**GESELLSCHAFT FÜR DATENSCHUTZ
UND DATENSICHERUNG e.V.**

# Stellungnahme

## der Gesellschaft für Datenschutz und Datensicherung e.V. (GDD)

## zur öffentlichen Anhörung
## des Innenausschusses des Deutschen Bundestages
## zur Thematik „Modernisierung des Datenschutzes“
## am 05. März 2007

***Zum Themenkreis 1 „Modernisierung des Datenschutzes“***

### *1. Ausgangssituation*

Das gegenwärtige Datenschutzrecht ist durch eine Zersplitterung in verschiedene Rechtsbereiche, eine mangelnde Verständlichkeit und eine nicht zeitgerechte Regelung des technisch organisatorischen Datenschutzes gekennzeichnet.

Eine Fülle bereichsspezifischer Regelungen hat zu einer Zersplitterung des Datenschutzrechts geführt. Diese Spezialgesetze sind zum Teil nicht mit den allgemeinen Grundsätzen des Datenschutzrechts abgestimmt und deshalb auch nur aus sich selbst heraus interpretierbar. Zudem ist das Datenschutzrecht durch lange, verschachtelte Formulierungen und vielfache übergreifende Verweisungen sowie durch vielfältige Ausnahme- und Sonderregelungen in weiten Bereichen unverständlich geworden. Die Normenfülle im Datenschutzrecht hat zu Widersprüchlichkeiten hinsichtlich der Anforderungen und Wertungen der jetzigen Vorschriften geführt. Damit ist eine Unübersichtlichkeit, übermäßige Kompliziertheit und Widersprüchlichkeit zu konstatieren, die die Effektivität des Datenschutzrechts beeinträchtigt.

Mit Blick auf die technische Entwicklung geben die für die Wirtschaft maßgeblichen Regelungen des Bundesdatenschutzgesetzes (BDSG) keine zeitgerechten Antworten und bedürfen der Überarbeitung.

Von daher ist eine Modernisierung des Datenschutzrechts angezeigt.

### *2. Grundsätze einer Modernisierung*

Das Datenschutzrecht wird bestimmt durch die Vorgaben europäischer Richtlinien, insbesondere der EG-Datenschutzrichtlinie sowie der Kommunikations-Datenschutzrichtlinie. Eine Modernisierung des Datenschutzrechts sollten die europäischen Richtlinienvorgaben zeitgemäß und zukunftsorientiert konkretisieren, jedoch nicht über den gesetzten Rahmen hinausgehen. Insofern sollte der Grundsatz der so genannten Eins-zu-Eins-Umsetzung von

Richtlinien weitgehend beibehalten werden, um der Harmonisierung des Datenschutzrechts auf europäischer Ebene nicht entgegen zu wirken und Wettbewerbsnachteile für die deutsche Wirtschaft beim Datenverkehr zu vermeiden.

Die Zersplitterung und mangelnde Verständlichkeit des Datenschutzrechts kann bei der Modernisierung rechtssystematisch in der Weise aufgehoben werden, dass das BDSG als Basisgesetz des Datenschutzes bereichsspezifischen Regelungen vorgeht. Bereichsspezifische Regelungen außerhalb des BDSG sollten nur Ausnahmen von den allgemeinen Regelungen enthalten, sofern der Regelungstatbestand bzw. die Art der Datenverarbeitung eine solche Spezialregelung notwendig macht. So empfiehlt es sich, die Regelungen des Telekommunikationsgesetzes und des vor der Verabschiedung stehenden Telemediengesetzes wegen ihrer besonderen praktischen Bedeutung in das BDSG zu integrieren.

### *3. Zulässigkeit der Datenverarbeitung*

a) Die Differenzierung der Zulässigkeitsvoraussetzungen beim Umgang mit personenbezogenen Daten im öffentlichen Bereich und in der Privatwirtschaft sollte beibehalten werden. Die Differenzierung trägt dem Umstand Rechnung, dass die Datenverarbeitung durch Verwaltung und Wirtschaft auf Grund unterschiedlicher Rechtspositionen erfolgt. Im öffentlichen Bereich dient die Datenverarbeitung der Erfüllung staatlicher Aufgaben auf Grund gesetzlicher Ermächtigungen. Deshalb sind diese Datenverarbeitung durch die jeweiligen Ermächtigungsnormen begrenzt. Im privatrechtlichen Bereich erfolgt die Datenverarbeitung auf Grundlage von Vertragsbeziehungen und geschäftlichen Kontakten. Insoweit ist die Datenverarbeitung in der Wirtschaft auf Grundlage unterschiedlicher grundrechtlich geschützte Positionen - der Vertrags-, Unternehmens- und Gewerbefreiheit (Art. 2 Abs. 1 und Art. 12 GG) auf der einen Seite und dem Grundrecht auf informationelle Selbstbestimmung (Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG) auf der anderen Seite - zu legalisieren.

