verbraucherzentrale Bundesverband

02. Juni 2010

Änderungsbedarf im Datenschutzrecht

Forderungskatalog zur Modernisierung des BDSG

Verbraucherzentrale Bundesverband e.V. – vzbv
Fachbereich Wirtschaft
Markgrafenstr. 66
10969 Berlin
wirtschaft@vzbv.de
www.vzbv.de

Inhalt

A. Einleitung

Das BDSG hat am Ende der 16. LP Änderungen erfahren. So wurden u.a. neue Regelungen zum Scoring und zu Auskunfteien eingeführt sowie die Regelungen zum sog. Listenprivileg geändert und die zur Auftragsdatenverarbeitung konkretisiert. Die Einführung eines Datenschutzaudit-Gesetzes im Zuge der Novelle ist hingegen gescheitert. Der Datenschutz in Deutschland bleibt dennoch weiterhin regelungsbedürftig. Es bestehen nach wie vor enorme Defizite bspw. in den Bereichen Adresshandel insbesondere beim sog. Listenprivileg, aber auch beim Scoring. Hier gab es zwar endlich Regelungen, die Transparenz für die Verbraucher gebracht haben. Diese Regelungen bleiben aber dennoch weit hinter einem angemessen Verbraucherschutz zurück. Auch an der in § 9a BDSG verankerten Verpflichtung, ein Datenschutzaudit-Gesetz zu schaffen, hat sich der Gesetzgeber bislang die Zähne ausgebissen – ohne Ergebnis für die Verbraucher.

Darüber hinaus gibt es weitreichenden Änderungsbedarf, der vom Gesetzgeber noch gar nicht in Angriff genommen wurde. Hierzu gehört, dass Datenschutzrecht verständlicher und lesbarer zu gestalten. Die Regelungen müssen zudem zukunftsfit gemacht werden. Das geltende Datenschutzrecht stammt noch aus einer „analogen" Zeit, in der das größte Schutzbedürfnis der Verbraucher gegenüber dem Staat als Datenhalter gesehen wurde. Mittlerweile ist es eine enorme Herausforderung für das Datenschutzrecht geworden, das Grundrecht auf informationelle Selbstbestimmung hauptsächlich vor privaten, auch internationalen Datenverwendern zu schützen, die digitalen Realitäten zu erfassen und gleichzeitig auf neue Änderungen der fortschreitenden Technik flexibel reagieren zu können.

Um dies alles zu gewährleisten muss das Datenschutzrecht grundlegenden Veränderungen unterzogen werden.

B. Strukturelle und grundsätzliche Änderungen

1. Lesbarkeit und Verständlichkeit

Damit das BDSG verständlicher wird sollte es sprachlich überarbeitet werden. Daneben sollten einzelne Paragraphen oder Abschnitte unabhängig von etwaigen inhaltlichen Änderungen vereinfacht werden, d.h. systematisch klarer strukturiert werden. Es finden sich einzelne Normen, in denen auf Grund zeitlich versetzter Änderungen komplizierte und verschachtelte Systematiken von Grundsätzen, Ausnahmen und mehrfachen Rückausnahmen entstanden sind.

Die Verständlichkeit des BDSG muss durch eine Neustrukturierung des Normengefüges verbessert werden. Die allgemeinen Vorschriften sollten überarbeitet und erweitert werden. Speziell die Zielvorgaben des Datenschutzes, Datensparsamkeit, Datenvermeidung und die Zweckbindung jeglichen Umgangs mit Daten sollten zu verbindlichen, allgemeingültigen Normen erhoben werden, die stets zu beachten sind. Sie müssen für alle verantwortlichen Stellen gelten und unabhängig von verwendeter Technik oder Art der Datenverarbeitung sein. Aus so normierten Grundsätzen hätten die Betroffenen Ansprüche auf deren Einhaltung.

Wie alle Regelungen im allgemeinen Teil, sollte die Nichtbeachtung sanktioniert werden, denn sie bilden die „Philosophie", die jedem Umgang mit Daten im Lichte des Grundrechts auf

informationelle Selbstbestimmung als Ausfluss der Menschenwürde zu Grunde liegen soll. Zur Stärkung und besonderen Betonung des Zweckbindungsgrundsatzes sollte dieser durch eine eigene Norm hervorgehoben und konkretisiert werden.

Die Unterscheidung zwischen öffentlichen und nicht öffentlichen Stellen sollte aufgehoben werden. Die Grundsätze des Datenschutzes und der Datenverarbeitung sollten allgemein gültig sein, so dass jede Stelle sie zu beachten hat. Dies wäre auch eine Annäherung an die EU-Datenschutzrichtlinie, die eine solche Unterscheidung nicht kennt, und würde zur Übersichtlichkeit beitragen. Es ist nicht einleuchtend, warum öffentliche Stellen anderen Regelungen im Umgang mit Daten unterliegen sollen, als private. Die Verwirklichung des Grundrechtschutzes wird dadurch in keiner Weise befördert.

Eine Erweiterung des Adressatenkreises des BDSG ist zu überlegen. Derzeit sind nur Betroffene und verantwortliche Stellen von den Regelungen angesprochen. Eine Ausweitung auf Hersteller und Entwickler von bspw. Datenverarbeitungssoftware und -systemen ist sinnvoll. Die Prinzipien der Datenvermeidung und Datensparsamkeit müssten so zwingend wesentlich früher berücksichtigt werden. Auch müssten Datenverarbeitungssysteme und –verfahren dann so ausgerichtet werden, dass tatsächlich nur diejenigen Daten Erhoben und Verarbeitet werden die für den jeweiligen Zweck erforderlich sind. Ein weiterer Vorteil der Erweiterung des Adressatenkreises auf Entwickler und Hersteller liegt in der damit automatisch einhergehenden Förderung der Forschung und technischen Weiterentwicklung auf diesem Gebiet.

Eine rechtliche Einordnung von potentiell personenbeziehbaren Daten muss erfolgen.

Für nicht öffentliche Stellen gilt das BDSG nur, soweit es sich um automatisierte Datenverarbeitung oder nicht automatisierte Dateien handelt. Nicht umfasst sind daher einfache Papierakten, die in den Anwendungsbereich der öffentlichen Stellen fallen. Hier muss eine Erweiterung auch für nicht öffentliche Stellen erfolgen.

Die Verbesserung der Lesbarkeit und Verständlichkeit des BDSG ist im Koalitionsvertrag zwischen CDU/CSU und FDP niedergeschrieben.

