Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Peter Schaar
Bundesbeauftragter für den Datenschutz
und die Informationsfreiheit

Stellungnahme
zum Gesetzentwurf zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften

I. Einleitung

Die Datenschutzvorfälle dieses und des vergangenen Jahres haben drei Kernprobleme des Datenschutzes in der Privatwirtschaft offen gelegt:

1. Die Bürgerinnen und Bürger sind gegenüber den Daten sammelnden Unternehmen weitestgehend machtlos.
Die Unternehmen entscheiden über die Bedingungen, zu denen mit persönlichen Informationen Handel getrieben wird. Gegenüber den Betroffenen werden die massenhaften Datensammlungen und deren Auswirkungen auf die geschäftliche Handlungsfähigkeit des Einzelnen weitgehend verheimlicht. In vielen Fällen werden Informationspflichten missachtet. Selbst dort, wo die Betroffenen informiert werden, verursacht es erheblichen Zeitaufwand, die vielfach sehr umfangreiche Vertragsanlagen oder Datenschutzhinweise zu lesen.

2. Der Datenschutzaufsicht fehlen wirksame Kontroll-, Eingriffs- und Sanktionsinstrumente.
Die Aufsichtsbehörden im Bund und in den Ländern stoßen bei ihren Bemühungen zur Aufklärung und Eindämmung des Datenmissbrauchs an rechtliche und faktische Grenzen. Seit Jahren warnen sie vor den Gefahren der massenhaften Datensammlung und berichten über Datenschutzrisiken. Doch selbst wenn eine Aufsichtsbehörde Datenschutzverstöße in einem Unternehmen aufdeckt (etwa wiederkehrende Datendiebstähle in einem Callcenter), hat sie häufig genug nur die Möglichkeit, diese zu rügen, kann jedoch dem Unternehmen keine Auflagen machen oder die Datenverarbeitung untersagen.

3. Vielen Unternehmen fehlt eine positive Datenschutzkultur.
In weiten Bereichen findet Datenschutz in der Privatwirtschaft nicht statt oder wird als lästige Pflichtübung wahrgenommen. Allenfalls dort, wo Verstöße mit einem öffentlichen Imageverlust einhergehen könnten, bemüht man sich um eine konstruktive Zu-

sammenarbeit mit den Aufsichtsbehörden. Die Datenschutzaufsichtsbehörden werden häufig als Bittsteller betrachtet, Verbesserungen zugunsten des informationellen Selbstbestimmungsrechts lediglich als Bedrohung der wirtschaftlichen Handlungsfreiheit angesehen. Während es zum Allgemeingut gehört, vor dem staatlichen Überwachungswahn zu warnen, sind die Albträume orwellschen Ausmaßes in der Privatwirtschaft längst Realität.

Die Datenschutzvorfälle haben daran bereits eines geändert: den Bürgerinnen und Bürgern haben sie die wirtschaftliche Bedeutung ihrer Daten vor Augen geführt und ihre Hilflosigkeit angesichts des Umgangs mit denselben in der Privatwirtschaft. Es wird nicht mehr davon gesprochen, man „hätte nichts zu verbergen“. Umfragen ergeben: 64% der EU-Bürger sind in Sachen Datenschutz besorgt. In Deutschland stieg der Anteil der besorgten Bürger besonders stark, nämlich in den letzten fünf Jahren von 58% auf 86%. (Eurobarometer, April 2008) Zwei Drittel der Deutschen haben nach einer ARD-Umfrage mittlerweile Angst vor Datenmissbrauch. 95 % wünschen sich daher, dass ihre Daten nur noch mit Zustimmung weitergeben werden dürfen. (infratest dimap 2008)

Dem veränderten technologischen Rahmen und der zugespitzten Risikosituation sollte gesetzlich Rechnung getragen werden:

1. Die Streichung des Listenprivilegs ist verfassungsrechtlich geboten.
Wie der Präsident des Bundesverfassungsgerichts, Professor Dr. Dres. h.c. Papier, kürzlich ausgeführt hat, kann nur so dem Grundrecht auf informationelle Selbstbestimmung im nicht-öffentlichen Bereich hinreichend Geltung verschafft werden. Personenbezogene Daten sind nämlich keine frei verfügbaren Rohstoffe, auf die die Privatwirtschaft nach eigenem Gutdünken zugreifen kann. Personenbezogene Daten, die nicht für Vertragszwecke benötigt werden, sind nicht nur ein Abfallprodukt der Informationsgesellschaft. Den Betroffenen muss die Souveränität über ihre Daten wieder eingeräumt werden.

