Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
16(4)176 C

verbraucherzentrale Bundesverband

Datum: 26.02.2007

Stellungnahme des Verbraucherzentrale Bundesverbands (vzbv) zur öffentlichen Anhörung im Innenausschuss des Deutschen Bundestages am 5. März 2007 zum Thema: Modernisierung des Datenschutzes

Der Datenschutz ist ein wesentliches Instrument, um die informationelle Selbstbestimmung der Bürger zu gewährleisten. Häufig wird argumentiert, dass die deutschen Datenschutzgesetze selbst im europäischen Vergleich vorbildlich sind und ein hohes Schutzniveau garantieren, so dass kein Verbesserungsbedarf besteht. Meist basieren solche Bewertungen allerdings auf der rechts*theoretischen* Analyse der Datenschutzgesetze. Die *Praxis* sieht eher ernüchternd aus. Defizite werden durch ausufernde Begehrlichkeiten von Seiten des Staates, durch eine Zunahme der Begehrlichkeit privater Stellen und durch technologische Entwicklungen hin zur allgegenwärtigen Datenverarbeitung weiter verschärft.

Unsere Stellungnahme ist in drei Abschnitte unterteilt, die sich an der Tagesordnung der Anhörung orientieren. Im ersten Abschnitt zur Modernisierung des Datenschutzes fordern wir:

- die ausufernde Begehrlichkeit des Staates zu begrenzen;
- die Datenschutzgesetze an neue Herausforderungen anzupassen und eine Vereinheitlichung der Datenschutzgesetzgebung vorzunehmen;
- das Prinzip der Einwilligung zu stärken;
- die Koppelungen ausdrücklich zu verbieten;
- die Rechtsdurchsetzung zu verbessern;
- zu klären, wie mit personen*beziehbaren* Daten umzugehen ist;
- und bessere Kontroll- und Sanktionsmöglichkeiten zu schaffen.

Im zweiten Abschnitt geht die Stellungnahme auf das Datenschutzaudit ein und stellt dar, warum es aus Verbrauchersicht geboten ist, ein Ausführungsgesetz für § 9a Satz 2 BDSG zu verabschieden. Das Datenschutzaudit sollte als ein marktwirtschaftliches Instrument für eine Verbesserung des Datenschutzes und der -sicherheit gefördert werden.

Im dritten Abschnitt zum Scoring zeigen wir zum Teil gravierende Defizite und Verstöße gegen § 6a BDSG auf und fordern weitgehende Transparenzrechte für Verbraucher insbesondere in Hinblick auf eine Offenlegung der Scoringverfahren. Was die Einführung von Informationspflichten bei Datenschutzpannen angeht, wäre zu prüfen, ob bestehende Gesetze nicht bereits heute ausreichen.

Bundesverband der Verbraucherzentralen
und Verbraucherverbände
Verbraucherzentrale Bundesverband e. V.

1) Modernisierung des Datenschutzes

Das Grundrecht auf informationelle Selbstbestimmung ist Bestandteil des allgemeinen Persönlichkeitsrechts und genießt damit Verfassungsrang. Ein Datenschutz auf hohem Niveau hat gleichzeitig viel mit Verbraucherschutz zu tun. Er sorgt für einen effektiven Schutz vor belästigender Werbung, vor einer intransparenten Datenerhebung, die mit Hilfe von Scoringverfahren gegen die Verbraucher verwendet werden kann, vor Identitätsklau und anderen Formen des Datenmissbrauchs im Internet. Allerdings wird der Datenschutz durch eine Reihe aktueller Entwicklungen herausgefordert.

a) Die ausufernde Begehrlichkeit des Staates begrenzen

Oberster Maßstab für die Beurteilung eines umfassenden und effektiven Datenschutzes ist die informationelle Selbstbestimmung. Der Bürger/Verbraucher muss selbst entscheiden können, welche Daten er wem und zu welchem Zweck gibt. Maßnahmen der Bundesregierung (und der EU) im Rahmen des so genannten Antiterrorkampfes haben in den vergangenen Jahren zu einer zunehmenden Aushöhlung des Grundrechts auf informationelle Selbstbestimmung geführt. Vorläufiger Kulminationspunkt dieser problematischen Entwicklungen ist das Vorhaben der „Vorratsdatenspeicherung", einer nicht anlassbezogenen massenhaften Speicherung von Daten aller Bürger über alle Kommunikationsnetze und über einen langen Zeitraum.