b) Für den Bereich der Privatwirtschaft ist es - anders als im öffentlichen Bereich - erforderlich, die Datenverarbeitung neben der vertraglichen Grundlage auch auf eine Interessenabwägung zu stützen. Bereits die EG-Datenschutzrichtlinie legalisiert den Umgang mit personenbezogenen Daten in Art. 7 f) auf Grundlage einer Interessenabwägung. Es ist notwendig, diese Richtlinienvorgabe im BDSG beizubehalten, um den jeweiligen grundrechtlichen geschützten Positionen gerecht zu werden. Ein reines „opt-in“ der Datenverarbeitung würde zu nicht akzeptablen Verarbeitungsverboten führen. Denn es kann nicht unterstellt werden, dass die wirtschaftliche Nutzung personenbezogener Daten per se die Rechte des Einzelnen beeinträchtigt.
   Weiterhin gilt es zu berücksichtigen, dass auch die Wirksamkeit einer Einwilligung hinsichtlich ihrer Reichweite und ihres Umfangs der Regel eine Interessenabwägung voraussetzt. So hat das Bundesverfassungsgericht in seinem Beschluss vom 23.10.2006 (1 BvR 2027/02) die Gestaltung von Einwilligungsklauseln von der Sicherstellung eines hinreichenden informationellen Selbstschutzes für den Betroffnen abhängig gemacht hat.
   Vor dem Hintergrund der den Betroffenen im Datenschutzrecht zugewiesenen Rechte würde eine Streichung der Abwägungsklausel zu keinen erkennbaren Datenschutzvorteilen führen.

c) Der im BDSG verankerte Grundsatz der Datenvermeidung und der Datensparsamkeit soll den Datennutzer bei mehreren Gestaltungsmöglichkeiten anhalten, diejenige Form zu wählen, die am wenigsten personenbezogene Daten erfordert. Das Gebot der Datenvermeidung und der Datensparsamkeit kann durch Anonymisierung oder Pseudonymisierung der betroffenen Person erreicht werden. Wegen der Bedeutung dieses Grundsatzes ist es notwendig, den Begriff der „Pseudonymisierung“ gesetzlich eindeutiger zu regeln. Denn nach bisheriger Gesetzeslage sind Pseudonyme personenbezogene Daten mit der Folge, dass sie keinen erleichterten Zulässigkeitsvoraussetzungen unterliegen. Dadurch entfällt für die verantwortliche Stelle der Anreiz, Daten vor ihrer weiteren Verarbeitung zu pseu-

donymisieren. Eines solchen Anreizes bedarf es, da mit der Psyeudonymisierung regelmäßig ein erheblicher technischer und finanzieller Aufwand verbunden ist. Insofern bieten Landesdatenschutzgesetze, z.B. das LDSG von Nordrhein-Westfalen, praxisnähere Anforderungen an die Pseudonymisierung, die auf die Herrschaft über Zuordnungsmerkmale abstellen.

d) In der praktischen Anwendung des BDSG führt Anknüpfung an die „verantwortliche Stelle" zu erheblichen Problemen bei der Zusammenarbeit von Unternehmen im Konzern sowie bei verbundenen Unternehmen. Denn die Begriffsdefinition der „verantwortlichen Stelle" führt dazu, dass die Weiterabe personenbezogener Daten von einer justischen Person zur einer anderen in der Regel als Übermittlung zu werten ist, die ihrerseits strengeren Zulässigkeitsvoraussetzungen unterliegt. In einem Konzern oder bei verbundenen Unternehmen sind die unterschiedlichen Aufgaben aus betriebswirtschaftlichen Gründen aber auf verschiedene juristische Personen verteilt. Der jeweils notwendige Datenfluss ist deshalb vielfach datenschutzrechtlich problematisch oder macht administrativ aufwendige vertragliche Regelungen zwischen den konzernangehörigen Unternehmen notwendig.
   Ein modernes Datenschutzrecht sollte den betriebwirtschaftlich notwendigen Datenfluss im Konzern sachgerecht regeln. Hier bedarf es einer Klärung der Reichweite des Begriffs des „für die Verarbeitung Verantwortlicher" i.S.v. Art. 2 d) der EG-Datenschutzrichtlinie. Ziel sollte die Aufnahme eine Konzernklausel in das BDSG sein. Gegebenfalls müsste auf europäischer Ebene eine sachgerechte Legalisierung der Datenweitergabe innerhalb eines Konzerns oder bei verbundenen Unternehmen angestoßen werden, um eine Anpassung an die wirtschaftlichen Gegebenheiten zu erreichen.

