

W

Deutscher Bundestag ■ Wissenschaftliche Dienste

**Datenschutzrechtliche Regelungen im Bereich der
Geschäftstätigkeit von Banken und Sparkassen**

- Ausarbeitung -



Wissenschaftliche Dienste des Deutschen Bundestages

Verfasser/in: [REDACTED]

Datenschutzrechtliche Regelungen im Bereich der Geschäftstätigkeit von Banken und Sparkassen

Ausarbeitung WD 3 - 3000 - 317/08

Abschluss der Arbeit: 1. September 2008

Fachbereich WD 3: Verfassung und Verwaltung

Telefon: [REDACTED]

Ausarbeitungen und andere Informationsangebote der Wissenschaftlichen Dienste geben nicht die Auffassung des Deutschen Bundestages, eines seiner Organe oder der Bundestagsverwaltung wieder. Vielmehr liegen sie in der fachlichen Verantwortung der Verfasserinnen und Verfasser sowie der Fachbereichsleitung. Die Arbeiten der Wissenschaftlichen Dienste sind dazu bestimmt, Mitglieder des Deutschen Bundestages bei der Wahrnehmung des Mandats zu unterstützen. Der Deutsche Bundestag behält sich die Rechte der Veröffentlichung und Verbreitung vor. Beides bedarf der Zustimmung der Leitung der Abteilung W.

Inhaltsverzeichnis		Seite
1.	Einleitung	4
2.	Die Regelungen des Bundesdatenschutzgesetzes	4
2.1.	Zum Anwendungsbereich des BDSG	4
2.2.	Der generelle Erlaubnis- und Einwilligungsvorbehalt des BDSG	5
2.3.	Besondere Regelungen für nicht-öffentliche Stellen und öffentlich-rechtliche Wettbewerbsunternehmen	6
2.3.1.	Übermittlung und Nutzung personenbezogener Daten zu Werbezwecken	7
2.3.2.	Verantwortlichkeit und Sorgfaltspflichten bei der Datenverarbeitung im Auftrag	8
2.4.	Bußgeld- und Strafvorschriften im BDSG	9
3.	Weitere Problemfelder im Bereich der Geschäftstätigkeit der Banken und Sparkassen	10

1. Einleitung

Die aktuellen „Datenklaukandale“ und der illegale Handel mit Daten haben in der Öffentlichkeit eine Debatte über das Thema Datenschutz ausgelöst. Diskutiert werden in diesem Zusammenhang u.a. die Datenverarbeitung bei Callcentern, der legale und illegale Adressenhandel sowie der Verkauf von Kontodaten und damit im Zusammenhang stehend das unberechtigte Abbuchen von Girokonten aufgrund fingierter Verträge.

Im Folgenden soll ein Überblick über die Regelungen des Bundesdatenschutzgesetzes¹ (BDSG), insbesondere was ihre Geltung für die Geschäftstätigkeit von Banken und Sparkassen betrifft, gegeben werden.

2. Die Regelungen des Bundesdatenschutzgesetzes

Zweck des BDSG ist es nach § 1 Abs. 1 BDSG, „den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird“. Zur Erreichung dieses Zwecks enthält das BDSG detaillierte Regelungen dazu, unter welchen Voraussetzungen öffentliche und nicht-öffentliche Stellen personenbezogene Daten erheben, verarbeiten und nutzen dürfen.

Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich ihrer Veröffentlichung anzuwenden sind, gehen sie gemäß § 1 Abs. 3 S. 1 BDSG den Vorschriften des BDSG allerdings vor. Wie § 1 Abs. 3 S. 2 BDSG zudem bestimmt, bleibt die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, unberührt. Zu den letztgenannten, gesetzlich nicht geregelten, nur im Landesrecht wurzelnden Geheimhaltungspflichten gehört auch das **Bankgeheimnis**.²

2.1. Zum Anwendungsbereich des BDSG

Das BDSG gilt gemäß § 1 Abs. 2 Nr. 1 und 2 BDSG für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

- **öffentliche Stellen des Bundes**,
- **öffentliche Stellen der Länder**, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie Bundesrecht ausführen oder als Organe der

1 Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 22. August 2006 (BGBl. I S. 1970).