Wir fordern die Bundesregierung auf, bei Maßnahmen zur Terrorabwehr die Verhältnismäßigkeit zu wahren und nicht gegen Grundrechte zu verstoßen. Daher lehnen wir insbesondere eine nicht-anlassbezogene Vorratsdatenspeicherung ab. Die vom BMJ jüngst vorgelegte Entwurfsfassung greift tief in das Recht auf informationelle Selbstbestimmung jedes Bürgers ein. Wir befürchten, dass eine Umsetzung des Referentenentwurfs Verbraucherinteressen gerade in der Telekommunikation, in der das Fernmeldegeheimnis das grundlegende Prinzip darstellt, massiv verletzen würde.

b) Anpassung der Datenschutzgesetze an neue Herausforderungen und Vereinheitlichung

Die Datenschutzgesetze sind erst in den letzten Jahrzehnten entstanden. Stand bis Ende der 90er Jahre die Verhinderung des Datenmissbrauchs durch *öffentliche* Stellen im Vordergrund und basierte die Datenschutzgesetzgebung auf der Prämisse der Vermeidung von Datenerfassung und -verarbeitung, ist die Datenschutzgesetzgebung heute in dreifacher Hinsicht herausgefordert.

Zum einen wird die informationelle Selbstbestimmung zunehmend durch *private* Stellen ausgehöhlt. Einige Zahlen illustrieren diese Entwicklung:

- der Markt für individualisiertes Marketing wächst rasant: 2004 gaben Unternehmen in Deutschland 25 Mrd. Euro fürs Direktmarketing aus. Innerhalb eines Jahres wuchs der Umsatz um knapp 30 Prozent auf 32 Mrd. Euro;
- das Wirtschafsmagazin Capital hat errechnet, dass allein die vier größten Auskunfteien der Wirtschaft jährlich mehr als 140 Millionen Datensätze über Verbraucher liefern – Tendenz steigend;
- jeder Bundesbürger über 18 Jahren in durchschnittlich 52 *kommerziellen* Datenbanken erfasst ist.

Diese Entwicklungen zeigen, dass die in der Wirtschaft gesammelten und genutzten Daten die Privatsphäre mindestens so stark gefährden, wie die von öffentlichen Dienststellen gespeicherten Informationen.

Zum anderen fordern technische Entwicklungen den Datenschutz heraus. Die Digitalisierung unserer Lebenswelt schreitet stetig voran und das Szenario eines allgegenwärtigen Datenaustauschs zwischen Objekten und Subjekten – was mit dem Stichwort ubiquitous computing beschrieben wird – nimmt u.a. mit der Entwicklung der RFID-Technologie konkrete Form an. Die bisherigen Grundanforderungen, dass die Datenerfassung transparent zu erfolgen hat, dass eine Einwilligung vorliegen muss, dass es eine Zweckbestimmung in der Datenverarbeitung geben muss und auch das Gebot der Datensparsamkeit müssen mit den technischen Entwicklungen mithalten.

Schließlich wird die Anwendung des Datenschutzrechts dadurch erschwert, dass der Datenschutz nicht in einem Gesetz gebündelt, sondern in zahlreichen bereichsspezifischen Regelungen zerfasert ist. Das erschwert Verbrauchern und Unternehmern den Überblick über Ihre Rechte und Pflichten.