e) Einer Klärung bedarf die Inanspruchnahme von Dienstleistern durch Berufsgeheimnisträger. Die in § 203 StGB genannten Berufsgeheimnisträger sind vielfach auf die Inanspruchnahme von externen Dienstleistern angewiesen, die im Wege einer Auftragsdatenverarbeitung im Sinne von §11 BDSG für die geheimnisverpflichteten Auftraggeber weisungsgebunden tätig werden. Als Beispiel mag etwa die digitale Archivierung von Krankenunterlagen dienen. In derartigen Fällen divergiert jedoch vielfach die strafrechtliche von der datenschutzrechtlichen Beurteilung der Datenweitergabe. Während nach dem BDSG die Weitergabe personenbezogener Daten unter den Voraussetzungen des § 11 BDSG privilegiert ist, liegt nach dem StGB hierin eine „unbefugte Offenbarung", es sei denn es liegen Einzeleinwilligungen der Patienten vor (vgl. OLG Düsseldorf, CR 1997, 536 ff.). Ob landesrechtliche Vorschriften, die unter datenschutzrechtlichen Gesichtspunkten regeln, unter welchen Voraussetzungen ausnahmsweise eine Verarbeitung von Patientendaten im Auftrag erfolgen darf (z. B. in Landesdatenschutz- oder Landeskrankenhausgesetzen) als Rechtfertigungsgrund herangezogen werden können, ist nicht mit hinreichender Rechtssicherheit geklärt.
   Durch eine gesetzliche Klarstellung, wonach die Auftragsdatenverarbeitung i.S.v. § 11 BDSG den Tatbestand der „unbefugten Offenbarung" ausschließt, würde auch Berufsgeheimnisträgern bei einer datenschutzkonformen Auftragsdatenverarbeitung das - organisatorisch und wirtschaftlich vielfach sinnvolle - Outsourcing ermöglicht. Wie bereits für den externen Datenschutzbeauftragten vorgesehen, könnte auch der Auftragnehmer mit einem entsprechenden Zeugnisverweigerungsrecht ausgestattet werden, an das sich ein Beschlagnahmeverbot anschließt. Auch hier könnte durch eine entsprechende Änderung des § 203 StGB der Geheimnisschutz durch die Strafbewehrung einer Verletzung der Schweigepflicht flankierend sichergestellt werden.

### *4. Technische Entwicklungen als Herausforderung für den Datenschutz*

Ein modernes Datenschutzrecht muss in der Lage sein, Lösungen zu Datenschutzfragen durch neue technische Entwicklungen zu geben. Die aktuelle Diskussion um die Themen „RFID" oder „allgegenwärtige Datenverarbeitung" belegen diese Herausforderung.

Wenig sinnvoll erscheint es, auf technische Entwicklungen stets mit neuen bereichsspezifischen Vorgaben zu reagieren. Auf gesetzlicher Seite sollte auf in der Rechtsordnung anerkannte, unbestimmte, technikneutrale Rechtsbegriffe abgestellt werden. Diese ermöglichen im Zusammenspiel mit den Regelungen zur Interessenabwägung (siehe oben 2 c) die Beurteilung auch neuer technischer Entwicklungen.

Entscheidende Bedeutung für eine praktisch datenschutzgerechte Handhabung technischer Entwicklungen kommt der Selbstregulierung im Datenschutz zu. Insoweit sind die betroffenen Hersteller und Anwender zur Gewährleistung eines von der Gesellschaft akzeptierten Umfangs der Datenverarbeitung gefordert, zunächst eigenverantwortlich die Grundsätze des Datenschutzrechts bezogen auf die Technik zu konkretisieren.

Auf Herausforderungen für den Datenschutz durch die technische Entwicklung sollte auch eine technikorientierte Lösung gefunden werden. Der Datenschutz sollte bereits Bestandteil von Produkten und Diensten sein. Ein entscheidendes Instrument zur Umsetzung dieser Forderung stellt eine anerkannte Zertifizierung datenschutzkonformer Produkte wie Hard- und Software nach einem Produkt-Audit dar. (siehe auch die Ausführungen zum Themenkreis 2).