2. Die Nichtbeachtung von Datenschutzbestimmungen darf nicht länger ein Wettbewerbsvorteil sein.
Es bedarf einer effektiven Datenschutzaufsicht, auch im Interesse der rechtstreuen Unternehmen.

3. Die Einhaltung eines hohen Datenschutzstandards muss sich für Unternehmen lohnen.
Datenschutz darf nicht länger lästige Pflichterfüllung sein. Unternehmen müssen darin gefördert werden, eine positive Datenschutzkultur zu entwickeln und einen hohen Datenschutzstandard als Wettbewerbsvorteil zu begreifen.

Diesen Vorgaben wird der vorgelegte Gesetzentwurf im Ansatz gerecht, bedarf aber an verschiedener Stelle noch der Nachbesserung. Der „Datenschutzgipfel“ am 4. September letzten Jahres hat in der Öffentlichkeit die Erwartung entstehen lassen, dass eine wirksame und zügige Verbesserung des Datenschutzes in der Privatwirtschaft erfolgt. Diese Erwartung sollte nicht enttäuscht werden.

II. Datenschutzaudit

1. Zum Entwurf des Datenschutzauditgesetzes allgemein [Artikel 1 – DSAG-E]

Der Gesetzentwurf beruht auf der Erkenntnis, dass eine nachhaltige positive Veränderung der Datenschutzkultur und damit eine Verbesserung des Datenschutzniveaus in der Privatwirtschaft nicht allein mit der – freilich notwendigen – Verschärfung von Gesetzen und der Stärkung der Datenschutzaufsicht gelingen kann. Vielmehr bedarf es auch der Einführung wettbewerbswirksamer Anreize, damit die Unternehmen ein eigenes Interesse an einer datenschutzgerechten und datenschutzfreundlichen Arbeitsweise haben. Eine transparente und standardisierte Zertifizierung und die Auszeichnung mit einem Gütesiegel für guten Datenschutz soll einen derartigen Anreiz erzeugen.

Insofern geht der vorgelegte Gesetzentwurf in die richtige Richtung. Die an den Zertifizierungen nach dem Öko-Landbaugesetz sowie dem Umweltauditgesetz angelehnte Konzeption folgt einem im Datenschutzrecht völlig neuen Ansatz: So ist geplant, dass ein Unternehmen das Recht erwirbt, ein Gütesiegel zu führen, wenn es sich insbesondere einer permanenten Kontrolle einer Kontrollstelle unterwirft. Anders als beim Datenschutzaudit nach schleswig-holsteinischem Landesrecht, bei dem nach einer erfolgreichen unabhängigen Zertifizierung von einer staatlichen Stelle ein Gütesiegel für eine bestimmte Zeit verliehen wird, dokumentiert das Gütesiegel nach der Grundidee des DSAG-E die dauerhafte Befolgung definierter datenschutzrechtlicher Standards, die entsprechend der technischen Entwicklung dynamisch angepasst werden können. Die vorgesehene Konzeption des Datenschutzaudits enthält darüber hinaus eine Reihe weiterer positiver Ansätze:

- Freiwilligkeit
- Schaffung wettbewerblicher Anreize zur Verbesserung des Datenschutzes
- Vergleichbarkeit der zertifizierten Gegenstände aufgrund der Anwendung transparenter Richtlinien
- Transparenz durch zahlreiche Veröffentlichungspflichten

Auf der anderen Seite erfordert die Umsetzung des vorgesehenen Datenschutzaudits bei den in erster Linie zuständigen Landesbehörden einen nicht unerheblichen bürokratischen Aufwand. Es ist zwar erfreulich, dass der bürokratische Aufwand für die Unternehmen als eher gering anzusehen ist; dem steht allerdings ein umso höherer Aufwand auf Seiten der Verwaltung gegenüber. Zudem lässt der sehr komplizierte Gesetzentwurf an zentralen Punkten große Auslegungsspielräume zu. Schließlich wird durch den Entwurf der für die Akzeptanz des Audits unabdingbare hohe Qualitätsstandard nicht durchgehend gesichert.