Daher fordern wir eine Anpassung der Datenschutzgesetze an die neuen Herausforderungen und eine Vereinheitlichung dieser Regelungen. Damit die Ökonomisierung des Datenschutzes, die o.g. technologischen Entwicklungen und die Zergliederung nicht zu einer Aushöhlung des Datenschutzes führen, ist es erforderlich, dass die Datenschutzgesetzgebung modernisiert und auf einem hohen Schutzniveau vereinheitlicht wird. Hierbei sollten die Anforderungen an Transparenz, Einwilligung, Zweckbegrenzung und Datensparsamkeit neu definiert werden und Möglichkeiten für den Selbstschutz in Form von Anonymisierung und Pseudonymisierung verbessert werden. Auch sollten das Datenschutzrecht auf ein allgemeines Recht gegründet und bereichsspezifische Regelungen auf ein Minimum reduziert werden.

c) Prinzip der Einwilligung stärken

Nach dem BDSG sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten verboten, es sei denn, sie sind durch das BDSG oder eine andere Rechtsvorschrift ausdrücklich erlaubt oder angeordnet oder der Betroffene hat dazu seine Einwilligung erklärt. Wichtig bei der freiwilligen Einwilligung ist, dass diese (i) in Schriftform erfolgt, (ii) der Betroffene über die Tragweite seiner Entscheidung aufgeklärt ist und (iii) die Einwilligung freiwillig, d.h. frei von Zwang, erfolgt.

Ein Gutachten des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, das der Verbraucherzentrale Bundesverband in Auftrag gegeben hat, stellt fest, dass es bei fast allen Kundenkartenprogrammen, die in der Studie untersucht wurden, zum Teil gravierende Verstöße gegen Datenschutzregelungen gab. Zu den häufigsten Verstößen zählen das unverhältnismäßig umfangreiche Sammeln von Daten, eine fehlende Information der Verbraucher über ihre Datenschutzrechte und unzureichende Einwilligungserklärungen über die Verwendung der Daten.

Ein aktuelles Beispiel für die Unzulänglichkeit der bestehenden Gesetze ist der Branchenführer *Payback*. Der vzbv interpretiert das BDSG dahingehend, dass die freiwillige Einwilligung zur Datenverarbeitung eine aktive Handlung der Betroffenen voraussetzt. Diese drückt sich in dem so genannten Opt-In aus. Die Praxis bei *Payback* entspricht jedoch dem Opt-Out. Hier wird

standardmäßig die Einwilligung der Verbraucher zur Verwendung der Daten zu Werbezwecken vorausgesetzt. Will der Verbraucher nicht einwilligen, muss er eine aktive Handlung des *Auskreuzens* vollziehen. Der vzbv sieht den Grundsatz der Freiwilligkeit hiermit auf den Kopf gestellt und hat daher Klage gegen *Payback* eingereicht. Der vzbv bekam in der ersten Instanz vom LG München I Recht. Dem konnte sich jedoch die Berufungsinstanz (OLG München) nicht anschließen.

Die Bedeutung des Unterschieds zwischen einer Opt-In und einer Opt-Out-Regelung wird durch Untersuchungen illustriert. In diesen Studien wird festgestellt, dass lediglich ca. 20 Prozent der Verbraucher bei einem Ankreuz-Verfahren die Einwilligung zur Verwendung der Daten für Werbezwecke erteilen würden. Sind sie jedoch gehalten, eine Einwilligung zurückzuziehen, dann tun dies nur 20 Prozent. Das heißt, dass die Art der Formulierung der Einwilligung einen wesentlichen Einfluss darauf hat, wie viele Verbraucher diese Einwilligung erteilen. Der Grund hierbei dürfte darin zu finden sein, dass Verbraucher es zum einen nicht gewohnt sind, in Verträgen Dinge zu streichen und zum anderen befürchten, dass die Streichung der Einwilligung dazu führen könnte, dass sie dann keine Rabattpunkte mehr bekommen.