### *5. Neuregelung des technisch-organisatorischen Datenschutzes*

Gesetzgeberisch ist jedoch eine Neuregelung der Grundsätze zum technisch organisatorischen Datenschutz im BDSG angezeigt. Die Regelung des § 9 und Anlage ist durch Maßnahmeorientierung gekennzeichnet, die ihrerseits weitgehend auf die Großrechnerwelt abstellt. Deshalb sollten die bisherigen maßnahmenorientierten Regelungen abgelöst und durch die technikneutralen Sicherheitsziele Vertraulichkeit, Integrität, Verfügbarkeit und Revisionsfähigkeit ersetzt werden. Insoweit sind einige Landesdatenschutzgesetze (Nordrhein-Westfalen, Berlin, Hamburg, Mecklenburg-Vorpommern, Sachsen-Anhalt, Thüringen) ein Vorbild für die rechtliche Neugestaltung des technisch-organisatorischen Datenschutzes. Beibehalten werden sollte jedoch der Grundsatz der Angemessenheit und der Verhältnismäßigkeit der technisch-organisatorischen Maßnahmen, die auf Grundlage einer unternehmensspezifischen Gefährdungsanalyse zu treffen sind.

### *6. Transparenz der Datenverarbeitung*

Wesentlicher Akzeptanzfaktor für den Umgang mit personenbezogenen Daten ist die Transparenz für den Betroffenen. Diese ist insbesondere durch Informations-, Aufklärungs-, Benachrichtigungs- und Auskunftspflichten in der EG-Datenschutzrichtlinie und der Kommunikationsdatenschutzrichtlinie und damit im BDSG und im bereichspezifischen Datenschutzrecht ausreichend geregelt. In der Praxis sind jedoch Vollzugsdefizite zu konstatieren.
Die Transparenz muss das Ziel haben, den Betroffenen ausreichend über den Umfang des Umgangs mit seinen Daten zu informieren. Die Transparenz der Datenverarbeitung findet jedoch ihre Grenze in der allgemeinen Verständlichkeit. Von daher ist die Forderung nach einer gesetzlichen Regelung zur Veröffentlichung der Struktur der Verarbeitung personenbezogener Daten auf Betriebssystemebene wenig sinnvoll.

### *7. Stärkung des betrieblichen und behördlichen Datenschutzbeauftragten*

Die Compliance der Unternehmen und Behörden mit den Datenschutzanforderungen wird von deren Datenschutzbeauftragten wahrgenommen. Insofern sind die vielfältigen datenschutzrechtlichen Vorgaben der EG-Datenschutzrichtlinie bzw. nationalen Datenschutzgesetze organisatorisch personifiziert.

Die Verpflichtung zur Bestellung eines Datenschutzbeauftragten stellt für die Unternehmen keinen bürokratischen Aufwand dar. Im Gegenteil wird durch die Bestellverpflichtung die europarechtliche Vorgabe eine Meldung der Datenverarbeitung an staatliche Meldebehörden in der Regel ersetzt.
Die europarechtlich geforderte Unabhängigkeit des betrieblichen Datenschutzbeauftragten ist im BDSG weitgehend konkretisiert worden. Probleme in der Praxis ergeben sich auf Grund von Vollzugsdefiziten. Eindeutig gesetzlicher Handlungsbedarf besteht jedoch hinsichtlich der Ausstattung des betrieblichen Datenschutzbeauftragten. Bisher sind ihm nach dem BDSG „Hilfspersonal, Räume, Einrichtungen, Geräte und Mittel“ zur Verfügung zu stellen. Gesetzlich nicht aufgenommen wurde der Zeitfaktor für die Wahrnehmung der Aufgaben des Datenschutzbeauftragten. Eine Umfrage der GDD aus dem Jahr 2004 belegt, dass Datenschutzbeauftragte in der Regel neben dieser Funktion andere Aufgaben im Unternehmen wahrnehmen. Vielfach geäußerte Defizite hinsichtlich des mit der Wahrnehmung dieser Funktion anfallenden zeitlichen Aufwandes geben Veranlassung, den Faktor „Zeit“ in die Mittelausstattung des Datenschutzbeauftragten gesetzlich zu ergänzen.

Weiterhin sollte der Gesetzgeber die Funktion eines Konzerndatenschutzbeauftragten gesetzlich regeln. Die erleichterte Bestellung eines Datenschutzbeauftragten im Konzern würden entsprechende bürokratische Einzelbestellungsakte verhindern. Zudem kann über Konzerndatenschutzbeauftragte die Rolle des Datenschutzes im Konzernverbund gestärkt werden.