2. Verhältnis zwischen Landesbehörden und Kontrollstellen [Artikel 1 (§§ 2, 3 und 16 DSAG)]

Dem Gesetzentwurf ist nicht sicher zu entnehmen, welche Möglichkeiten die Länder bei der Durchführung des Gesetzes haben. Der Wortlaut des Gesetzentwurfs lässt unterschiedliche Konstellationen zu, die sich zum Teil widersprechen.

Insbesondere für den Fall, dass ein Land die Rechtsverordnung nach § 16 Abs. 1 DSAG-E nicht erlässt, ist fraglich, wie das Kontrollsystem von diesem Land organisiert werden kann. So ist nicht klar, ob in diesem Fall eine staatliche Stelle die Aufgaben der Kontrollstelle im Sinne von § 3 DSAG-E wahrnehmen könnte. Sofern der Entwurf die Tätigkeit einer öffentlich-rechtlich verfassten Kontrollstelle ermöglicht, stellt sich die weitere Frage, wie diese in das auf private Kontrollstellen zugeschnittene System des Gesetzentwurfs integriert werden kann. Eine Zulassung durch den BfDI oder gar deren Entzug wäre z. B. aus kompetenzrechtlichen Gründen ausgeschlossen.

Umgekehrt ist Inhalt und Umfang der Beleihung einer privaten Kontrollstelle nach § 16 Abs. 1 DSAG-E nicht klar. Der Wortlaut würde es auch ermöglichen, dass eine private Kontrollstelle Überwachungsaufgaben nach den §§ 7, 8 DSAG-E ausübt und damit andere ebenso private Kontrollstellen beaufsichtigt.

Insgesamt ist das Verhältnis zwischen Kontrollstelle nach § 3 DSAG-E und zuständiger Behörde nach § 2 Abs. 1 DSAG-E klarer zu formulieren. Dabei ist insbesondere der Inhalt und Zweck des in § 3 DSAG-E enthaltenen Verordnungsvorbehalts eindeutig zu fassen.

3. Kontrolldichte
[Artikel 1 (§ 3 DSAG)]

§ 3 DSAG-E bietet i. V. m. § 9 DSAG-E die Möglichkeit, dass ein Unternehmen die Befugnis erhält, ein Gütesiegel zu führen, sobald es sich formal der Kontrolle der Kontrollstelle unterworfen und die übrigen Bedingungen des § 1 Satz 2 DSAG-E formal erfüllt hat. Eine tatsächliche erstmalige Kontrolle muss nach dem Gesetzentwurf erst stattfinden, „sobald der ordnungsgemäße Geschäftsbetrieb“ dies ermöglicht.

In der Praxis würde dies bedeuten, dass ein Unternehmen mit einem Gütesiegel werben und den daraus resultierenden Wettbewerbsvorteil erzielen kann, obwohl es u. U. keine der in § 1 Satz 2 DSAG-E genannten Anforderungen erfüllt. Es genügt die bloße Anzeige eines Datenschutzkonzepts oder einer informationstechnischen Einrichtung beim BfDI verbunden mit der Erklärung, die materiellen Anforderungen zu erfüllen, um bereits das Gütesiegel führen zu dürfen. Der BfDI hat in diesem Zusammenhang keine Prüfungskompetenz hinsichtlich der tatsächlichen Qualität des angezeigten Gegenstands. Das zum Vorbild genommene Kontrollverfahren im ökologischen Landbau enthält eine solche Einschränkung im Übrigen nicht.

Das im Gesetzentwurf vorgesehene Verfahren würde daher Gefahr laufen, das Vertrauen in die Qualität des Datenschutzaudits nachhaltig zu erschüttern. Zum einen ist der Zeitraum, den eine Kontrollstelle benötigt, um ihre Arbeitsfähigkeit herzustellen, im Gesetzentwurf nicht begrenzt. Eine beabsichtigte oder unbeabsichtigte Nichtherstellung der Arbeitsfähigkeit ist zudem nicht sanktioniert. Es wäre also möglich, dass über längere Zeit die Erstkontrolle nicht stattfindet, da für deren Durchführung – anders als bei den Zweit- und weiteren Kontrollen – keine absolute Frist gesetzt ist. Darauf zu vertrauen, dass sich die Unternehmen rechtstreu verhalten und nur dann ein Datenschutzkonzept oder eine informationstechnische Einrichtung beim BfDI anzeigen, wenn alle Voraussetzungen erfüllt sind, erscheint angesichts der Datenschutzvorfälle der vergangenen Monate realitätsfern. Es ist vielmehr damit zu rechnen, dass gerade im schnelllebigen Internetbereich Unternehmen missbräuchlich das Gütesiegel führen, die bereits vor der Erstkontrolle nicht mehr existieren. Zudem kann anschließend das gleiche Geschäftsmodell mit einem neuen Unternehmen fortgeführt und dabei wieder das Gütesiegel verwendet werden.