Daher fordert der vzbv, im BDSG klar zu stellen, dass die Verwendung von personenbezogenen Daten für jeden anderen Zweck als zur Vertragserfüllung von der freiwilligen und expliziten Einwilligung des Betroffenen abhängig ist. Eine solche Einwilligung wird durch das Opt-In zum Ausdruck gebracht.

d) Koppelung ausdrücklich verbieten

Das Prinzip der informationellen Selbstbestimmung basiert auf der *Freiwilligkeit* der Einwilligung zur Weitergabe von Informationen. Es gibt jedoch Fälle, in denen ein Vertragsschluss von der Einwilligung der Verwendung personenbezogener Informationen, die über die Informationen, die zur Vertragserfüllung notwendig sind, hinausgehen, abhängig gemacht wird. Hierbei wird u.a. §3 Abs. 4 des Teledienstedatenschutzgesetzes ausgenutzt, der besagt, dass Unternehmen keine Koppelung vornehmen dürfen, es sei denn, es gibt andere Anbieter, auf die der Verbraucher ausweichen kann. Jüngstes Beispiel hierfür ist *Ebay*. *Ebay* macht die Nutzung seiner Plattform von der Einwilligung zur Verwendung persönlicher Daten zu Werbezwecken abhängig. Gegen diese Praxis hat der vzbv Klage erhoben und in erster Instanz verloren. Das OLG Brandenburg hat die Berufung zurückgewiesen und die Revision nicht zugelassen, so dass das Urteil rechtskräftig ist. Die Begründung des Gerichts lautet, dass eine Monopolstellung in Bezug auf die von *Ebay* angebotenen Teledienste nicht angenommen werden und der Verbraucher auf ein anderes Angebot zurückgreifen könne. Hiermit fällt das Teledienstedatenschutzgesetz hinter das Schutzniveau des BDSG zurück. – Das Telemdediengesetz hat diese Schutzlücke nicht geschlossen.

Daher fordern wir ein ausdrückliches Kopplungsverbot. Ein Vertragsschluss darf nicht von der Weiterverarbeitung von Daten, die nicht für die Vertragserfüllung erforderlich sind, abhängig gemacht werden. Verbraucher dürfen bei der Entscheidung, ein Produkt zu kaufen, nicht gezwungen werden, personenbezogene Daten weiterzugeben. Eine datenschutzrechtliche Einwilligungserklärungen, mit denen der Kunde erst kurz vor Vertragsabschluss konfrontiert wird, setzt ihn unter einen erheblichen Einwilligungsdruck, weil sich der Kunde zu diesem Zeitpunkt häufig bereits für das jeweilige Produkt entschieden hat. In dieser Situation fällt es in der Regel

schwer, die datenschutzrechtliche Dimension des Vertragsschlusses angemessen zu berücksichtigen. Gerade in der Hektik des kommerziellen Alltags kann der Kunde die Tragweite einer Einwilligung und die damit verbundenen Konsequenzen häufig gar nicht erkennen. Viele Kunden wissen nicht, dass sie mit einer einzigen Unterschrift eine Kette von Werbung, Erfassung der Einkaufsgewohnheiten und eine Weitergabe der Daten an Dritte mit Konsequenzen für spätere Vertragsabschlüsse in Gang setzen. Gekoppelte Einwilligungen sind dem Kunden deshalb in aller Regel leichter zu entlocken. Personenbezogene Daten sind keine Ware wie jede andere. Verbraucher müssen daher Entscheidungen frei von datenschutzfremden Zwängen treffen können. Um einer fortschreitenden Aushöhlung des Rechts auf informationelle Selbstbestimmung durch rein kommerzielle Interessen entgegenzuwirken, halten wir ein Koppelungsverbot im BDSG für dringend erforderlich.

e) Rechtsdurchsetzung verbessern

Da das BDSG und das Telemediengesetz (bisher Teledienstedatenschutzgesetz) von der Rechtsprechung bislang nicht als Verbraucherschutzgesetze angesehen werden, haben Verbraucherorganisationen nur sehr eingeschränkte Möglichkeiten, gegen Verstöße vorzugehen. So können Verbraucherorganisationen zwar heute über AGB-Verfahren beispielsweise gegen das fehlende Opt-In oder die Kopplung vorgehen, nicht jedoch gegen die gesetzeswidrige Verarbeitung von Daten.