2. Technikneutralität

Das BDSG muss sich in seiner Struktur nicht nur gegenüber den jetzigen Herausforderungen der digitalen Welt öffnen, sondern daneben auch gegenüber zukünftigen Änderungen flexibel sein. Daher müssen technikneutrale Regelungen geschaffen werden, die unabhängig vom genutzten Medium allgemeingültige Regeln für den Umgang mit Daten schaffen. Diese Regelungen müssen im allgemeinen Teil verortet werden und für alle verantwortlichen Stellen und Betroffene gelten. Sie können von speziellen Regeln für einzelne Bereiche, wie dem Internet oder wie bereits heute für Telekommunikationsdienstleistungen (TKG) flankiert, dürfen von diesen jedoch nicht verdrängt werden. In jedem Fall ist eine Aufspaltung in zu viele Einzelgesetze zu vermeiden.

Zur Gewährleistung der Flexibilität des Datenschutzrechtes sollten die Regelungen in § 9 BDSG zum technischen und organisatorischen Datenschutz neu gefasst werden. Es sollte eine Ausrichtung an technikneutralen Schutzzielen erfolgen. Anhand dieser Schutzziele, die

allgemeingültig für jede Form der Datennutzung gelten, müssen durch die verantwortlichen Stellen Maßnahmen zu deren Erfüllung ergreifen.

C. Inhaltliche Änderungen

1. Transparenz

Die Erhebung, Verarbeitung und Nutzung von Daten muss insgesamt transparenter werden. Der Betroffene soll in die Lage versetzt werden, seine bereits nach dem BDSG bestehenden Auskunftsrechte auch tatsächlich geltend machen zu können. Dazu muss er wissen, wer welche Daten zu welchem Zweck gespeichert hat. Diese Informationen sind gleichfalls integraler Bestandteil eines Datenschutzkonzeptes, dass dem Grundrecht auf informationelle Selbstbestimmung angemessen Geltung verschafft.

Die größte Hürde besteht darin, dass der Betroffene oft keine Kenntnis davon hat, wer Daten über ihn hält. Die Auskunftsrechte laufen in diesen Fällen leer. Ebenso werden Daten oft unbemerkt erhoben, so zum Beispiel bei den Spuren, die jeder Surfer im Internet hinterlässt. Damit der Verbraucher Souverän über seine Daten bleibt, müssen klare, technikneutrale und allgemeingültige Regelungen getroffen werden, die eine ausreichende Information der Betroffenen sicher stellt.

Transparenz ist zu erreichen, in dem der Verbraucher Herr über seine Daten bleibt – jederzeit und uneingeschränkt. Eine Möglichkeit hierfür ist die aktive, informierte und freiwillige Einwilligung in die Datennutzung (siehe unten 2.).

Darüber hinaus kann ein Datenbrief Transparenz schaffen und einen Anreiz für das Vergessen von Daten setzen. Es sollen nur Daten gespeichert werden, die auch tatsächlich gebraucht werden. Nicht notwendige Daten sollen den Unternehmen und Behörden zum lästigen Klotz am Bein werden, den sie möglichst schnell loswerden wollen. Und der Verbraucher soll darüber in Kenntnis sein.

Der Datenbrief ist als Teil eines Gesamtprozesses zu betrachten, an dessen Ende eine bessere Aufklärung der Verbraucher, die leichtere Durchsetzung ihrer Rechte und ein besserer Umgang mit ihren Daten durch die Datenhalter steht.

Mehr Transparenz muss auch geschaffen werden, wenn es um die Frage geht, welche Stelle für welche Datennutzung verantwortlich ist, insbesondere bei grenzüberschreitenden Sachverhalten und im Falle von Auftragsdatenverarbeitung.

2. Aktive, informierte und freiwillige Einwilligung

Ein Weg zu Transparenz und damit zu Verbrauchern, die die Folgen ihres datenbezogenen Verhaltens realistisch abschätzen können, ist die aktive, informierte und freiwillige Einwilligung. Hierzu bedarf es einer grundsätzlichen Opt-In Regelung, die nicht durch weitreichende Ausnahmen ausgehöhlt wird (siehe hierzu unten zu § 28 BDSG).

Die Einwilligung muss aktiv sein. Der Betroffene muss durch aktives, bewusstes Handeln zustimmen, damit die Einwilligung wirksam wird. Dies kann z.B. digital durch aktives anklicken eines Kontrollkästchens oder schriftlich durch gesonderte Unterschrift geschehen. Nicht

ausreichend sind konkludente Erklärungen über das Akzeptieren der AGB oder gar durch bloßes Nutzen einer Internetseite.

Einwilligungen in Datenerhebung und -verarbeitung müssen informiert erteilt werden. Der Betroffene muss vor Erteilung der Einwilligung wissen, welche Folgen seine Einwilligung hat. Hierfür muss er informiert werden, welche Daten zu welchem Zweck erhoben werden, wie diese verwendet werden und ob und an wen sie weitergegeben werden. Er muss über seine Rechte betreffend die Daten informiert werden. Der Betroffene muss darüber informiert sein, ob Daten erhoben werden, die er nicht selbst mitteilt, z.B. Standortdaten, die das Mobiltelefon automatisch versendet oder Daten die während des surfen im Internet im Hintergrund gespeichert werden. Die verantwortliche Stelle muss den Betroffenen über diese Dinge verständlich, lesbar und exponiert informieren.

Die Einwilligung muss freiwillig sein. Sie darf weder generalisiert noch gekoppelt werden oder zur Umgehung eines gesetzlichen Erhebungsverbotes eingeholt werden. Dies gilt im Besonderen für Daten, die durch die Nutzung von digitalen und mobilen Kommunikationsmitteln anfallen und die nicht bloß der technischen Funktionalität des Kommunikationsmediums dienen. Das Kopplungsverbot ist entsprechend auszuweiten, so dass alle Einwilligungen erfasst sind, nicht bloß solche zu Werbezwecken.

Eine Regelung zur rechtlichen Einordnung potenziell personenbeziehbarer Daten ist in diesem Zusammenhang von Bedeutung.