2 Gola/Schomerus, BDSG-Kommentar, 8. Auflage, München 2005, § 1 Rn. 25.



Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,

- **nicht-öffentliche Stellen**, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

In privatrechtlicher Organisationsform, etwa als Aktiengesellschaft, betriebene Kreditinstitute (**Banken**) fallen nach der in § 2 Abs. 4 BDSG enthaltenen Definition unter den Begriff „nicht-öffentliche Stellen“. **Sparkassen** hingegen zählen formal nach der in § 2 Abs. 2 BDSG enthaltenen Definition zu den öffentlichen Stellen der Länder. Sie **werden** jedoch, soweit es um die Erhebung, die Verarbeitung und die Nutzung personenbezogener Daten geht, **wie nicht-öffentliche Stellen behandelt**, vgl. § 27 Abs. 1 S. 1 Nr. 2 b).³ Eine entsprechende Klarstellung enthält z.B. das Bayerische Datenschutzgesetz⁴ in seinem Art. 3 Abs. 2 S. 2: „Für öffentlich-rechtliche Kreditinstitute sowie für ihre Zusammenschlüsse und Verbände gelten die Vorschriften des Bundesdatenschutzgesetzes, die auf privatrechtliche Kreditinstitute anzuwenden sind“.

2.2. Der generelle Erlaubnis- und Einwilligungsvorbehalt des BDSG

Die Erhebung, die Verarbeitung und die Nutzung personenbezogener Daten sind nach § 4 Abs. 1 BDSG **nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat**. Das BDSG selbst enthält Rechtsgrundlagen für die Datenverarbeitung durch nicht-öffentliche Stellen in seinen §§ 4 Abs. 2 und 3, 28 Abs. 1 (für eigene Zwecke), 29 Abs. 1 und 30 Abs. 1 (für „fremde Zwecke“). Eine über die in den genannten Vorschriften für zulässig erklärten Zwecke hinausgehende Verarbeitung personenbezogener Daten ist nur zulässig, wenn der Betroffene darin eingewilligt hat.

Die grundsätzlichen **Voraussetzungen für eine wirksame Einwilligung** regelt im Einzelnen § 4a Abs. 1 BDSG. Danach muss die Einwilligung auf der freien Entscheidung des Betroffenen beruhen. Der Betroffene ist zudem auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten hinzuweisen. Die Einwilligung bedarf der **Schriftform**, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen

3 Dazu Simitis, in: Simitis (Hrsg.), Kommentar zum Bundesdatenschutzgesetz, 5. Auflage 2003, § 27 Rn. 6f.

4 Vom 23. Juli 1993 (GVBl. S. 498, BayRS 204-1-I), zuletzt geändert durch Gesetz vom 10. Juni 2008 (GVBl 2008, S. 315).

schriftlich erteilt werden, so ist sie **besonders hervorzuheben** (§ 4a Abs. 1 S. 4 BDSG). Dadurch soll verhindert werden, dass die Einwilligung bei Formularverträgen im sog. „Kleingedruckten“ versteckt wird und der Betroffene sie durch seine Unterschrift erteilt, ohne sich dessen bewusst zu sein.

Gemäß § 4 Abs. 3 BDSG ist der Betroffene außerdem über die Identität der verantwortlichen Stelle, die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und die Kategorien der Empfänger der Daten zu unterrichten, soweit er nach den Umständen des Einzelfalls nicht mit der Übermittlung an diese rechnen muss.

2.3. Besondere Regelungen für nicht-öffentliche Stellen und öffentlich-rechtliche Wettbewerbsunternehmen

Für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch **nicht-öffentliche Stellen** und **öffentlich-rechtliche Wettbewerbsunternehmen** gelten die besonderen Regelungen des Dritten Abschnitts des BDSG (§§ 27 ff. BDSG). Wie oben erläutert werden damit sowohl Banken als auch Sparkassen erfasst.

Gemäß § 28 Abs. 1 S. 1 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel **für die Erfüllung eigener Geschäftszwecke** zulässig,

- wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient,
- soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, **oder**
- wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Die **Zwecke**, für die die Daten verarbeitet oder genutzt werden sollen, sind bereits bei der Erhebung der personenbezogenen Daten **konkret festzulegen**, § 28 Abs. 1 S. 2 BDSG.

Gemäß § 34 Abs. 1 S. 1 BDSG kann der Betroffene **Auskunft** verlangen über die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen, über Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und über den Zweck der Speicherung.