Daher fordern wir eine Anerkennung des BDSG und anderer Datenschutzgesetze als Verbraucherschutzvorschriften. Verbraucherorganisationen müssen das Recht erhalten, auch gegen Verstöße, die über AGB-Verstöße hinausgehen, vorzugehen.

f) Klärung, wie mit personen*beziehbaren* Daten umzugehen ist

Eine breite und intensive Nutzung des Internets und der RFID-Technologie erleichtert es, anhand von personen*beziehbaren* Daten Kundenprofile zu erstellen. Personenbeziehbare Daten sind Daten, die indirekt auf eine Person bezogen werden können. Nach unserer Auffassung sind solche personenbeziehbare Daten als personenbezogene Daten einzustufen. Hierüber gibt es allerdings große Unklarheit, die sowohl im Sinne der Verbraucher als auch der Wirtschaft ausgeräumt werden sollten.

Ein Beispiel für die Gefahr, wie Informationen, die für sich genommen keine personenbezogene Daten enthalten, durch eine Verknüpfung sehr wohl einen Personenbezug ermöglichen, liefert der Internetdiensteanbieter AOL. Im August 2006 stellte AOL eine Log-Datei seines Suchdienstes mit 20 Millionen Suchanfragen ins Internet. Beim Einstellen glaubten die AOL-Mitarbeiter, dass es zur Anonymisierung der Daten ausreichen würde, die Mitgliedsnummern der erfassten Nutzer auszutauschen. Es dauerte allerdings nur zwei Tage bis Journalisten die Identität einer Nutzerin anhand ihrer Suchanfragen aufdecken konnten. Zwar wurde die Log-Datei von AOL aus dem Internet genommen, die Daten kursieren jedoch weiterhin im Internet und ermöglichen Einblicke in die finanzielle Situation, Krankheiten, Lebensschicksale und das Sexualleben der betroffenen Nutzer.

Das BDSG muss daher klarstellen, dass personenbeziehbare Daten als personenbezogene Daten einzustufen sind.

g) Schaffung besserer Kontroll- und Sanktionsmöglichkeiten

Ein Hauptgrund dafür, dass es eine große Anzahl von Verletzungen der Datenschutzgesetze gibt, ist der, dass Unternehmen bei Verstößen keine spürbaren Sanktionen fürchten müssen. Daher muss der Vollzug gestärkt werden. Hierfür müssen die Datenschutzkontrollinstanzen unabhängiger und in die Lage versetzt werden, regelmäßige Kontrollen in Unternehmen durchzuführen sowie Verstöße durch empfindliche Sanktionen effektiv zu unterbinden. (Eine stärkere Unabhängigkeit wird auch von der EU angemahnt – siehe Vertragsverletzungsverfahren vor dem EuGH.)

Das Fehlen von effektiven Kontroll- und Sanktionsmöglichkeiten erklärt auch, warum Verbraucher ein mangelhaftes Problembewusstsein in Bezug auf den Datenschutz haben. So wird z.B. die Anzahl der Telefonüberwachungen von Bürgern stark unterschätzt. Während Verbraucher schätzten, dass derzeit jährlich ca. 10.000 Personen von der Telefonüberwachung betroffen sind, liegt die Realität bei ca. 200.000.[1] Einen gleichen Trend kennt man auch aus dem Ausland. In einer Befragung unter britischen Bürgern wurde die Zahl der vorhandenen Videokameras auf 10.000 geschätzt. Die Zahl lag jedoch bei rund 4 Millionen.[2]

2) Datenschutzaudit

Für die Einhaltung der Datenschutzgesetzgebung im privaten Bereich sind traditionell die Datenschutzaufsichtsbehörden und die betrieblichen Datenschutzbeauftragten zuständig. Es zeigt sich jedoch, dass dieses traditionelle Aufsichts- und Kontrollverfahren an einer zu geringen Kontrolldichte leidet, die zu spürbaren Vollzugsdefiziten führt. Die Folge hiervon ist, dass viele Datenschutzverstöße unsanktioniert bleiben. Dies bedeutet im Umkehrschluss, dass es für Unternehmer an Anreizen fehlt, Datenschutz umzusetzen.