Die Einwilligung muss zeitlich begrenzt werden. Häufig kann der Verbraucher – auch trotz neuer Hinweis- und Dokumentationspflichten – nicht mehr nachvollziehen wohin seine einst erteilte Einwilligung gewandert ist. Auch verblasst das Bewusstsein der rechtlichen Konsequenzen einer einmal erteilten Einwilligung mit der Zeit, Das gerade bei der mittlerweile sehr großen Anzahl speziell an Werbeeinwilligungen, die bereits alltäglich sind. Einmal erteilte Einwilligungen behalten für die verantwortlichen Stellen auch nicht ewig einen geschäftlichen Nutzen. Die Datenbestände veralten vielmehr sehr schnell, sind aber nur mit einer gewissen Aktualität wirklich brauchbar. Daher sollte nach bspw. 2 Jahren die Einwilligung ihre Wirksamkeit verlieren, mit der Folge, dass die Daten entweder gelöscht werden müssen oder eine neue Einwilligung eingeholt werden muss.

Einwilligungen müssen nachgewiesen werden. Im Streitfall hat die verantwortliche Stelle nachzuweisen, dass eine Einwilligung vorliegt. Dies funktioniert in der Praxis häufig nicht. Die verantwortlichen Stellen behaupten häufig eine Einwilligung zu haben, weisen diese aber nicht nach. Es muss eine gesetzliche Klarstellung erfolgen, dass dieser Anspruch besteht.

Die 2009 neu eingeführte elektronische Einwilligung wurde nicht im Allgemeinen Teil unter § 4a BDSG normiert, sondern in § 28 IIIa BDSG (siehe hierzu unten bei § 28 BDSG). Sie ist somit nur in dessen Anwendungsbereich, namentlich für Werbeeinwilligungen, gültig. Eine Regelung im Allgemeinen Teil des BDSG wäre angebracht, damit der elektronischen Einwilligung generelle Geltung zukommt.

Ein Sammelrückruf für Einwilligungen sollte eingeführt werden. In der Regel werden von einem Anbieter auch Einwilligungen für die Weitergabe von Daten an Dritte eingeholt. Widerruft der Verbraucher seine Einwilligungen bei diesem Anbieter, ist der Widerruf jedoch nur für den jeweiligen Anbieter maßgeblich. Der Anbieter ist nicht dazu verpflichtet, den Widerruf weiter zu geben. Dieses Verfahren ist verbraucherunfreundlich. Die meisten Verbraucher werden sich nicht an das Kleingedruckte erinnern, in dem niedergelegt wurde, an welche Dritte die Daten weitergegeben wurden. Daher muss das Unternehmen, das die Einwilligung erhalten und die Daten an Dritte weiter geleitet hat, auch zur Weiterleitung des Widerrufs verpflichtet werden.

Es sollte überlegt werden, in wie weit man für Kinder und Jugendliche spezielle Datenschutzregelungen treffen kann. Diese Gruppe ist besonders schutzwürdig und verfügt je nach Alter über ein weniger ausgeprägtes Verständnis bezüglich der rechtlichen Konsequenzen ihres Handelns. Kinder und Jugendliche sind zudem gerade im Bereich der sozialen Netzwerke wesentlich anfälliger, einem Gruppenzwang zu folgen1.

3. Datenschutz und Internet

Als Pendant zum Brief-, Post- und Fernmeldegeheimnis nach Art. 10 GG ist ein Mediennutzungsgeheimnis für den elektronischen Verkehr einzuführen. Art. 10 GG ist für seinen Regelungsbereich als Konkretisierung des allgemeinen Persönlichkeitsrechts nach Art. 2 I GG zu werten und ist somit auch Ausfluss der Menschenwürde. Das Mediennutzungsgeheimnis sollte dem entsprechend als Ausfluss der Menschenwürde in Form einer Konkretisierung des allgemeinen Persönlichkeitsrechts zur Geltung kommen.

Sogenannte „Privacy by default“ Lösungen sind verpflichtend einzuführen, d.h. die Grundeinstellungen von Internetdiensten müssen so gesetzt sein, dass ohne Veränderungen durch den Nutzer der größtmögliche Datenschutz gilt. Der Nutzer kann dann aktiv und freiwillig davon abweichen, wenn er dies wünscht.

Darüber hinaus ist sicherzustellen, dass beim sogenannten Cloud Computing deutsche Datenschutzstandards für die ausgelagerten Daten gelten. Dies ist zum einen über internationale Vereinbarungen zu erreichen. Zum anderen sollte im BDSG geregelt werden, dass Auslagerung von Daten bei weniger hohem Schutzniveau im Zielland verboten wird.

Es sollte eine Verpflichtung eingeführt werden, anonyme und pseudonyme Nutzungsmöglichkeiten von Internetdiensten anzubieten.

Ein Recht auf Datenportabilität sollte eingeführt werden. Von diesem Recht ist umfasst, dass Verbraucher ihre einmal auf einer Plattform abgelegten oder eingestellten Daten barrierefrei zu einer anderen Plattform „transportieren“ dürfen. Dies schließt die vollständige und rückstandslose Löschung auf der ersten Plattform ein. Durch dieses Recht wird die Herrschaft der Verbraucher über ihre Onlinedaten gestärkt.

---

1 Vgl. BEUC discussion paper: „Data collection, targeting and profiling of consumers online“, 4, in dem auch Vorgeschlagen wird, dass Online-Marketing-Formen zu verbieten sind, die die kognitive oder emotionale Entwicklung von Kindern und Jugendlichen negativ beeinflussen und nennt hier die zunehmende Fettleibigkeit von Kindern als Beispiel.

Personenbezogene Daten in der Onlinewelt sollten einem Verfallsdatum unterliegen, nach dessen Ablauf die Daten entweder automatisch gelöscht werden, oder der Betroffene aktiv und freiwillig einer weiteren Haltbarkeit mit erneutem Verfallsdatum zustimmt. Dies ist ein entscheidender Schritt hin zu einem neuen Recht auf „Vergesslichkeit des Netzes".

4. Stiftung Datenschutz

Eine Kernaufgabe der Stiftung Datenschutz soll in der Schaffung von Rahmenbedingungen für ein Datenschutzaudit liegen. Es sollen Anforderungen bezüglich Datenschutz und Datensicherheit in Unternehmen, öffentlichen und privaten Institutionen erarbeitet werden, die über das gesetzlich geforderte Maß hinaus gehen. Dies ist insbesondere deshalb notwendig, da sonst eine Kompetenzüberschneidung zu den Datenschutzaufsichtsbehörden entsteht. Diese sind mit der Überwachung der Einhaltung der datenschutzrechtlichen Regelungen betraut. Würde nur der gesetzliche Mindeststandard anhand der Anforderungen zertifiziert, so würde zum einen die gleiche Prüfung doppelt durchgeführt, zum anderen bestünde die Gefahr, dass die unterschiedlichen Institutionen zu unterschiedlichen Ergebnissen kommen. Darüber hinaus ist die Nichteinhaltung der gesetzlichen Standards Bußgeldbewährt, so dass hier ein staatliches Monopol zur Aufklärung von Verstößen besteht. Zudem bedarf es marktgesteuerter Ansätze zur Förderung des Datenschutzes, die nur über ein Mehr an Schutz zu erreichen sind, denn nur so kann ein Anreiz für die Fortentwicklung des Datenschutzes im Sinne einer Best Practice gesetzt werden. Die Stiftung könnte auch die spätere Zertifizierung von Unternehmen, öffentlichen und privaten Institutionen vornehmen. Hierfür sind aber auch andere Möglichkeiten denkbar.