Es ist daher dringend anzuraten, gesetzlich vorzusehen, dass das Gütesiegel erst dann geführt werden darf, wenn die Erstkontrolle durchgeführt wurde und die nicht-öffentliche Stelle die Anzeige nach § 9 Abs. 1 DSAG-E beim BfDI erstattet hat. Zu empfehlen wäre außerdem,

dass die Sicherstellung des ordnungsgemäßen Geschäftsbetriebs der Kontrollstelle auch in den Katalog der Zulassungsvoraussetzungen in § 4 DSAG- E aufgenommen wird.

Unabhängig von der Erstkontrolle wird die Kontrolldichte auch im Übrigen nicht dem Anspruch an einen hohen Qualitätsstandard beim Audit gerecht. Art und Häufigkeit der Kontrollen sollten sich nicht allein am Risiko des Auftretens von Verstößen orientieren, sondern angesichts der hohen Innovationsdichte in der Informationstechnik auch daran, was nach dem Stand der Technik geboten ist. Zudem ist die Mindestkontrolldichte von 18 Monaten ab der dritten Kontrolle aus den gleichen Gründen zu lang.

4. Untersagung der Kennzeichnung mit dem Gütesiegel [Artikel 1 (§ 7 Abs. 2 DSAG)]

Nach dem Wortlaut des § 7 Abs. 2 DSAG-E kann die Kennzeichnung mit einem Gütesiegel durch die zuständige Behörde nur dann untersagt werden, wenn sie von der Kontrollstelle über Verstöße unterrichtet worden ist. Erfährt die zuständige Stelle auf einem andern als diesem formal vorgesehenen Wege von Verstößen, ist eine Untersagung nicht vorgesehen. Diese Rechtsunsicherheit ist ebenfalls geeignet, die Qualität des Datenschutzaudits zu beeinträchtigen.

Es muss deshalb klargestellt werden, dass die Kennzeichnung mit dem Gütesiegel immer dann untersagt werden kann, wenn die materiellen Voraussetzungen für die Untersagung gegeben sind. Woher die Anhaltspunkte und Beweise für Verstöße kommen, spielt hierfür keine Rolle.

5. Stellung des Datenschutzauditausschusses [Artikel 1 (§ 15 DSAG)]

Obwohl der Datenschutzauditausschuss unabhängig ist (§ 12 Abs. 1 Satz 2 DSAG-E), unterliegt er einer sehr weitgehenden Rechtaufsicht durch das BMI. Zweifel bestehen hier insbesondere im Hinblick auf die Möglichkeit der Ersatzvornahme. Es besteht das Risiko, dass das BMI als Rechtsaufsicht im Wege der Ersatzvornahme selbst Richtlinien in Kraft setzt, obwohl es nicht über die gleiche fachliche Kompetenz verfügt wie der mit Spezialisten besetzte Ausschuss. Dies birgt die Gefahr, dass das Vertrauen in den fachlichen Wert der Richtlinien beeinträchtigt wird.

Deshalb wäre zu überlegen, ob als schärfste Aufsichtsmaßnahme eine Aufhebung von Beschlüssen in Betracht kommt, eine Ersatzvornahme jedoch ausgeschlossen wird. Praktisch hätte dies zur Folge, dass es z. B. eine bestimmte Richtlinie nicht gibt und ein hierauf bezogenes Datenschutzaudit nicht stattfinden kann. Dieses Ergebnis wäre einem Auditverfahren auf der Grundlage einer vom BMI im Wege der Ersatzvornahme in Kraft gesetzten Richtlinie vorzuziehen.