Dringend regelungsbedürftig ist das Verhältnis des betrieblichen Datenschutzbeauftragten zur Mitarbeitervertretung. Nach dem Urteil des Bundesarbeitsgerichtes vom 11.11.1997 hat dieser kein Kontrollrecht bei der Mitarbeitervertretung. Dieses führt zu einem unter Datenschutzgesichtspunkten kontrollfreien Bereich im Unternehmen. Im übrigen gibt es Wertungswiderspruch zur EG-Datenschutzrichtlinie, die den Datenschutzbeauftragten zur Führung der meldepflichtigen Informationen des gesamten Unternehmens verpflichtet und die Mitarbeitervertretung von entsprechenden internen Meldepflichten nicht ausnimmt. Hier sollte der Gesetzgeber zumindest ein Recht des Datenschutzbeauftragten zur Kontrolle der Mitarbeitervertretung hinsichtlich der Wahrung der gesetzlichen Betroffenenrechte regeln.

## *Zum Themenkreis 2.: „Datenschutz-Audit“*

### *1. Gegenstand der Auditierung*

Der sachliche Anwendungsbereich der Ermächtigungsnorm für ein Datenschutzauditgesetz in § 9a BDSG bezieht sich auf Anbieter von Datenverarbeitungssystemen und -programmen und Daten verarbeitende Stellen, wobei Prüfungsgegenstand das Datenschutzkonzept sowie die technischen Einrichtungen sind.

Die GDD hat das Thema Datenschutzaudit in ihren Erfa-Kreisen mit ca. 1.000 Datenschutzverantwortlichen eingehend diskutiert. Danach wird die gesetzliche Regelung eines freiwilligen Produkt- sowie eines Dienstleistungsaudits im nicht öffentlichen Bereich befürwortet. Die Auditierung gesamter Unternehmen oder interner Verfahren wird dagegen als nicht sinnvoll anzusehen, da lediglich ein bürokratischer Aufwand ohne Wettbewerbsvorteil für das Unternehmen absehbar ist.

### *2. Maßstab der Auditierung*

Die Inhalte eines Produktaudits bedürfen einer detaillierteren Regelung. Beispiele für die Methodik der Erarbeitung des Anforderungskatalogs für ein Produktaudit bieten die vom BSI und BfDI entwickelten Schutzprofile auf Basis von ISO/IEC 15408.

Im Bereich des Dienstleistungsaudits kommen vor allem Auftragsnehmer im Rahmen einer Auftragsdatenverarbeitung gem. § 11 BDSG in Betracht. Ein Gütesiegel hinsichtlich der Datenschutzkonformität der angebotenen Dienstleistung erleichtert auf der Auftraggeberseite die gesetzlich geforderte sorgfältige Auswahl. Auf der Auftragnehmerseite kann die Zertifizierung der Datenschutzkonformität der angebotenen Dienstleistung als Qualitäts- und Wettbewerbsvorteil genutzt werden.

Maßstab der Auditierung sollte die Erfüllung der datenschutzrechtlichen Normen sein. Sowohl beim Produkt- als auch beim Dienstleistungsaudit liegt dabei der Schwerpunkt auf der Erfüllung der technisch-organisatorischen Maßnahmen im Rahmen der Verhältnismäßigkeit. Eine Übererfüllung der gesetzlichen Vorgaben als Voraussetzung für die Zertifizierung wird von der GDD abgelehnt. Die gesetzlichen Datenschutzanforderungen sind keine Mindestanforderung sondern entsprechen dem jeweiligen Schutzzweck und Schutzbedürfnis.

### *3. Zertifizierungsstelle*

Der Schwerpunkt des Produkt- und Dienstleistungsaudits liegt, wie oben aufgeführt, im Bereich der Erfüllung der technischen und organisatorischen Anforderungen. Von daher bietet sich an, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) die Funktion als Zertifizierungsstelle zuzuweisen.
Gegen die Übertragung der Aufgaben der Zertifizierungsstelle auf die Datenschutzaufsichtsbehörden spricht eine Inkompatibilität mit ihren Kontrollaufgaben nach § 38 BDSG. Zertifizierung und Kontrolle sollten nicht auf eine Stelle vereinigt werden. Dieselben Argumente sprechen auch gegen eine Benennung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) als Zertifizierungsstelle.
Die Akkreditierung der Auditoren sollte zur Vermeidung der Errichtung neuer Instanzen von einer bereits bestehenden Institution mit entsprechenden Erfahrungen vorgenommen werden. Hier bietet sich die IHK-Organisation an, der gesetzlich die öffentliche Bestellung und Vereidigung von Sachverständigen zugewiesen ist. Der DIHK hat gegenüber dem Bundesministerium des Innern bereits seine Bereitschaft zur Mitwirkung am Auditverfahren signalisiert.