Das Umsetzungsdefizit wird durch eine Erhebung des Wirtschaftsmagazins WISO exemplarisch verdeutlicht. Das BDSG gibt Verbrauchern das Recht, bei Unternehmen nachzufragen, welche Daten über sie gespeichert sind, was mit diesen gemacht wird, und Daten ggf. löschen zu lassen. WISO hat in dieser Erhebung geprüft, inwieweit die Unternehmen ihren Pflichten in der Praxis nachkommen. Das Ergebnis der Untersuchung war, dass Unternehmen ihrer Auskunftspflicht über gespeicherte Daten nur in ungenügender Weise nachkommen. Die Wartezeiten für die Beantwortung von Anfragen betrugen zwischen 2 und 42 Tagen, die Hälfte der Unternehmen musste in einem Schreiben angemahnt werden und von Neckermann, KarstadtQuelle und Mobilcom hätten die Verbraucher bis heute nichts gehört, wenn WISO nicht nachgehakt hätte.

Im Zuge der jüngsten Novelle des Bundesdatenschutzgesetzes wurden daher ergänzende selbstregulierende und selbstkontrollierende Verfahren vorgeschlagen, die nicht auf Verbot,

---

[1] TAUCIS: Technologiefolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung, Studie im Auftrag des Bundesministeriums für Bildung und Forschung (Juli 2006).

[2] Ebenda.

Kontrolle und Sanktion aufbauen, sondern auf marktwirtschaftlichen Anreizen basieren. Eines dieser marktwirtschaftlichen Instrumente ist das Datenschutzaudit. Das Datenschutzaudit ist ein freiwilliges Instrument für die Überprüfung der datenschutzrechtlichen Eignung von Produkten, Dienstleistungen und Verfahren. Das Ziel des Datenschutzaudits ist es, die Transparenz über den Datenschutz und die Datensicherheit zu erhöhen, Vertrauen von Nutzern zu gewinnen und für eine kontinuierliche Verbesserung des Datenschutzes und der Datensicherheit zu sorgen.

Zwar wurde das Instrument des Datenschutzaudits bei der jüngsten Novellierung des Bundesdatenschutzgesetzes eingeführt. Allerdings fehlt es bislang an einem Ausführungsgesetz zu § 9a BDSG. Ein solches Ausführungsgesetz müsste „nähere Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter" regeln. Eine solche Regelung ist nicht nur für die Wirtschaft wichtig, die Rechts- und Anwendungssicherheit benötigt, sondern auch für die Verbraucher. Erfahrungen mit Labels zeigen, dass diese nur dann wirken, wenn Verbraucher ihnen vertrauen können und wenn sie auf den ersten Blick sichtbar sind. Das Beispiel der Eierkennzeichnung zeigt, wie stark der marktwirtschaftliche Anreizmechanismus wirken kann, wenn diese Kriterien erfüllt sind. Seitdem Verbraucher durch eine eindeutige Kennzeichnung auf den ersten Blick erkennen können, welche Eier aus der Legebatterie kommen, steigt der Absatz von Eiern, die nicht der Käfighaltung entstammen, rasant an, und Eier aus der Käfighaltung werden gemieden.

Dieses Beispiel verdeutlicht, dass ein Datenschutzaudit eine wichtige marktwirtschaftliche Lenkungswirkung entfalten könnte. Ein Datenschutzaudit ist unbürokratisch, da es auf dem Prinzip der Freiwilligkeit beruht und es belohnt die Unternehmen, die sich durch Datenfreundlichkeit auszeichnen. Effizient umgesetzt kann es daher sowohl im Sinne der Verbraucher als auch der Unternehmen wirken.