III. Änderung datenschutzrechtlicher Vorschriften

1. Stärkung des betrieblichen und behördlichen Datenschutzbeauftragten [Artikel 2 Nummer 2 (§ 4f Absatz 3)]

Der erweiterte Kündigungsschutz für den betrieblichen und behördlichen Datenschutzbeauftragten ist neu und ein sinnvoller Vorschlag zur Stärkung der Position des Beauftragten. Es hat sich in der Praxis gezeigt, dass über den Weg der Kündigung die Unabhängigkeit des Beauftragten stark gefährdet werden kann.

Hinsichtlich der Anforderungen an die erforderliche Fachkunde beschränkt sich die Regelung auf die Verpflichtung, die Teilnahme an Fort- und Weiterbildungsmaßnahmen zu ermöglichen und zu finanzieren. Dies ist keine wesentliche Verbesserung, kann dies doch zum Teil bereits heute dem Gesetze entnommen werden. Dort jedoch, wo eine gesetzgeberische Klärung sinnvoll gewesen wäre, nämlich der konkreten fachlichen Anforderungen an die Art der zu erwerbenden Qualifikationen (wie etwa beim betrieblichen Sicherheitsbeauftragten), schweigt der Entwurf.

2. Streichung des Listenprivilegs [Artikel 2 Nummer 5 (§ 28)]

Die Streichung des Listenprivilegs und die Einführung der Einwilligungslösung ist das richtige Signal, um das Selbstbestimmungsrecht der Bürgerinnen und Bürger in der Privatwirtschaft zu stärken.

Nach § 28 Abs. 3 Nr. 3 BDSG dürfen bestimmte personenbezogene Daten für Zwecke der Werbung sowie der Markt- und Meinungsforschung derzeit genutzt und übermittelt werden, solange die Betroffenen nicht widersprechen. Dieses Listenprivileg ist mit erheblichen Gefahren für den Betroffenen verbunden, denn die auf diesem Weg privilegierten personenbezogenen Daten lassen sich nicht ohne weiteres von weiteren Datensammlungen isolieren. Insbesondere lässt sich der Informationsgehalt mit Hilfe der Angabe steuern und variieren, die es ermöglicht, die Zugehörigkeit zu einer bestimmten, den Übermittlungsadressaten interes-

sierenden Personengruppe zu finden. Mit der Übermittlung der Listendaten können Zusatzinformationen verbunden sein, die weit über das vom Gesetzgeber akzeptierte Informationsspektrum hinausreichen. Damit geht diese Norm über die Problematik unerwünschter Werbung hinaus, sie ist der Einstieg in die Möglichkeiten der heimlichen Profilbildung.

Eine Widerspruchslösung bürdet demgegenüber das Risiko einer illegalen Datenweitergabe allein den Betroffenen auf. Sie haben zwar in der Theorie ein Widerspruchsrecht, fürchten aber häufig einen schlechteren Service oder sonstigen Malus bei den Unternehmen, wenn sie diesen das Datensammeln untersagen. Zudem wird es den Betroffenen nicht immer leicht gemacht, diesen Widerspruch auch auszuüben. Häufig bedarf es erst des Einschaltens der zuständigen Datenschutzaufsichtsbehörde, um die verantwortliche Stelle zu einem rechtskonformen Verhalten zu veranlassen.

Die nun vorgeschlagene Regelung schafft einen angemessenen Ausgleich zwischen den Interessen der werbenden Unternehmen und den Betroffenen. Nach wie vor wird die Direktwerbung möglich sein, zudem werden sich neue Werbeformen entwickeln. Es wird von ihrer Seriosität abhängen, ob und inwieweit es gelingt, von den Bürgerinnen und Bürgern eine Einwilligung zu erhalten. Das Beispiel der Kundenkartensysteme belegt, dass eine Vielzahl von Bürgerinnen und Bürgern durchaus bereit ist, ihr Konsumprofil nutzbar zu machen.