Die Zertifizierung einzelner Produkte und Dienstleistungen könnte ebenfalls zur Verbesserung des Datenschutzniveaus in Deutschland beitragen. Produkte und Dienstleistungen, die auf dem deutschen Markt angeboten werden, könnten auf die Einhaltung besonders hoher Datenschutzstandards oder besonders hoher Gewährleistung von Datensicherheit hin zertifiziert werden. Die Stiftung Datenschutz könnte hierfür die Standards erarbeiten und die Akkreditierung der späteren Zertifizierungsstellen durchführen.

Die Ansiedlung vergleichender Produkt- und Dienstleistungsprüfungen (Datentest) nach dem Vorbild der Stiftung Warentest bei der Stiftung Datenschutz ist nicht sinnvoll. Die Stiftung Warentest könnte Datensicherheits- und Datenschutzkriterien in Ihren Test stärker berücksichtigen oder selbst vergleichende Datenschutztests durchführen.

Die Stärkung der Datenschutzkompetenz der Entscheidungsträger und Verantwortlichen in öffentlichen und privaten Institutionen bspw. durch Aufklärungskampagnen oder Schulungen sollte eine Hauptaufgabe der Stiftung Datenschutz werden. Die Stiftung kann zudem, in Absprache mit den vorhandenen Akteuren, die Verbraucherorganisationen dabei unterstützen, durch geeignetes Informationsmaterial sowie Bildungs- und Aufklärungsangebote die Öffentlichkeit über die Bedeutung des Datenschutzes, die Risiken ungenügenden Datenschutzes und die Möglichkeiten des Selbstdatenschutzes zu informieren und dadurch auf eine Stärkung des Selbstdatenschutzes hinzuwirken. Hier kann eine enge Zusammenarbeit mit den bereits sehr erfahrenen Verbraucherzentralen hilfreich sein. Für die Verbraucherinformation sind hauptsächlich die Verbraucherorganisationen zuständig.

Die Stiftung soll einen aktiven Beitrag zur Fortentwicklung des Datenschutzrechts leisten. Sie soll Konzepte entwerfen, wie modernes Datenschutzrecht aussehen kann. Hierfür kann die Stiftung beispielsweise Rechtsvergleiche durchführen oder Wissenschaftswettbewerbe ausschreiben.

5. Verbandsklagerecht

Verbraucherverbände müssen mit dem Recht ausgestattet werden, gegen Datenschutzverstöße zu klagen. Verbraucherorganisationen sind im Bereich des Datenschutzes häufig die Hände gebunden, da das Datenschutzrecht von den Gerichten nicht als verbraucherschützende Norm im Sinne des § 2 des Unterlassungsklagegesetzes (UKlaG) anerkannt wird. Kommt ein Unternehmen beispielsweise den gesetzlichen Verpflichtungen nicht nach, Verbrauchern über die gespeicherten Daten Auskunft zu erteilen oder verwendet das Unternehmen die Daten zu Zwecken, für die keine Einwilligung vorliegt, können Verbraucherorganisationen ihre Verbandsklagebefugnisse nicht einsetzen. Gesetzeswidriges Verhalten wird demnach häufig nicht sanktioniert, da der einzelne Verbraucher den Aufwand scheut zu klagen. Analog beispielsweise zu den Klagerechten im Bereich des unlauteren Wettbewerbs (UWG) sollten Verbraucher durch qualifizierte Verbraucherorganisationen auch im Datenschutz geschützt werden. Daher bedarf es einer Klarstellung im UKlaG, nach der Datenschutzvorschriften, soweit sie die Rechte der Verbraucher betreffen, Verbraucherschutzgesetze im Sinne des UKlaG darstellen. Diese Forderung wird auch von den Bundesländern unterstützt.

Zudem sollte § 29 ZPO (Besonderer Gerichtsstand des Erfüllungsorts) Anwendung finden.

6. Datenschutz international durchsetzbar machen

Die Regelungen des Safe-Harbor-Abkommens haben sich nicht bewährt. Die Durchsetzung deutschen Datenschutzrechts bei Anbietern außerhalb der EU findet faktisch nicht statt. Es muss klargestellt werden, dass wer Daten deutscher Verbraucher verarbeitet, deutschem oder europäischem Recht unterliegt, anstatt den Standort der Datenverarbeitung als Referenz heranzuziehen.

Die Verarbeitung darf nur erlaubt sein, sofern europäische Standards auch bei Datenschutzaufsicht und rechtlichen Durchsetzungsmöglichkeiten für den Einzelnen durch das Herkunftsland des Datenverwenders eingehalten oder überschritten werden.

7. Einzelne Normen des BDSG

a) § 3 BDSG – Begriffsbestimmungen

Einige Begriffsdefinitionen im aktuellen BDSG bedürfen der Konkretisierung. Sowohl die Begriffe „öffentlich zugängliche Daten“ und „Verarbeiten“ sollten neu definiert werden.

„Öffentlich zugängliche Daten“: Diese Terminologie umfasste bei ihrer Einführung hauptsächlich Medien wie gedruckte Telefonbücher oder öffentliche Register. Im Internetzeitalter bekommt dieser Begriff neue Bedeutung, welche die Anwendungsmöglichkeiten der Normen, in denen der Begriff verwendet wird, nahezu ausufern lässt. Der Begriff muss daher neu und einschränkend definiert werden.

„Verarbeiten“: In der Europäischen Datenschutzrichtlinie und anderen europäischen nationalen Regelwerken gibt es keine Trennung zwischen den verschiedenen Umgangsformen für Daten. Das deutsche Recht unterscheidet zwischen Verarbeiten, Erheben, und Nutzen. Dies führt zu einer Vielzahl von unübersichtlichen Normen, in denen die Begriffe hintereinander aufgeführt sind. Sie lassen sich schlecht lesen und es besteht die Gefahr des Überlesens, wenn in einer Norm nur zwei der drei Begriffe auftauchen.