Personenbezogene Daten sind gemäß § 35 Abs. 2 S. 2 BDSG zu **löschen**, wenn

- ihre Speicherung unzulässig ist,

- es sich um Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit, über Gesundheit oder das Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann,
- sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist, **oder**
- sie geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden und eine Prüfung jeweils am Ende des vierten Kalenderjahres beginnend mit ihrer erstmaligen Speicherung ergibt, dass eine längerwährende Speicherung nicht erforderlich ist.

2.3.1. Übermittlung und Nutzung personenbezogener Daten zu Werbezwecken

Die Übermittlung oder Nutzung von personenbezogenen Daten zu Zwecken der **Werbung und der Markt- oder Meinungsforschung** ist gemäß § 28 Abs. 3 Nr. 3 BDSG zulässig, wenn es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf

- eine Angabe über die Zugehörigkeit des Betroffenen zu dieser Personengruppe,
- Berufs-, Branchen- oder Geschäftsbezeichnung,
- Namen,
- Titel,
- akademische Grade,
- Anschrift und
- Geburtsjahr

beschränken **und** kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat. Die Nutzung von **Kontodaten** für Werbezwecke ist damit unzulässig, wenn nicht der Betroffene gemäß § 4a BDSG ausdrücklich darin eingewilligt hat. Die in § 28 Abs. 3 Nr. 3 BDSG liegende Privilegierung der Datenverarbeitung zu Werbezwecken stößt aber auch davon abgesehen auf **Kritik**. Gefordert wird, die Weitergabe von personenbezogenen Daten zu Werbezwecken generell von einer ausdrücklichen Einwilligung des Betroffenen nach § 4a BDSG abhängig zu machen.⁵

Der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung kann der Betroffene **widersprechen**. Tut er dies, so ist eine Nutzung oder Übermittlung seiner Daten zu diesen Zwecken gemäß § 28 Abs. 4 S. 1 BDSG unzulässig. Bei der Ansprache - etwa durch Briefpost oder im Rahmen eines

5 Vgl. z.B. Weichert, Schlussfolgerungen aus dem Bekanntwerden des illegalen Verkaufs von Kontodaten, verfügbar unter <https://www.datenschutzzentrum.de/kontodaten/gesetzgebungsbedarf.html> (letzter Abruf: 27.08.2008), dort unter IV., Abs. 3.

Telefongesprächs - ist der Betroffene nach § 28 Abs. 4 S. 2 BDSG über die verantwortliche Stelle (also die Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt, vgl. § 3 Abs. 7 BDSG) und das Widerspruchsrecht zu unterrichten. Soweit der Ansprechende personenbezogene Daten nutzt, die bei einer dem Betroffenen nicht bekannten Stelle gespeichert sind, hat er auch sicherzustellen, dass der Betroffene Kenntnis über die Herkunft der Daten erhalten kann. Der Betroffene kann auch bei dem ihn ansprechenden Dritten, dem die Daten nach § 28 Abs. 3 BDSG übermittelt wurden, widersprechen, mit der Folge, dass dieser Dritte die Daten für die Zwecke der Werbung und Markt- oder Meinungsforschung zu **sperr**en hat, vgl. § 28 Abs. 4 S. 3 BDSG.

Der Verstoß gegen die genannte Verpflichtung zur Unterrichtung im Fall der Ansprache zu Werbe-, Markt- oder Meinungsforschungszwecken stellt gemäß § 43 Abs. 1 Nr. 3 BDSG eine **Ordnungswidrigkeit** dar, die mit einer Geldbuße bis zu 25.000 € geahndet werden kann.

Gemäß § 28 Abs. 5 BDSG darf der Dritte, dem die Daten übermittelt worden sind, diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden (sog. **Zweckbindung**). Für andere Zwecke darf der beauftragte Dritte die ihm übermittelten Daten gemäß § 28 Abs. 5 S. 2 nur unter den Voraussetzungen des § 28 Abs. 2 und 3 BDSG verarbeiten oder nutzen, worauf ihn die übermittelnde Stelle nach § 28 Abs. 5 S. 3 BDSG hinzuweisen hat. Diese in § 28 Abs. 5 S. 2 ermöglichte Verwendung der übermittelten Daten durch das beauftragte Unternehmen für andere Zwecke stößt im Schrifttum auf **Kritik**. Damit werde dem Adressaten der Übermittlung fast genau der Verwendungsspielraum eingeräumt, der auch der übermittelnden Stelle zustehe. Die in § 28 Abs. 5 S. 1 BDSG postulierte strikte Zweckbindung der übermittelten Daten werde dadurch faktisch aufgehoben und sei mit den Grundsätzen des Datenschutzes nicht vereinbar.⁶