Adressierte Werbung ist danach in den folgenden Konstellationen möglich:

1. Die eigenen Kundinnen und Kunden können weiter beworben werden wie bisher.
   Beispiele:
   - Versandhändler können weiterhin ihre Kundenbeziehungen pflegen.
   - Telefonunternehmen können über die neuesten Tarife informieren.
   - Handwerkskammern können ihre angeschlossenen Mitglieder bewerben.
2. Daten von sonstigen Personen dürfen grundsätzlich nur für Werbezwecke verwendet werden, wenn sie zuvor in die Übermittlung ihrer Daten eingewilligt haben.
   - Aber: Haushaltsbefragungen, Kundenbindungssysteme oder Informationsanforderungen von Verbrauchern bleiben erlaubt
3. Gezielte Internetwerbung (Targeting) bleibt weiterhin möglich
   - Das Telemediengesetz erlaubt es den Anbietern von Telemedien, für Zwecke der Werbung und Marktforschung Nutzungsprofile bei Verwendung von Pseudonymen zu erstellen, soweit die Nutzerinnen und Nutzer dem nicht widersprechen. Daran soll sich nichts ändern.
4. Parteienwerbung
   - Parteienwerbung bleibt wegen der Privilegierung im Melderecht über eine Melderegisterauskunft möglich.

5. Werbung gegenüber Freiberuflern und Gewerbetreibenden (B2B) bleibt möglich
   - Angaben auf Messen o.ä. Veranstaltungen können für Werbeansprache genutzt werden.

6. Beilage von Werbeprospekten anderer Unternehmen zur eigenen Geschäftspost
   Beispiele:
   - Zeitungsverlag kann Werbung für passende Angebote beilegen, also etwa die Motorradzeitschrift besondere Konditionen beim Motorradausstatter anbieten.
   - Versicherungsunternehmen können Prospekte verbundener Unternehmen oder Kooperationspartner (Banken etc.) wie bisher beilegen.

7. Werbung anerkannter Spendenorganisationen
   Beispiel
   - Spendenorganisationen sollen weiterhin wie bisher listenmäßig zusammengefasste Daten nutzen können.

Es ist richtig, dass sich durch die veränderten Rahmenbedingungen Werbung in Zukunft stärker an den Interessen der Verbraucherinnen und Verbraucher ausrichten muss. Dies ist aber gerade die Chance für Unternehmen, durch einen verantwortungsvollen Umgang mit den Daten der Verbraucherinnen und Verbraucher deren Vertrauen zu gewinnen. So funktionieren viele Kundenbindungssysteme schon seit Jahren erfolgreich auf der Basis des Einwilligungsprinzips. Direktmarketing ist zudem vor allem eine Strategie von deutschlandweit tätigen Großunternehmen oder Versandhändlern. Diese kennen ihre Kundinnen und Kunden nicht. Kleine und mittelständische Unternehmen hingegen haben bereits von ihrer Struktur her den Vorteil einer stärkeren Kundenbindung. Ihnen stehen daher die klassischen Werbeformen näher als das Direktmarketing in Form adressierter Werbeschreiben. Sie können ihre Kundinnen und Kunden tatsächlich direkt ansprechen. Umgekehrt haben sich andere Formen der Kundenbindung entwickelt, insbesondere die Kundenkartensysteme, mit denen große Unternehmen diese Schwäche ausgleichen.

Besonderer Bedeutung kommt dabei der Form der Einwilligung zu. Die Tragweite der Einwilligung muss den Betroffenen klar vor Augen geführt werden. Erfolgt die Einholung der Einwilligung daher im Zusammenhang mit anderen Erklärungen, so ist ein besonderes Tätigwerden des Betroffenen erforderlich. Er muss etwa durch Ankreuzen oder durch eine gesonderte Unterschrift zweifelsfrei zum Ausdruck bringen, dass er die Einwilligung bewusst erteilt. In Zukunft werden es der Betroffene ein Stück weit mehr in der Hand haben, inwieweit Unternehmen Daten über ihn sammeln. Dies bedingt jedoch, dass jeder sich der Konsequenzen seines Tuns auch klar wird und insbesondere zweifelsfrei seinen Willen zur Einwilligung bekundet. Hierfür genügt es nicht, bei den bisherigen Anforderungen des Gesetzes zu bleiben. Richtig ist, dass für diesen Bereich die Form der Einwilligung damit verschärft wird. Angesichts der Gefahr, dass ohne diese Verschärfung jedoch das Einwilligungserfordernis durch pauschale Formulierungen konterkariert wird, ist dies eine notwendige Maßnahme. Sinnvoll wäre es

jedoch, dies zum Anlass zu nehmen, die Form der Einwilligung in § 4a BDSG, die auch in anderen Zusammenhängen datenschutzpolitisch fragwürdig geworden ist, insgesamt zu überarbeiten.