In § 3 IX BDSG sollten genombezogene Daten in den Kreis der besonderen Arten personenbezogener Daten aufgenommen werden.

b) § 4 BDSG – Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

In § 4 BDSG werden die Zulässigkeiten der Datenerhebung, -verarbeitung und -nutzung geregelt. In der Praxis hat sich insbesondere § 4 III 1 BDSG als problematisch erwiesen. Die bisherigen Einschränkungen „sofern er nicht bereits auf andere Weise Kenntnis erlangt hat“ und „die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalls nicht mit der Übermittlung an diese rechnen muss“ haben dazu geführt, dass die Informationspflicht der verantwortlichen Stelle über die Erhebung der Daten gegenüber den Verbrauchern ein Ausnahmefall, anstatt wie intendiert die Regel darstellte. Diese Informations- und Dokumentationspflichten sind jedoch essentiell für Verbraucher, damit sie wissen, von wem und für welche Zwecke die Daten erhoben und an welchen Empfängerkreis sie weitergegeben werden. Daher sollten diese Einschränkungen ersatzlos gestrichen werden.

c) §§ 7 und 8 BDSG – Schadenersatz

Die Schadenersatzregelungen sollten schärfer sein. § 7 BDSG vermutet Verschulden, § 8 BDSG ist verschuldensunabhängig. In § 8 BDSG sollte die Höchstgrenze der Ersatzsumme von 130 000 Euro überprüft werden. Hier ist eine differenziertere Regelung angebracht. Zu überlegen wäre beispielsweise, die die jeweils haftende Vermögensmasse zu berücksichtigen. Auch ist die Höchstsumme die eine verantwortliche Stelle zu leisten hat insgesamt begrenzt. Das bedeutet, dass bei einer Vielzahl von Betroffenen, jeder einzelne nur einen geringen Anteil der Schadenssumme erstattet bekommt. Aber gerade bei der automatisierten Datenverarbeitung besteht die Gefahr, dass eine Vielzahl unterschiedlicher Betroffener Schaden erleiden. Die zahlbare Höchstsumme sollte daher pro einzelnem Geschädigten gelten und nicht insgesamt.

Die Gefährdungshaftung bei Datenschutzverstößen sollte nicht wie bisher nur für öffentliche, sondern auch für nicht-öffentliche Stellen gelten, was mit der geforderten grundsätzlichen Aufhebung der Unterscheidung zwischen diesen beiden erreicht würde.

Immaterielle Schäden sollten über die Einführung eines pauschalen Schadenersatzes geltend gemacht werden können, d.h. der Geschädigte muss nicht einen exakt bezifferten Schaden angeben. Ausreichend ist die Darlegung, dass ein immaterieller Schaden vorliegt.

d) § 9a BDSG – Datenschutzaudit

Das Datenschutzauditgesetz, welches im Zuge der zweiten BDSG-Novelle eingeführt werden sollte, ist in Gänze gescheitert. Die Schaffung eines Datenschutzaudits ist nachwievor notwendig und sinnvoll. Sie kann im Rahmen einer zu errichtenden Stiftung Datenschutz in Angriff genommen werden (siehe hierzu unten Stiftung Datenschutz). Es muss eine gesetzliche Grundlage geschaffen werden, die ein Mindestmaß an inhaltlichen Vorgaben enthält.

e) § 11 BDSG – Auftragsdatenverarbeitung

In § 11 II 2 BDSG wurde die Regelung zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch andere Stellen im Auftrag konkretisiert und präzisiert. Zusätzlich sollte in § 11 II 4 BDSG die Häufigkeit, Tiefe und Dokumentation von Kontrollen bei den Auftragnehmern durch den Auftraggeber näher geregelt werden. Dies ist insbesondere für die Fälle notwendig, in denen Verbraucherdaten unterschiedlicher Herkunft bei einem Unternehmen (wie einem Call- Center) liegen. Wenn hier nicht ausreichend kontrolliert wird, besteht eine hohe Missbrauchsgefahr darin, dass die Daten unberechtigt miteinander verknüpft werden.

Für Berufsgeheimnisträger, die als Auftraggeber Daten an Dritte übermitteln, besteht eine Regelungslücke, die geschlossen werden muss. Beispielsweise zeigen sich in der Praxis immer wieder Probleme, wenn Ärzte zu Abrechnungszwecken Gesundheitsdaten an externe Buchhalter oder andere Dienstleister übermitteln.

f) § 28 BDSG – Datenerhebung und -speicherung für eigene Geschäftszwecke

Die noch im Gesetzentwurf der BDSG-Novelle II in der 16. WP geplante vollständige Abschaffung des Listenprivilegs in § 28 BDSG ist nicht erfolgt. Das Listenprivileg in § 28 BDSG ist aber nicht nur erhalten geblieben. Es werden auch weiterhin Anreize gesetzt, Daten listenmäßig und automatisiert zu Speichern und zu verarbeiten. So sind die Haftungsregelungen in § 8 BDSG für den Verantwortlichen günstiger, wenn er viele Betroffene durch eine unzulässige Datennutzung geschädigt werden, da die Haftungssumme den gleichen Höchstsätzen unterliegt, wie bei nur einer durch eine einzelne Person verursachte Schädigung. Auch § 10 BDSG, der die Einrichtung automatisierter Abrufverfahren regelt, sieht in Abs. IV vor, dass sich bei stichprobenartigen Kontrollen der Zulässigkeit eines automatisierten Datenabrufs im Falle der Abrufung eines Gesamtbestandes an Daten vieler Personen, die Kontrolle nur auf die Zulässigkeit des Gesamtabrufs beziehen muss. Ob Daten einzelner innerhalb dieses Bestandes unzulässig abgerufen werden, unterliegt nicht der Kontrolle. Die Zulässigkeit der einzelnen Datenabrufe für sich richtet sich, wie die des Gesamtpakets, zwar nicht nach § 10 BDSG, sondern nach den Vorschriften, die den Abruf an sich erlauben (z.B. §§ 28, 29 BDSG). Sollen jedoch unzulässige Abrufe und Nutzungen durchgeführt werden, was gerade im Bereich des Adresshandels zu befürchten ist, so die Regelung des § 10 IV 4 BDSG ein weiterer Baustein, der vor Entdeckung schützen kann.