### *4. Der Datenschutzbeauftragte im Auditverfahren*

Der betriebliche Datenschutzbeauftragte ist nach den Vorgaben der EG-Datenschutzrichtlinie und der entsprechenden Umsetzung im BDSG im Rahmen seiner Aufgabenwahrnehmung unabhängig. Im Rahmen des Auditierungsverfahrens muss dieser Grundsatz gewahrt bleiben. Deswegen sollte der Datenschutzbeauftragte nicht originär Gegenstand der Auditierung sein. Seine Einbindung in den Prozess der Auditierung sollte aber rechtlich sichergestellt werden.

## *Zum Themenkreis 3.: „Scoring und Unternehmensinformationspflicht bei Datenschutzpannen“*

## *I. Zum Thema „Scoring“*

Scoringsysteme stellen für die Wirtschaft ein unverzichtbares Instrument dar, um bei Massengeschäften das vermutliche Verhalten potenzieller Kunden sowie das mit der Vertragsvergabe einhergehende Risiko sachgerecht einschätzen zu können. Aus Sicht des Kunden ist es aber erforderlich, dass die Verfahren für ihn eine entsprechende Transparenz aufweisen und er zudem über angemessene Möglichkeiten zur Korrektur von Fehleinschätzungen verfügt, die daraus resultieren, dass lediglich statistische Wahrscheinlichkeiten zu Grunde gelegt worden sind.

### *1. Zur Begrenzung der beim Scoring verwandten Informationen*

Das Scoring darf ausschließlich auf Grundlage valider statistischer Methoden erfolgen. Insoweit begrenzen bereits die bestehenden Erlaubnisnormen des BDSG die Datennutzung. Eine gesetzliche Regelung zur Begrenzung ausschließlich auf Vermögens- und Zahlungsinformationen der beim Scoring verwandten Informationen ist je nach Zweck des Scorings (z.B. Werbe-, Marketing- oder Fraud-Scoring) nicht zielführend.

Zur Klarstellung dieses Sachverhalts kann im BDSG in der Regelung zur automatisierten Einzelentscheidungen (§ 6a BDSG) eine Vorschrift ergänzend aufgenommen werden, die Scoringverfahren von allgemeinen Auswahlverfahren differenziert. Insoweit können Scoringverfahren i.S.v. elektronischen Bewertungsverfahren von einem berechtigten Interesse der verantwortlichen Stelle und anerkannten wissenschaftlichen Methoden abhängig gemacht werden.

Ein genereller gesetzlicher Ausschluss potenziell diskriminierender Merkmale wie ethnische Zugehörigkeit, Geschlecht, Alter, Nationalität bei jeder Form des Scorings ist nicht sachgerecht. Bei der Verwendung dieser Informationen ist der Sachzusammenhang und das Ziel des Scorings entscheidend. So kann es durchaus sinnvoll sein, im Rahmen eines Scorings bestimmte Gruppen auszuschließen, wenn die Entscheidung für die Personengruppen mit den jeweiligen potenziellen Diskriminierungsmerkmalen nicht sinnvoll oder nicht zu vereinbaren wäre (z.B. Millionenkredit für finanzschwachen Hundertjährigen). In Hinblick auf die Verwendung potenziell diskriminierender Merkmale sind somit die Zulässigkeitsregeln des BDSG bzw. des Allgemeinen Gleichbehandlungsgesetzes (AGG) ausreichend.

### *2. Transparenz hinsichtlich der gewonnen Scorewerte*

Bei der Beurteilung der Transparenzanforderungen hinsichtlich der Funktionsweise der Scoringsysteme ist eine Abwägung zwischen einem anerkennungswerten Informationsinteresse des Betroffenen auf der einen Seite und den Betriebs- und Geschäftsgeheimnissen der Scoreanbieter auf der anderen Seite vorzunehmen. Im Übrigen gilt es zu beachten, dass durch die Kenntnis der scorebildenden Merkmale auch die Möglichkeit eröffnet wird, die Ergebnisse von Scoringverfahren zu manipulieren.

Vor diesem Hintergrund ist aus Sicht der GDD zu erwägen, die entscheidungserheblichsten Merkmale offen zu legen. Insoweit könnte die Regelung der automatisierten Einzelentscheidung (§ 6a BDSG) in ihrem Absatz 3, der die Transparenzanforderungen regelt, ergänzt werden.