Die von Wirtschaftsverbänden vorgeschlagenen Alternativen zur Einführung der Einwilligungslösung, insbesondere die Privilegierung auditierter Unternehmen, sind nicht geeignet, das geplante Ziel, den Datenschutz in der Privatwirtschaft zu stärken, zu erreichen. Gerade das geplante Datenschutzaudit soll dazu dienen, herausragende, besonders datenschutzfreundliche Verfahren und Konzepte auszuzeichnen. Es soll kein flächendeckender, privatwirtschaftlich getragener Ersatz einer Datenschutzaufsicht sein. Das Bio-Siegel ersetzt schließlich auch keine Hygienemittelkontrolle. Es wäre zudem für die Verbraucherinnen und Verbraucher geradezu absurd, wenn sie bei auditierten, und damit besonders prämierten, Unternehmen einen schlechteren Datenschutz befürchten müssten, weil diese Unternehmen ihre Daten weiterhin ohne ihre Zustimmung weiterverkaufen dürften, was ansonsten unzulässig wäre. Das Audit wäre insofern eine Prämierung einer objektiv schlechteren Datenschutzpraxis.

Die vorgesehene Einwilligungslösung ist zudem mit Europarecht vereinbar. Nach der EG-Datenschutzrichtlinie ist bei der Nutzung von personenbezogenen Daten zu Zwecken der Werbung eine Widerspruchslösung (opt-out-Modell) die Mindestanforderung an den nationalen Gesetzgeber. Diesem bleibt es aber im Interesse der Verbraucherinnen und Verbraucher unbenommen, schärfere Anforderungen zu stellen, insbesondere dann, wenn die Widerspruchslösung – wie hier – in der Praxis versagt hat.

3. Einführung eines Koppelungsverbots [Artikel 2 Nummer 5 (§ 28 Absatz 3b – neu –)]

Die Einführung des aus dem Telekommunikationsrecht bekannten Koppelungsverbotes ist eine sinnvolle Ergänzung, die insbesondere die Freiwilligkeit der erteilten Einwilligung sicherstellen soll. Der Abschluss eines Vertrages darf nämlich nicht davon abhängig gemacht werden, dass der Betroffene in die Weitergabe seiner persönlichen Daten an Dritte zu Werbezwecken einwilligt. Es besteht jedoch die Gefahr, dass die vorgeschlagene Regelung in der Praxis nicht greifen wird, da sie auf marktbeherrschende Unternehmen beschränkt ist.

Hinter der Formulierung, dass gleichwertige vertragliche Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise vom Betroffenen in Anspruch genommen werden können, verbirgt sich die Überlegung, dass es im freien Wettbewerb immer Unternehmen geben wird, die eine gleichwertige Leistung anbieten, ohne die Preisgabe von nicht für die Vertragserfüllung notwendigen, mithin überflüssigen persönlichen Daten zu verlangen. Es obliegt dann dem Betroffenen herauszufinden, welche Anbieter dies sein könnten. Dies bedeutet, dass es nur marktbeherrschenden Unternehmen verboten ist, die Preisgabe von überflüssigen personenbezogenen Daten zu verlangen. Nur in diesem Fall besteht für den Betroffenen aufgrund der Marktbeherrschung keine Möglichkeit der Alternative. Nach der Rechtssprechung war

jedoch bisher selbst ein Unternehmen wie Ebay, das bei Online-Auktionen einen Marktanteil von 70 % hat, nicht marktbeherrschend. Daher dürfte diese Regelung nicht geeignet sein, eine unzulässige Koppelung selbst bei denjenigen Unternehmen zu verbieten, die nach Sicht der Betroffenen eine marktbeherrschende Stellung einnehmen.

Das Koppelungsverbot sollte daher nicht auf marktbeherrschende Unternehmen beschränkt werden.