Um das Grundrecht auf informationelle Selbstbestimmung zu verwirklichen und vor Beeinträchtigungen zu schützen, müssen die Verbraucher die Souveränität über ihre Daten und die zu ihnen gehörenden Informationen haben. Hierzu bedarf es:

1) Opt- In

Die Selbstbestimmung der Verbraucher muss insbesondere durch die Einführung einer konsequenten Einwilligungslösung (Opt.-in) hergestellt werden. Einwilligungen in Datenerhebung und -verarbeitung müssen aktiv, informiert und freiwillig sein und dürfen weder generalisiert noch gekoppelt werden.

Durch das Listenprivileg werden bestimmte Daten über Verbraucher auch ohne deren Einwilligung und Wissen für Werbe- und Marketingzwecke verkauft und vermietet. Während Unternehmen Geld mit den Daten der Verbraucher verdienen, können Verbraucher keine Kontroll- und Steuerungsfunktion über die Verwendung ihrer Daten ausüben. Das Listenprivileg widerspricht dem – der Verbraucherpolitik zu Grunde liegenden – Leitbild des mündigen Verbrauchers, der selbst entscheidet, wem er welche seiner Daten zur Verfügung stellt. Das Listenprivileg ist daher gänzlich abzuschaffen.

Erfolgt eine Abschaffung des Listenprivilegs nicht, ist weiterer Regelungsbedarf vorhanden:

Die Ausnahme, nach der listenförmige Daten weiterhin zum Zwecke der Spendenwerbung genutzt werden können, sollte an Kriterien geknüpft werden. Die Spendenorganisationen sollten, wollen sie die Ausnahme nutzen, zum einen ein Datenschutzaudit durchgeführt haben und zum anderen über ein Spendensiegel des Deutschen Zentralinstituts für soziale Fragen (DZI) verfügen oder Mitglied des Deutschen Spendenrats e.V. sein.

Werbeansprachen im Sinne des § 7 II UWG setzen für den Bereich der Werbung in elektronischer Form (E-Mail, SMS) sowie über Telefon und per Fax grundsätzlich eine ausdrückliche Einwilligung des Verbrauchers voraus. Werbeansprachen, aber dezidiert auch Befragungen der Markt- und Meinungsforschung, sind nicht vom UWG erfasst, soweit diese nicht in einem objektiven Zusammenhang zum Warenabsatz stehen und damit auch keine geschäftliche Handlung sind. Ausgehend von dem Schutzzweck dieser Regelungen, Verbraucher vor der unverlangten Kontaktaufnahme zu Werbezwecken und derartigen Belästigungen zu schützen, findet sich zu § 28 III 1 BDSG ein Widerspruch. Die nach dem UWG erforderliche *ausdrückliche* Einwilligung für eine Werbeansprache findet sich derzeit dort nicht wieder.

Das hat zur Folge, dass die Kontaktaufnahmen zu Zwecken der Markt- und Meinungsforschung auch dann möglich sind, wenn der angerufene Verbraucher zuvor nicht ausdrücklich eingewilligt hat. Eine thematische Differenzierung nach einer zielgerichteten Werbeansprache im Sinne des UWG und einer Ansprache zu Zwecken der Meinungsforschung im Sinne des BDSG ist sachlich nicht zu rechtfertigen. In § 28 III 1 BDSG muss klargestellt werden, dass es Verarbeitung oder Nutzung personenbezogener Daten für Zwecke der Markt- und Meinungsforschung einer ausdrücklichen Einwilligung bedarf.

Weiterer Regelungsbedarf besteht in § 28 III 4 BDSG. Dieser erlaubt die Übermittlung von Listendaten zum Zwecke der Werbung, wenn die Übermittlung nach § 34 Ia 1 BDSG

gespeichert wird (Pflicht des Übermittlers) und aus der darauffolgenden Verwendung, also der Werbung, die Stelle, welche die Daten erstmalig erhoben hat eindeutig hervorgeht (Pflicht des Empfängers). Verstöße gegen die Speicherungspflicht sind mit einem Bußgeld bedroht (§ 43 I Nr. 8a BDSG). Kurios an der Norm ist, dass die Pflicht des Datenempfängers, die Herkunft der Daten zu benennen, eine Voraussetzung für die Zulässigkeit der Übermittlung ist. Wird hiergegen verstoßen, ist die Übermittlung rückwirkend als unzulässig zu betrachten, und gegen den Datenübermittler kann ein Bußgeld verhängt werden. Dieser sollte sich daher vertraglich die Einhaltung der Kennzeichnungspflicht zusichern lassen.

In § 28 III 6 BDSG sollte klargestellt werden, dass der Abwägungsvorbehalt mit des schutzwürdigen Interessen des Betroffenen – entsprechend der gültigen, im Widerspruch zum Wortlaut stehenden Rechtslage – auch für die Beipack- und Empfehlungswerbung nach Satz 5 gilt.

§ 28 III 2 Nr. 1 BDSG enthält eine Ausnahme zum Opt-In Grundsatz, wenn die verantwortliche Stelle die Daten für Werbung mit eignen Angeboten nutzt. Hier sollte eine Einschränkung auf Werbung mit eigenen ähnlichen Produkten oder Dienstleistungen erfolgen. Sowohl Art. 13 II RL 2002/58/EG als auch § 7 III Nr. 2 UWG erlauben die Werbung in ihrem Anwendungsbereich nur eingeschränkt für eigene *ähnliche* Angebote. Das BDSG widerspricht in so weit dem UWG zu Lasten der Verbraucher und verstößt gegen die EU-Richtlinie.

2) <u>Kopplungsverbot</u>

Das Kopplungsverbot ist auf sämtliche Einwilligungen, nicht nur solche zu Werbezwecken, auszuweiten und im allgemeinen Teil des BDSG zu verorten.

Der Wortlaut des § 28 III b BDSG könnte geändert werden, um klarer herauszustellen, dass nicht gemeint ist, dass das Unternehmen, mit dem der Verbraucher in eine vertragliche Beziehung treten will, eine marktbeherrschende Stellung inne hat. Vielmehr sind auch die Fälle erfasst, in denen kein anderer Anbieter derselben Leistung auf die Einwilligung verzichten mag oder dem Verbraucher auf andere Weise ein anderer Leistungserbringer nicht zumutbar ist (marktweite Kopplung). Eindeutiger und klarer wäre dies im Wortlaut herausgestellt, wenn dieser von „ohne die Einwilligung“ in „ohne Einwilligung“ oder „ohne eine Einwilligung“ geändert würde. „Die Einwilligung“ könnte als die spezielle, von dem verantwortlichen Unternehmen konkret geforderte bedeuten.