Bei dieser Transparenzregelung ist zu berücksichtigen, dass ein Score-Wert eine Gesamtbetrachtung auf Basis der Kombination aller eingeflossenen Merkmale darstellt. Über die Datenbasis kann der Betroffene sich aufgrund seines Auskunftsrechts nach § 34 BDSG informieren. Hieraus wird für ihn jedoch nicht ersichtlich, wie die Gewichtung der Merkmale erfolgt. In aller Regel lassen sich jedoch, etwa bei Kreditentscheidungen, aber die Hauptmerkmale identifizieren. Wenn der Betroffene diese Hauptmerkmale kennt, kann er beurteilen, auf welchen Annahmen der Scorewert beruht.

Allerdings müssen bei einer solchen zusätzlichen Transparenzregelung verschiedene weitere Aspekte berücksichtigt werden: Aufgrund der Faktoren Zeitpunkt der Bildung des Scorewertes und des individuellen Datenbestandes ist der Scorewert zum Zeitpunkt der Abfrage flüchtig. Daher sind mit erheblichen technischen Aufwand die Systeme so zu gestalten, dass die Momentaufnahme der Abfrage nachvollziehbar gespeichert werden kann, um hieraus die entscheidungserheblichsten Merkmale zeit- und personenindividuell ableiten zu können. Diese Umstellung ist absehbar zeit- und kostenintensiv. Zudem sind für diese zusätzlich zu speichernden Daten datenschutzrechtliche Rahmenbedingungen insbesondere hinsichtlich der Nutzungsbedingungen und Speicherdauer zu schaffen.

Die vorgeschlagene Transparenzanforderung im Rahmen des § 6a BDSG gilt sowohl bei der eigenständigen Nutzung von Informationen für das Scoring als auch bei der Einschaltung von Dritten, die als Dienstleister fungieren

## *II. Zum Thema „Unternehmensinformationspflicht bei Datenschutzpannen“*

### *1. Unbestimmtheit des Antrags*

Zunächst ist festzustellen, dass der Antrag von BÜNDNIS 90/Die GRÜNEN hinsichtlich des Auslösungsfalls der angeregten Informationspflicht relativ unbestimmt ist. Was mit dem Begriff „Datenschutzpannen“ genau gemeint ist, ist nur bedingt erkennbar zumal der Antrag insofern unterschiedliche Begriffe verwendet. So ist unter Gliederungspunkt I. 2. die Rede von unsachgemäßem Umgang mit Daten Betroffener. Unter Gliederungspunkt I. 4. ist zum einen die Rede von datenschutzrechtlichen Sicherheitsverletzungen und zum anderen von fahrlässigem oder rechtswidrigem Handeln im Rahmen der Verwaltung von Kundendaten. Unter Punkt II. 1., wo eine BDSG-Änderung angeregt wird, geht es dann um die Verletzung von Sorgfaltspflichten bei der Erhebung, Speicherung und Verwertung personenbezogener Daten. Würde der Deutsche Bundestag einen gesetzgeberischen Handlungsbedarf hinsichtlich der Schaffung der in Rede stehenden Informationspflichten sehen, wären die Auslösungsfälle dieser unternehmerischen Pflichten dem verfassungsrechtlichen Bestimmtheitsgrundsatz entsprechend zu konkretisieren.

Ergänzend sei darauf hingewiesen, dass der Antrag auch in Bezug auf die Ausgestaltung einer Informationspflicht wenig Konkretes beinhaltet. So werden beispielsweise Fragen zum Zeitpunkt und zur Form der Information gar nicht angesprochen.

### *2. Regelungsbedarf und -standort*

Primär sollte nach Auffassung der GDD geklärt werden, ob angesichts der im Bundesdatenschutzgesetz (BDSG) bereits geregelten Pflichten überhaupt weiterer gesetzgeberischer Handlungsbedarf hinsichtlich einer BDSG-Änderung besteht.

In diesem Zusammenhang wird darauf hingewiesen, dass das BDSG in § 4 Abs. 1 bereits ein grundsätzliches Datenverarbeitungsverbot mir Erlaubnisvorbehalt enthält, das durch vom Unternehmen zu treffende technisch-organisatorische Datensicherheitsmaßnahmen (§ 9

BDSG und Anlage) flankiert wird. Daneben enthält das BDSG in den §§ 43, 44 auch ordnungs- und strafrechtliche Sanktionen für fahrlässige bzw. vorsätzliche Pflichtverletzungen beim Umgang mit personenbezogenen Daten. Darüber hinaus sieht § 7 BDSG auch Schadensersatzansprüche im Falle unzulässiger oder unrichtiger Datenverarbeitung vor.