Eine gegen § 28 Abs. 5 S. 2 BDSG verstoßende Übermittlung oder Nutzung stellt nach § 43 Abs. 1 Nr. 4 BDSG eine **Ordnungswidrigkeit** dar, die mit einer Geldbuße bis zu 25.000 € geahndet werden kann.

2.3.2. Verantwortlichkeit und Sorgfaltspflichten bei der Datenverarbeitung im Auftrag

Grundsätzliche Anforderungen an die auftraggebende Stelle bei der Bereitstellung von personenbezogenen Daten an Dritte wie z.B. sog. **Callcenter**, die im Auftrag eines Un-

6 Simitis (Fn. 3), § 28 Rn. 310ff., 316, der für eine möglichst restriktive Auslegung des § 28 Abs. 5 S. 2 BDSG plädiert.

ternehmens etwa Akquise, Kundenrückgewinnung oder Kundenbetreuung durchführen, ist in § 11 Absätze 1 bis 3 BDSG geregelt:



„(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei die Datenerhebung, -verarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden. Der Auftraggeber hat sich von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen“.

2.4. Bußgeld- und Strafvorschriften im BDSG

Das BDSG selbst enthält in seinen §§ 43 und 44 Bußgeld- und Strafvorschriften.

Die Tatbestände des § 43 Abs. 1 BDSG betreffen **Verstöße gegen Verfahrensvorschriften**. Dazu gehören die bereits genannten Sanktionierungen von Verstößen gegen die Unterrichtungspflichten bei der Ansprache zu Werbe- oder Marktforschungszwecken und den Grundsatz der Zweckbindung an einen Dritten übermittelter Daten (siehe unter 2.3.1.), beispielsweise aber auch der Verstoß gegen die Verpflichtung zur Bestellung eines betrieblichen oder behördlichen Beauftragten für den Datenschutz (Nr. 2 der Vorschrift). Ordnungswidrigkeiten nach § 43 Abs. 1 BDSG können mit **Geldbuße bis zu 25.000 €** geahndet werden.

Die Tatbestände des § 43 Abs. 2 BDSG betreffen **Verstöße gegen materielle Schutzvorschriften** des BDSG. § 43 Abs. 2 BDSG lautet:

„Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,
2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,
3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abrufen oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,
4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,
5. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 5 Satz 1, auch in Verbindung mit § 29 Abs. 4, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1, die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt, oder
6. entgegen § 30 Abs. 1 Satz 2 die in § 30 Abs. 1 Satz 1 bezeichneten Merkmale oder entgegen § 40 Abs. 2 Satz 3 die in § 40 Abs. 2 Satz 2 bezeichneten Merkmale mit den Einzelangaben zusammenführt“.

Solche Ordnungswidrigkeiten können gemäß § 43 Abs. 3 BDSG mit **Geldbuße bis zu 250.000 €** geahndet werden.

Wer eine in § 43 Abs. 2 BDSG bezeichnete **vorsätzliche** Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird gemäß § 44 Abs. 1 BDSG mit **Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe** bestraft. Gemäß § 44 Abs. 2 BDSG wird die Tat nur auf Antrag verfolgt. Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die Aufsichtsbehörde.

3. Weitere Problemfelder im Bereich der Geschäftstätigkeit der Banken und Sparkassen

Um die Bereitschaft und die Fähigkeit eines potentiellen Kreditnehmers, einen Kredit zurückzuzahlen, und damit die Wahrscheinlichkeit eines Kreditausfalls einzuschätzen, können sich Banken und Sparkassen einer externen Bonitätsprüfung per Punktesystem („**Scoring**“) bedienen. Scoring-Verfahren, auch Punktwertverfahren genannt, werden u.a. von Kreditauskunfteien verwandt. Sie stellen eine „auf mathematisch-statistischen

Verfahren gründende Auswertungsmethode dar, die eine Mehrzahl von Menschen oder Merkmalen in eine Reihenfolge nach mehreren Kriterien bringt. Der ermittelte Score-Wert wird als Risikoprognose an Vertragspartner weitergegeben“.⁷