Es könnte zudem eine Beweislastumkehr eingeführt werden, so dass die verantwortliche Stelle die Beweislast dafür trägt, dass dem Betroffenen ein Alternativzugang zu gleichwertigen Leistungen auf dem Markt ohne Einwilligung nicht möglich ist. Die Unternehmen einer Branche haben einen deutlich besseren Überblick über die am Markt befindlichen Angebote. Sie sollten im Zweifel darlegen, dass es ein gleichwertiges Angebot ohne Kopplung für den Verbraucher gegeben hätte. Die Umkehr der Beweislast bedeutet nicht, dass ein Unternehmen verpflichtet sein sollte einem Verbraucher einen Konkurrenten zu „empfehlen“, bei dem keine Einwilligung verlangt wird. Vielmehr sollte im Streitfall, nachdem der Verbraucher nicht in der Lage war durch eigene Anstrengungen ein gleichwertiges kopplungsfreies Angebot zu finden, die Vermutung gelten, dass ein solches auch nicht gibt und der Markt insgesamt koppelt. An die Anstrengungen des Verbrauchers müssen im Zuge einer solchen Regelung selbstverständlich

hohe Anforderungen gestellt werden, bspw. in Form einer Mindestzahl an weiteren Angeboten. Ziel ist es nicht, dass der Verbraucher mit der bloßen Behauptung keinen kopplungsfreien Marktzugang zu bekommen, die Suche danach auf die Unternehmen abwälzt. Das jeweils im Streitfall involvierte Unternehmen kann die Vermutung dann widerlegen, in dem es eine kopplungsfreie Alternative benennt.

Kurz: Kann der Verbraucher nach Einholung einer zumutbaren Anzahl weiterer Angebote (Branchenabhängig, vielleicht 3 oder 5) keinen Zugang zu einer bestimmten Dienstleistung ohne Einwilligung in die werbliche Nutzung seiner Daten finden, soll eine widerlegbare Vermutung gelten, dass es diesen nicht gibt oder er jedenfalls nicht zumutbar ist.

3) Elektronische Einwilligung und Einwilligungsbestätigung

Neu eingeführt wurde mit der 2. Novelle die elektronische Einwilligung. Diese wurde allerdings nicht im Allgemeinen Teil unter § 4a BDSG normiert, sondern in § 28 IIIa BDSG. Sie ist somit nur in dessen Anwendungsbereich gültig. Eine Regelung im Allgemeinen Teil des BDSG wäre angebracht, damit der elektronischen Einwilligung generelle Geltung zukommt.

Wird eine Werbeeinwilligung nicht schriftlich oder elektronisch erteilt, so muss die verantwortliche Stelle dem Betroffenen den Inhalt der Einwilligung schriftlich bestätigen. Die Rechtsfolge einer Unterlassenen Bestätigung ist im Gesetz nicht geregelt, so dass hier Unklarheiten bestehen. Sieht man die Bestätigung als Wirksamkeitsvoraussetzung der Einwilligung, so ist unklar welchen Status die mündliche Einwilligung zwischen ihrer Äußerung und der Bestätigung hat. Die Einwilligung könnte dann für diese Zeit wohl als schwebend unwirksam zu werten sein und die verantwortliche Stelle müsste den Zugang der Bestätigung im Zweifel beweisen. Dies wird sie regelmäßig nur über eine Zustellung erreichen können, was einen immensen Aufwand und vor allem erhebliche Kosten bedeuten würde. Auch eine denkbare Rückbestätigung durch den Betroffenen wäre nicht sachgerecht, da dann die vom Gesetz grundsätzlich als ausreichend betrachtete mündliche Einwilligung entkernt würde. Nach der Gesetzesbegründung soll der Betroffene durch die Bestätigung *„kontrollieren“* können, ob die „*verantwortliche Stelle die erteilte Einwilligung korrekt dokumentiert hat“*. Es wird also von einer wirksam erteilten Einwilligung ausgegangen, so dass die Bestätigung keine Wirksamkeitsvoraussetzung darstellt. Dies bedeutet, dass die Betroffenen im Zweifel auf die Redlichkeit der verantwortlichen Stellen angewiesen sind und im Falle einer nicht erfolgten Bestätigung wieder mühsam im Wege des Widerspruchs vorgehen müssen.

Es ist zu überlegen, ob nicht grundsätzlich per Telefon oder per Internet abgeschlossene Verträge für ihre Wirksamkeit einer schriftlich-postalischen Bestätigung bedürfen.

g) § 28a BDSG – Datenübermittlung an Auskunfteien

Mit § 28a BDSG wurde eine abschließende Sonderregelung für den Bereich der Datenübermittlung an Auskunfteien geschaffen, die am 01. April 2010 gilt. Es ist eine Sonderregelung für den Fall der Übermittlung von Daten säumiger Schuldner. Eine Übermittlung von Daten nach § 28a BDSG an Auskunfteien ist folglich nur zulässig, wenn eine geschuldete Leistung trotz Fälligkeit nicht erbracht wurde und (Auszug des hier Relevanten)

- der Betroffene nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden ist, zwischen der ersten Mahnung und der Übermittlung mindestens vier Wochen liegen, die verantwortliche Stelle den Betroffenen rechtzeitig vor der Übermittlung der Angaben, jedoch frühestens bei der ersten Mahnung über die bevorstehende Übermittlung unterrichtet hat und der Betroffene die Forderung nicht bestritten hat (Nr.4)

- oder das der Forderung zugrunde liegende Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann und die verantwortliche Stelle den Betroffenen über die bevorstehende Übermittlung unterrichtet hat (Nr.5).