Es erscheint zweifelhaft, ob das BDSG überhaupt der richtige Regelungsstandort für die vorgeschlagene Informationspflicht wäre. Das BDSG bezweckt primär den Schutz personenbezogener Daten. Jedenfalls die Frage eines (Mit-) Verschuldens der Daten verarbeitenden Stellen im Falle deliktischer Handlungen Dritter (z. B. bei Identitätsdiebstählen) ist eher eine (neben-) vertragliche bzw. zivilrechtliche Haftungsfrage.

### *3. Prinzip der Verhältnismäßigkeit*

In jedem Fall müsste eine Informationsregelung dem Prinzip der Verhältnismäßigkeit Rechnung tragen.

Sie müsste zunächst geeignet sein, die Betroffenen vor materiellen Schäden oder Persönlichkeitsrechtsverletzungen zu bewahren. Der Bedeutung des Problems nicht gerecht werdende Informationspflichten, die lediglich darauf abzielen die Unternehmen „öffentlich und umfassend“ anzuprangern wären demgegenüber keine legitimen Zwecke. Vielmehr müsste es darum gehen, die Betroffenen in die Lage zu versetzen, selbst Schutzmaßnahmen zur Verhinderung von weiterem Datenmissbrauch zu ergreifen.

Aus Sicht der GDD ist ferner allenfalls eine Regelung zur Abwendung von erheblichen materiellen Schäden oder empfindlichen Persönlichkeitsrechtsverletzungen angezeigt. Eine derartige Begrenzung, die der Antrag nicht vorsieht, ist notwendig, um die Belastung der Unternehmen angemessen zu begrenzen. Gleichzeitig würden aber die Rechte der Betroffenen gestärkt.

Wie bereits festgestellt (s. o. unter 1.), enthält der Antrag weder Ausführungen zum Auslösungsfall noch zur näheren Ausgestaltung einer Informationsverpflichtung. Danach würde jedwede Sorgfaltspflichtverletzung beim Umgang mit personenbezogenen Daten – ungeachtet des Ausmaßes eines möglichen Schadens des Betroffenen – die Unterrichtungspflicht auslösen können. Eine derart undifferenzierte Regelung wäre unangemessen.

Es dürfte keine zwingende Notwendigkeit bestehen, den Betroffenen zu informieren, wenn lediglich die Vertraulichkeit relativ unsensibler Daten (z. B. dienstliche E-Mail-Adresse) in Rede steht, und daher kein oder kaum ein nennenswerter Schaden des Betroffenen zu erwarten ist. Vielmehr wäre es sowohl aus Sicht der Unternehmen als auch aus der Perspektive der Betroffenen geradezu kontraproduktiv, wenn auch bei minimalen Zwischenfällen mit geringem Risiko massenhaft zu informieren wäre. Zu bedenken ist einerseits die damit Verbundene Belastung der Unternehmen; so sind Fälle bekannt, in denen die Rückfragen besorgter Betroffener ohne Call-Center-Support gar nicht zu bewältigen gewesen wären. Dieser Aufwand stünde andererseits in keinem Verhältnis zu seinem Nutzen; vielmehr kann von Nutzen gar keine Rede sein, wenn unnötige Bedenken geweckt werden müssten.

Im Fall der Information zur Abwendung erheblicher materieller Schäden oder empfindlicher Persönlichkeitsrechtsverletzungen müsste den Unternehmen ein angemessener Zeitraum für die Unterrichtung der Betroffenen zur Verfügung stehen. Hinsichtlich der Form der Information müssten den Unternehmen zumutbare und zeitgemäße Kommunikationsformen zur Verfügung stehen.

Schließlich weist die GDD auf die Möglichkeit zur Regelung bereichspezifischer Informationspflichten und darauf hin, dass auch Erkenntnisse aus der aktuell geführten Diskussion der Problematik im Zusammenhang mit einer Revision des EU-Rechtsrahmens für elektroni-

sche Kommunikation berücksichtigt werden sollten. Würden in den Mitgliedstaaten unterschiedliche Informationspflichten geregelt, wären Wettbewerbsverzerrungen zu befürchten.

Nach alledem sollte dem Antrag von Bündnis 90/DIE GRÜNEN in seiner bisherigen Form aus Sicht der GDD nicht zugestimmt werden.