3) Scoring und Unternehmensinformationspflicht bei Datenschutzpannen

a) Scoring zu Lasten des Verbrauchers

Eine neue Herausforderung an den Datenschutz erwächst aus der erheblichen Zunahme automatisierter Entscheidungen und Bewertungen von Informationen über Verbraucher, die unter dem Begriff *Scoring* zusammengefasst werden. Zwar werden Scoringverfahren bereits in vielen Bereichen eingesetzt, vorrangig – und aus Verbrauchersicht am bedeutendsten – sind jedoch Scoringverfahren bei Finanzdienstleistungen. Hier dienen sie dazu, die Bonität von Verbrauchern einzuschätzen. Diese Bonitätsbewertung dient nicht mehr nur für die Bewertung, *ob* einem Verbraucher ein Kredit gewährt wird, sondern *zu welchem Preis*.

In der Praxis der Anwendung von Scoringverfahren haben sich eine Reihe zum Teil gravierender Probleme gezeigt, die sowohl den Daten- als auch den Verbraucherschutz tangieren:

Regelmäßiger Verstoß gegen § 6a BDSG

§ 6a BDSG verbietet Entscheidungen, die ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, wenn diese die Betroffenen erheblich beeinträchtigen. Da jede Entscheidung, die nicht zum beworbenen Bestzinssatz führt, unweigerlich eine negative Entscheidung darstellt, darf eine Bonitätsbewertung unserer Meinung nach nicht allein auf der Grundlage einer automatisierten Entscheidung durchgeführt werden. In

der Praxis wird hiergegen jedoch regelmäßig verstoßen. Da der Scorewert eines Scoringunternehmens ein Geschäftsgeheimnis darstellt, ist weder der Verbraucher noch der Mitarbeiter in der Bank in der Lage nachzuvollziehen, wie der Scorewert zustande gekommen ist, ob die zugrunde liegenden Daten zutreffend sind und ob die Daten richtig interpretiert wurden.

Daher fordern wir, dass § 6a konsequent angewendet wird. D.h., dass Verbraucher entweder die beworbene Bestkonditionen erhalten müssen (da in diesem Fall keine Negativentscheidung vorliegt). Oder es muss den Verbrauchern und Kreditanbietern die Möglichkeit gegeben werden, sämtliche Daten und Annahmen, die in die automatisierten Entscheidung eingeflossen sind, einzusehen und zu kommentieren. Erst durch eine Offenlegung haben Verbraucher und Kreditanbieter die Möglichkeit, Bewertungen zu revidieren, um daraus einen neuen Bewertungsfaktor zu erstellen, der nicht alleinig auf der automatisierten Verarbeitung personenbezogener Daten basiert. Dies bedeutet in letzter Konsequenz, dass die Einstufung des Scoringverfahrens als Geschäftsgeheimnis aufzugeben ist.

Objektivität der Scoringverfahren im konkreten Einzelfall fraglich

Von Seiten der Anbieter wird die Objektivität der Scoringsysteme hervorgehoben. Dies erscheint uns im konkreten Einzellfall fraglich zu sein. Bezieht sich die Bewertung statistischer Merkmale auf die Gesamtheit des Portfolios, können statistisch signifikante Schlussfolgerungen gezogen werden. Auf den konkreten Einzellfall bezogen, können statistische Merkmale jedoch nicht als objektiv eingestuft werden. Dass ein Verbraucher häufig umgezogen ist, dass er mehrere Konten unterhält oder dass er mehrmals Kreditkonditionen angefragt hat, kann unterschiedliche Gründe haben, die in einem statistischen automatischen Verfahren nicht abgebildet werden können. Auch können statistische Verfahren nur dann zu mehr oder weniger zutreffenden Aussagen kommen, wenn die Datenlage ausreichend und zutreffend ist. Selbsttests des Verbraucherzentrale Bundesverbands und von Journalisten (Börse Online Heft 44/06) zeigen jedoch, dass diese oft unzureichend ist.