Besonders problematisch ist der Erlaubnistatbestand nach Nummer 4. Die Neuregelung zielt auf zahlungsunfähige oder zahlungsunwillige Schuldner. Die Frist soll beim Bestehen einer berechtigten Forderung ein zu schnelles Einmelden verhindern, da es sein kann, dass der Betroffene eine Forderung lediglich übersehen hat oder durch urlaubsbedingte Abwesenheit noch nicht darauf reagieren konnte. Die Norm birgt allerdings Missbrauchsgefahr und ein erhebliches Risiko für die Verbraucher. Sie ermöglicht es, bei entsprechend krimineller Haltung von unredlichen Unternehmen, gänzlich unberechtigte Forderungen einzumelden, wenn der Verbraucher nicht reagiert. Ein Ziel der in betrügerischer Absicht handelnden Unternehmen bei ungerechtfertigten Forderungen (z.B. fingierten Verträgen) ist es, eine bestätigte Adresse für den Adresshandel zu erhalten. Darüber hinaus spekulieren sie auf Verbraucher, die aus Angst vor einer Klage die meist nicht all zu hohen Forderungen begleichen. Die Forderung selbst ist durch die Betrüger nicht nachweisbar, weshalb diesbezüglich auch keine Klage oder andere rechtliche Konsequenzen zu befürchten waren. Der Verbraucher tat daher bislang gut daran, überhaupt nicht auf die Forderungen zu reagieren. Der neue § 28a I Nr. 4 BDSG bietet nun aber Druckmittel gegen den Verbraucher. Reagiert dieser nicht, so kann die Forderung in Auskunfteien wie bspw. der SCHUFA als Negativeintrag eingemeldet werden. Dies kann erhebliche Konsequenzen für den Verbraucher haben, der dadurch in seiner Kreditwürdigkeit falsch eingestuft wird. Folge davon kann sein, dass Unternehmen z.B. im Versandhandel oder im Telekommunikationsbereich plötzlich keinen Vertrag mit dem Verbraucher abschließen wollen, dieser nur per Nachnahme etwas bestellen kann oder im schlimmsten Fall seine laufenden Kreditverträge gekündigt werden.

Der Verbraucher muss daher nunmehr genau abwägen, ob er dieses Risiko eingehen will und eine entsprechende Güterabwägung vornehmen. Will er das nicht, muss er zukünftig auf die Forderung reagieren und den Missbrauch seiner Adressdaten und eventuelle weitere Forderungen (mit dem entsprechenden Ärger verbunden) in Kauf nehmen.

Diese Folge des Gesetzes wurde bei der Fassung von § 28a BDSG wohl weder gesehen noch beabsichtigt.

Die Regelung sollte so geändert werden, dass ein Missbrauch nicht mehr möglich ist. Es sollte daher sichergestellt werden, dass nach der Einmeldung bestrittene Forderungen wieder zu löschen sind.

Nummer 5 ist unter die Bedingung zu stellen, dass der Verbraucher offene Forderungen nicht bestreitet und auch ein nachträgliches Bestreiten zur Löschung führt. Andernfalls können über die Regelung die Einschränkungen der vorherigen Tatbestände umgangen werden.

h) § 28b BDSG – Scoring

Scoringverfahren sind erstmals gesetzlich geregelt und müssen nun gewisse Kriterien erfüllen. Für den Verbraucher wurde hier mehr Transparenz geschaffen. Allerdings besteht auch hier noch Nachbesserungsbedarf. Die Zulässigkeit von Scoring sollte auf die Einschätzung kreditorischer Risiken beschränkt werden. Zudem sollte ein vollständiges Verbot von Geoscoring und die gänzliche Unzulässigkeit der Verwendung von Schätzdaten eingeführt werden.

i) § 38 BDSG – Aufsichtsbehörde

Da die Eingriffsbefugnisse der Aufsichtsbehörden bereits erheblich verbessert wurde, kann diesbezüglich derzeit kein dringlicher Änderungsbedarf der Norm festgestellt werden. Allerdings ist an dieser Stelle die deutliche Forderung nach einer besseren personellen und finanziellen Ausstattung der Datenschutzbehörden anzubringen. Die löblichen Verbesserungen der Kompetenzen bleiben ein zahnloser Tiger, solange Unternehmen in Deutschland auf Grund mangelnden Personals schlicht nicht oder zu selten überprüft werden.

Der Koalitionsvertrag zwischen CDU/CSU und FDP sieht vor, die personelle und sächliche Ausstattung des Beauftragten für den Datenschutz und die Informationsfreiheit zu verbessern.

j) § 42a BDSG – Informationspflichten bei unrechtmäßiger Kenntniserlangung von Daten

Die neu eingeführten Informationspflichten bei Datenschutzverstößen und -pannen sollten auch für öffentliche Stellen gelten. Zudem ist die Beschränkung auf *schwerwiegende* Beeinträchtigungen der Betroffenen nicht tragbar. Die Beeinträchtigung kann sich mitunter erst wesentlich später zeigen, so dass der Präventionsgedanke hier im Vordergrund stehen muss. Der Verbraucher muss, damit er souverän mit der Situation umgehen kann, auch dann über einen Verstoß oder eine Panne informiert werden, wenn eine Beeinträchtigung (noch) nicht absehbar ist. Auch sollte immer der Betroffene direkt informiert werden. Die Möglichkeit der verantwortlichen Stelle über Zeitungen zu informieren bewirkt zwei Dinge. Zum einen ist nicht sichergestellt, dass jeder Betroffene Kenntnis erlangt. Zum anderen wird der Verbraucher gezwungen im Sinne einer Holschuld bei der Stelle nachzufragen, ob auch seine Daten betroffen sind. Dieser Auskunftsanspruch wiederum ist im BDSG jedoch nicht ausdrücklich geregelt. Er muss daher nach allgemeinen zivilrechtlichen Grundsätzen hergeleitet werden und kann bspw. als quasi-vertragliche Nebenpflicht nach §§ 241 II, 242 BGB bestehen[2].

2 In Betracht kommt auch ein Anspruch aus der allgemeinen Schadensminderungspflicht. Hier müsste der verantwortlichen Stelle allerdings Verschulden nachzuweisen sein. Ebenso ist § 42a BDSG ein Schutzgesetz im Sinne von § 823 II BGB. Vgl. hierzu Gabel, BB 2009, 2046.

Zudem wird die Informationspflicht erst ausgelöst, wenn die Daten unrechtmäßig übermittelt werden oder einem Dritten unrechtmäßig zur Kenntnis gelangen. Dies bedeutet, dass die Entwendung von Daten beispielsweise durch einen Mitarbeiter noch keine Informationspflicht auslöst, selbst wenn dies unbefugt geschieht. Erst wenn ein Dritter diese Daten tatsächlich zur Kenntnis erhält, greift die Norm. Dieser Ansatz ist zeitlich zu spät. Der Gesetzgeber hätte hier früher ansetzen müssen und jede unrechtmäßige Entwendung mit einschließen.

Die Regelung zu Informationspflichten bei unrechtmäßiger Kenntniserlangung kann bei einer Aufhebung der Unterscheidung zwischen öffentlichen und nicht öffentlichen Stellen in den allgemeinen Teil gestellt werden.