4. Einführung einer Informationspflicht bei Datenschutzverstößen in der Privatwirtschaft [Artikel 2 Nummer 8 (§ 42a – neu –), Artikel 3 Nummer3 (§ 15 a TMG – neu –) sowie Artikel 4 Nummer 1 (§ 93 Absatz 3 TKG – neu –]

Die Informationspflicht kann dazu beitragen, die Datenschutzkultur in Unternehmen zu fördern. Sie sollte sich aber auch auf öffentliche Stellen erstrecken und nicht auf bestimmte Datenarten beschränkt werden. So dürfte nicht vermittelbar sein, weshalb bei öffentlichen Stellen im Falle des Verlusts von personenbezogenen Daten nicht ähnliche Risiken bestehen, wie im nicht-öffentlichen Bereich.

Zudem greift die vorgesehene Informationspflicht nur bei bestimmten Datenarten und nur dann ein, wenn das betroffene Unternehmen zu dem Ergebnis gelangt, dass von dem Datenverlust schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen ausgehen können. Damit sind jedoch eine Vielzahl von Fällen gerade des Identitätsmissbrauchs nicht von der Informationspflicht umfasst. Seit einigen Jahren wird die Zunahme der Internetkriminalität und insbesondere des Identitätsmissbrauchs beklagt. Die unbefugte Weitergabe von Daten ist eine Quelle dieser Kriminalität. Daher ist der Verlust von Daten per se keine Bagatelle mehr, sondern muss von jeder Behörde und jedem Unternehmen grundsätzlich daraufhin überprüft werden, ob hiervon Gefahren für die Betroffenen ausgehen. Die Einführung einer Informationspflicht nur für spezielle Verluste einiger als besonders gefährdet eingestufter Daten sendet hier das falsche Signal. Umgekehrt könnte die erhöhte Informationspflicht dann über ein zweistufiges Informationsverfahren aufgefangen werden.

5. Erweiterung des Bußgeldkatalogs/Stärkung der Aufsichtsbehörden [Artikel 2 Nummer 9 (§ 43)]

Die Bußgeldtatbestände des § 43 BDSG weisen bisher nicht unerhebliche Lücken auf. Die nun vorgesehene Erweiterung ist daher zu begrüßen, da mit ihr auch die Einwirkungsbefugnisse der Datenschutzaufsichtsbehörden gestärkt werden und das Vollzugsdefizit gemindert werden kann.

Jedoch sind diese Maßnahmen noch nicht hinreichend. So stimmt es wenig zuversichtlich, wenn der illegale Handel mit 6 Millionen Adressdaten (wie im Sommer 2008 in Schleswig-Holstein) gerade einmal zu einem Bußgeld von 900 Euro geführt hat, woran auch die Novelle nichts ändern würde. Es ist daher notwendig, die Aufsichtsbehörden angemessen auszustatten. Damit ist nicht nur eine angemessene personelle und finanzielle Ausstattung gemeint, auch das Instrumentarium der Aufsichtsbehörden muss erweitert werden. Gefahrenabwehr können Datenschutzbehörden bislang nur bei festgestellten technischen und organisatorischen Mängeln nach § 9 BDSG, nicht aber bei den oftmals erheblich schwerwiegenderen materiell rechtlichen Datenschutzverstößen treffen. Erforderlich ist daher, § 38 Abs. 5 BDSG um die Möglichkeit zu erweitern, Anordnungen und Untersagungen auch in Bezug auf materiell rechtswidrige Datenverarbeitungen treffen zu können.

6. Gewinnabschöpfung
[Artikel 2 Nummer 9 (§ 43 Absatz 3)]

Die Einführung einer Möglichkeit zur Gewinnabschöpfung wird begrüßt. Mehr noch als die Anpassung des Bußgeldrahmens ist sie dazu geeignet, die Gewinne aus dem illegalen Datenhandel abzuziehen.

7. Übergangsfrist
[Artikel 2 Nummer 19 (§ 47)]

Die Übergangsfrist für die Weiternutzung bereits bestehender Datensammlungen nach dem Listenprivileg ist mit drei Jahren deutlich zu lang bemessen und widerspricht dem Interesse der Betroffenen an einer zügigen Verbesserung des Datenschutzes. Selbst mit den erforderlichen Umstellungsarbeiten in den Unternehmen dürfte eine Weiternutzung allenfalls für 1 - 2 Jahre ausreichend sein, zumal Teile der Werbewirtschaft bereits jetzt mit neuen Werbeideen auf die Veränderungen reagieren und damit eine schnelle und flexible Umstellung auf die neue Rechtslage zu erwarten ist.