Aus diesen Gründen müssen Datenbestände und Scoringverfahren für die Verbraucher transparenter werden. Eine besondere Herausforderung stellt sich jedoch in den Fällen, in denen Unternehmen Scorewerte von Dritten einholen. Das Auskunftsrecht nach § 34 BDSG erstreckt sich lediglich auf Daten, die bei einem Unternehmen liegen und nicht auf Daten, die von Dritten eingeholt werden.

Daher fordern wird, dass:
- Verbraucher das Recht haben müssen, auch die von Dritten gemeldeten Daten einsehen und ggf. korrigieren zu können;
- bei der Beurteilung der Kreditwürdigkeit von Verbrauchern nur kreditrelevante personenbezogene Faktoren berücksichtig werden dürfen;
- klare Haftungsregeln für Unternehmen und Auskunfteien eingeführt werden müssen, sollten Scores und Bonitätsbewertungen auf unsachlicher oder diskriminierende Grundlage beruhen;
- Scoringunternehmen Verbrauchern die über sie gespeicherten Daten kostenlos zur Verfügung stellen müssen.

Konditionsverschlechterung, wenn Verbraucher sich ‚mündig' verhalten

Da Banken zunehmend dazu übergehen, Verbrauchern nur noch Kreditangebote mit verbraucherabhängigen Eigenschaften abzugeben, holen die Kreditanbieter häufiger als bisher

Scorewerte bei Auskunfteien ein. Solche Bonitätsanfragen haben jedoch in der Regel einen negativen Einfluss auf den Scorewert. Das aus unserer Sicht ‚mündige' Verhalten des Verbrauchers, unterschiedliche Angebote einzuholen, wird von Auskunfteien negativ als Indiz dafür gewertet, mehrere Kredite gleichzeitig einholen zu wollen.

Schufa und Banken haben dem Verbraucherzentrale Bundesverband die Unsinnigkeit dieses Effekts zugestanden und Abhilfe versprochen. Allerdings sind wir mit dem Ergebnis noch nicht zufrieden. Die Schufa differenziert zwar seit geraumer Zeit zwischen ‚Kreditanfragen', die einen negativen Einfluss auf den Scorewert haben und ‚Konditionenabfragen', die keinen Einfluss auf den Scorewert haben. Allerdings hat FINANZtest erst kürzlich festgestellt, dass Banken zur Erstellung von Kreditangeboten in der Regel keine ‚Konditionenabfrage', sondern eine ‚Kreditanfrage' stellen, obwohl der Verbraucher nur ein Angebot einholen möchte. – Der Test der Stiftung Warentest ergab zudem Hinweise darauf, dass sich Anbieter durch den Hinweis auf diesen Effekt ggf. sogar einen rechtswidrigen Wettbewerbsvorteil verschaffen.

Daher fordern wir, dass nur der endgültige Abschluss eines Kreditvertrags zu einem Eintrag bei (Kredit-) Auskunfteien führen darf.

b) Unternehmensinformationspflicht bei Datenschutzpannen

Schäden, die Verbrauchern dadurch entstehen, dass Unternehmen gegen verbraucherschützende Regeln verstoßen, müssen möglichst effektiv und vollständig ausgeglichen werden. Daher ist das Ansinnen Informationspflichten für Unternehmen bei Datenschutzpannen einzuführen, grundsätzlich zu begrüßen. Allerdings ist unserer Meinung nach in einem ersten Schritt zu prüfen, in wie weit ein solches Unterfangen bereits heute auf Grundlage von bestehenden zivilrechtlichen Schadensersatzansprüchen wegen Verletzung des allgemeinen Persönlichkeitsrechts (unter Einschluss des Datenschutzrechts) zufriedenstellend gelöst werden kann und an welchen Stellen Regelungslücken festgestellt werden, die durch eine besondere Gesetzgebung zu Informationspflichten und daraus resultierenden zivilrechtlichen Schadensersatzansprüchen geschlossen werden müsste.