach § 4a BDSG reichen aus

Es ist nicht sachgerecht, mit § 28 Abs. 3a Satz 2 BDSG-E an die Form der Einwilligung für Vorgänge nach § 28 Abs. 3 Satz 1 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 nach 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.

Vorschlag § 28 Abs. 3a Satz 2 BDSG-E sollte gestrichen werden.

bb. 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 Beratungs- und 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 bisherigen 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 2 BDSG-E festgehalten werden, dann müsste entweder in § 28 Abs. 3 Satz 2 klargestellt werden, dass sich die dort normierten zusätzlichen Anforderungen an eine Einwilligungserklärung nur auf eine elektronisch erteilte Einwilligung beziehen, oder es ist in jedem Fall durch eine diesbezügliche Überleitungsvorschrift sicherzustellen, dass die vor dem Inkrafttreten des neuen Gesetzes eingeholten Einwilligungserklärungen weiterhin rechtsgültig bleiben (Bestandsschutz). 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.

Formulierungsvorschlag

Zum Bestandsschutz bestehender Einwilligungserklärungen sollte die Übergangsregelung in Artikel 2 Nummer 10 (§ 47 BDSG-E) wie folgt ergänzt werden:

„§47
Übergangsregelung

Für die Verarbeitung und Nutzung vor dem 1. Juli 2009 erhobener Daten ist § 28 in der bis dahin geltenden Fassung bis zum 1. Juli 2012 weiter anzuwenden. Für Einwilligungserklärungen des Betroffenen zur Verarbeitung und Nutzung personenbezogener Daten für Zwecke des Adresshandels, der Werbung oder der Markt- oder Meinungsforschung, die vor dem 1. Juli 2009 abgegeben wurden, ist dieses Gesetz in seiner bis dahin geltenden Fassung anzuwenden.“

c. Artikel 2 Nr. 5 e – § 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 könnte das Koppelungsverbot unter Abwägung aller Interessen zu rechtfertigen sein.

Vorschlag
§ 28 Abs. 3b BDSG-E sollte gestrichen werden.

d. Artikel 2 Nr. 8 – § 42a BDSG-E: Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Wie oben unter I.2. 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:

aa. Gleichbehandlung von „Datenpannen“ im öffentlichen und nichtöffentlichen 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 abhanden 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 nichtöffentlichen Bereich gleichermaßen erfassen.

bb. Fokussierung auf Bankkontoverbindungsdaten und Kreditkartennummern

Bei der Aufzählung der Datenarten in § 42a Satz 1 BDSG-E verwundert es, 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 Berufsgeheimnis (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.

cc. Evidenzschwelle und Reaktionsmöglichkeiten

Mit der Vorschrift wird nicht der Datenmissbrauch erschwert oder unterbunden, sondern dem Unternehmen als Opfer einer solchen 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.

dd. 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, kann aber wegen der Schutzmaßnahmen nichts mit diesen anfangen. Eine Informationspflicht ist dann mangels Gefährdungslage für die Betroffenen entbehrlich.

ee. 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 den Einsatz geeigneter Datenverschlüsselungstechniken alles wirtschaftlich und technisch Vertretbare unternommen hat, um der niemals mit letzter Sicherheit auszuschließenden Gefahr des Datendiebstahls zu begegnen. Ein solches datenschutzkonformes Handeln sollte dabei nicht zwingend von einem externen Datenschutzaudit abhängig gemacht werden. Dies würde dem

Freiwilligkeitsprinzip des Datenschutzauditgesetzes in Artikel 1 des Gesetzentwurfs zuwiderlaufen. Das Datenschutzaudit kann nicht zum Junktim datenschutzkonformen Unternehmerhandelns gemacht werden.

Formulierungsvorschlag

Unter Berücksichtigung der o. g. Punkte sollte die Vorschrift wie folgt geändert werden:

*„**(1)** Stellt eine **öffentliche oder** nichtöffentliche Stelle ~~im Sinne des § 2 Absatz 4 oder eine öffentliche Stelle nach § 27 Absatz 1 Satz 1 Nummer 2~~ fest, dass bei ihr gespeicherte*
1. besondere Arten personenbezogener Daten (§ 3 Absatz 9),
2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen oder
*4. personenbezogene **Bankkontoverbindungsdaten und Kreditkartennummern** ~~Daten zu Bank- oder Kreditkartenkonten~~ unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies nach **Absatz 2** ~~den Sätzen 2 bis 5~~ unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen. **Eine Benachrichtigungspflicht besteht nicht, wenn die abhanden gekommenen Daten durch Verschlüsselung nicht von Dritten gelesen werden können oder die verantwortliche Stelle die Beeinträchtigung für die Betroffenen durch geeignete Maßnahmen umgehend beseitigt hat.***

***(2)** Die Benachrichtigung des Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird. Die Benachrichtigung der Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. Die Benachrichtigung der zuständigen Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen enthalten. Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle die Information der Öffentlichkeit durch Anzeigen, ~~die mindestens eine halbe Seite umfassen,~~ in ~~mindestens zwei bundesweit erscheinenden~~ Tageszeitungen.*

(3) Eine Benachrichtigung, die der Benachrichtigungspflichtige erteilt hat, darf in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen ihn oder einen in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen des Benachrichtigungspflichtigen ***nicht zu seinen Lasten*** *~~nur mit Zustimmung des Benachrichtigungspflichtigen~~ verwendet werden.“*

e. Artikel 2 Nr. 9 c)bb) – § 43 Abs. 3 Sätze 2 und 3 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 Bestimmtheitserfordernisse von Sanktionen aber fraglich, zumal gemäß § 10 UWG und § 34a GWB auch andere Lösungsmöglichkeiten zur Verfügung stehen.