Eine Spezialregelung zum Scoring außerhalb des Bundesdatenschutzgesetzes stellt § 10 Abs. 1 Kreditwesengesetz⁸ (KWG) dar, der die Bonitätsprüfung durch Scoring ausdrücklich für zulässig erklärt. Diese Art der Bonitätsprüfung kann allerdings in Konflikt geraten mit dem **Verbot der automatisierten Einzelentscheidung**⁹ gemäß § 6a BDSG, welcher, da sich § 10 KWG nicht zu diesem Bereich verhält, neben dieser Spezialvorschrift wohl anwendbar bleibt. Nach § 6a Abs. 1 BDSG dürfen Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, grundsätzlich nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dient. Das automatisiert erzeugte Ergebnis muss von einem zuständigen Entscheidungsträger noch zur Kenntnis genommen, geprüft und bestätigt werden.¹⁰

Die Banken und Sparkassen können ferner besondere **Aufklärungspflichten** gegenüber ihren Kunden haben. Nach Auffassung des Berliner Beauftragten für den Datenschutz und die Informationsfreiheit müssen Banken bei Auslandsüberweisungen ihre Kunden vorab darüber informieren, dass das von ihnen angewandte Überweisungssystem **SWIFT** die Überweisungsdaten in den Vereinigten Staaten von Amerika (USA), „einem Land ohne ausreichendes Datenschutzniveau“¹¹, spiegelt. Generell bestehe zudem eine Informationspflicht gegenüber den Kunden darüber, dass sämtliche Kontobewegungen mithilfe des sog. **Research-Systems** auf geldwäscherelevante Besonderheiten untersucht werden.¹²

Im Zuge des aktuellen Skandals über den bekannt gewordenen illegalen Verkauf von Kontodaten wird vom Leiter des Unabhängigen Landeszentrums für Datenschutz

7 Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (Hrsg.), BfDI – Info 1, Bundesdatenschutzgesetz – Text und Erläuterung -, 13. Aufl., Sept. 2007, S. 46, verfügbar unter http://www.bfdi.bund.de/cln_007/nm_531948/SharedDocs/Publikationen/Infobroschueren/INFO1.html (letzter Abruf: 01.09.2008).

8 Kreditwesengesetz in der Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2776), zuletzt geändert durch Artikel 3 des Gesetzes vom 13. August 2008 (BGBl. I S. 1690). Dazu ausführlich: [Name], Datenschutz und externe Bonitätsprüfung per Punktesystem („Kreditscoring“), Wissenschaftliche Dienste des Bundestags, WD3 – 315/07, vom 29. August 2007.

9 In BfDI – Info 1 (Fn. 7), S. 46, auch als Grundsatz, dass die Maschine nicht über den Menschen entscheiden dürfe, bezeichnet.

10 Vgl. dazu auch Hoeren, Rechtliche Grundlagen des SCHUFA-Scoring-Verfahrens, Recht der Datenverarbeitung (RDV) 2007, S. 93 (98), der in diesem Fall § 6a BDSG noch nicht einmal für einschlägig hält, da der Punktwert lediglich ein Informationsbaustein für die Entscheidung des Kreditbearbeiters und nicht allein entscheidend für die Gewährung oder Ablehnung des Kredits sei.

11 Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2007, verfügbar unter: <http://www.datenschutz-berlin.de> (letzter Abruf: 01.09.2008), S. 58f.

12 Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit (Fn. 11), S. 59.

Schleswig-Holstein Weichert zudem eine Konkretisierung von **Informationspflichten** der Banken gegenüber ihren Kunden in solchen Fällen gefordert. „Sobald erste Beschwerden oder mehrfache Stornos von Abbuchungen in einer Bank über eine abbuchende Firma vorliegen, sollten alle weiteren Transaktionen gestoppt, als Grundlage die schriftliche Ermächtigung der Betroffenen eingefordert und die Betroffenen informiert werden“.¹³

W

13 Weichert (Fn. 5), dort unter VI., Abs. 2, unter Hinweis auf BGH, Urteil vom 06.05.2008 – XI ZR 56/07, der eine entsprechende Warnpflicht aufgrund vertraglicher Schutzpflichten angenommen hat, siehe dort Rn. 13ff. (bei juris).