DuD
Datenschutz und Datensicherheit

Datenschutz für Chipkarten

Die Anwendung des § 6 c BDSG auf Signatur- und Biometriekarten

Gerrit Hornung

Seit der Novelle von 2001 enthält das BDSG in § 6 c Anforderungen an mobile personenbezogene Speicher- und Verarbeitungsmedien. Anwendungsbereich und Regelungsgehalt der Norm werfen eine Reihe von Problemen auf. Der folgende Beitrag befasst sich eingehend mit der Anwendbarkeit auf Signaturkarten und Medien mit biometrischen Daten, gibt eine Übersicht über landesrechtliche Bestimmungen und beschreibt Anforderungen an Inhalt und Ablauf der Unterrichtung.

Gerrit Hornung, LL.M. in European Law
Mitglied der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) an der Universität Kassel
E-Mail: gerrit.hornung@uni-kassel.de

Einleitung

Die Einführung von § 6 c BDSG[1] war durch den Gedanken bestimmt, dass wegen der Intransparenz einer Verarbeitung auf mobilen personenbezogenen Speicher- und Verarbeitungsmedien erhöhte datenschutzrechtliche Gefahren für den Betroffenen entstehen.[2] Da diese Medien in einer Vielzahl von Alltagsaktivitäten elektronische Spuren hinterlassen, besteht auch das Risiko von problematischen Profilbildungen.[3] Dieses nimmt umso mehr zu, je mehr Funktionalitäten in einer einzigen Karte vereinigt werden. § 6 c BDSG verfolgt den Zweck, durch die Festlegung von Informationspflichten dem datenschutzrechtlichen Transparenzgebot Genüge zu tun.[4]

1 Anwendungsbereich

Die Transparenzpflichten gelten nur für „mobile personenbezogene Speicher- und Verarbeitungsmedien". Der Anwendungsbereich ist insoweit nicht leicht zu bestimmen, da BDSG und LDSG teilweise unterschiedliche Begriffsbestimmungen verwenden.[5]

1.1 Mobile personenbezogene Speicher- und Verarbeitungsmedien

Der Begriff der mobilen personenbezogenen Speicher- und Verarbeitungsmedien wird in § 3 Abs. 10 BDSG definiert. Danach ist erforderlich, dass der Datenträger an den Betroffenen ausgegeben wird, auf ihm personenbezogene Daten über die Speicherung hinaus automatisiert verarbeitet werden können und der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

Problematisch ist insbesondere die automatisierte Verarbeitung auf dem Medium. Teilweise genügt nach den LDSG ein automatisierter Datenaustausch[6] oder eine automatisierte Verarbeitung „durch" den Datenträger[7]. Auch der Entwurf von Bündnis 90/DIE GRÜNEN aus dem Jahr 1997 sah lediglich die Notwendigkeit einer direkten Kommunikation mit elektronischen Lese- und Schreibgeräten vor.[8] Diese Definitionen erfassen auch reine Speichermedien wie Magnetkarten. Dagegen schränkt das von § 3 Abs. 10 BDSG verwendete Kriterium der Verarbeitung durch das Medium selbst den Anwendungsbereich dieser Vorschrift und der auf sie verweisenden Normen (bislang nur § 6 c BDSG) erheblich ein, weil hierdurch reine Speichermedien ausgenommen sind.[9]

[1] Zur Gesetzgebungsgeschichte vgl. Simitis-*Bizer*, BDSG (2003), § 6 c Rn. 8ff. Zur Rechtslage vor der Novelle *Weichert*, DuD 1997, 266.

[2] Begründung des Änderungsantrag von SPD/Bündnis90/Die Grünen im Innenausschuss, BT-Drs. 14/5793, 63.

[3] *Weichert* in: Roßnagel, Handbuch Datenschutzrecht (2003), Rn. 44ff.

[4] *Gola/Schomerus*, BDSG (2002), § 6 c Rn. 2; Simitis-*Bizer* § 6 c Rn. 3.

[5] Wie das BDSG eine Verarbeitung auf dem Medium erfordernd: § 5 Abs. 1 LDSG BW, § 4 Abs. 3 Nr. 9 LDSG Bln, § 20 a Abs. 1 LDSG Brem, § 8 Abs. 2 HDSG, § 35 Abs. 1 LDSG RP, § 3 Abs. 9 LDSG Sl, § 2 Nr. 11 LDSG SA, § 18 Abs. 1 LDSG SH, § 6 a LDSG Nds.

[6] § 5 b LDSG HH, § 3 Abs. 10 LDSG MV.

[7] § 5 Abs. 3 LDSG Bbg.

[8] § 32 Abs. 1 des Entwurfs, BT-Drs. 13/9082, 12.

[9] Teilweise wird auch in der Literatur von dem weiteren Begriff in einigen Ländern ausgegangen, was die Gefahr von Missverständnissen mit sich bringt. So soll nach *Weichert* (Fn. 3), Rn. 20 ein Wesensmerkmal derartiger Medien sein, dass über eine „Schnittstelle ... automatisiert personenbezogene oder personenbeziehbare Daten ausgetauscht werden [können]". Derartiges geschieht aber auch bei reinen Speichermedien. Zumindest im Geltungsbereich von § 6 c BDSG

Zwar ist es richtig, dass mit der Benutzung personenbezogener Chiparten immer eine automatisierte Verarbeitung nach § 3 Abs. 2 BDSG angestoßen wird.[10] Nur kann daraus eben nicht gefolgert werden, jede Chipkarte fiele per se unter § 3 Abs. 10 BDSG, weil diese Norm eben eine Verarbeitung „über die Speicherung hinaus" verlangt und damit gerade nicht jede Verarbeitung nach § 3 Abs. 2 BDSG ausreicht. Erfasst ist nicht jede automatisierten Verarbeitung im Zusammenhang mit Chipkarten, sondern nur eine solche gerade auf der Karte.[11]

Hauptanwendungsbeispiel für mobile personenbezogene Speicher- und Verarbeitungsmedien sind Mikroprozessorchipkarten. Der Begriff wurde aber gewählt, weil er für zukünftige technische Entwicklungen offen gehalten werden sollte.[12] Nach der Gesetzesbegründung soll § 3 Abs. 10 BDSG keine Geräte mit eigener Steuerungseinheit wie Palm, Personal Digital Assistants, Handys oder Notebooks erfassen, da hier eine vielfältige Kontrolle durch den Benutzer möglich sei.[13] Dies ist jedoch nur unter exakt dieser Bedingung zutreffend. Sofern eines dieser Geräte über Soft- oder Hardwarebereiche verfügt, die der Kontrolle des Geräteinhabers entzogen sind und wie eine Chipkarte Daten verarbeiten, ist die Definition des § 3 Abs. 10 BDSG erfüllt.[14]

Unerheblich ist, ob das Medium zum Zeitpunkt der Ausgabe bereits ein Verarbeitungsverfahren oder zu verarbeitende Daten enthält.[15] Besteht die Fähigkeit, später ein automatisiertes Verfahren zu installieren, so löst dies bereits bei der Ausgabe die Pflichten des § 6 c BDSG aus, soweit die anderen Anforderungen von § 3 Abs. 10 BDSG erfüllt sind. Im Folgenden soll ein Blick auf zwei problematische Kartentypen geworfen werden, nämlich zum einen auf Chipkarten in Systemen biometrischer Identifikation, die in Zukunft z.B. bei Dienst- und Betriebsausweisen zum Einsatz kommen werden, zum anderen auf Signaturkarten.

1.1.1 Medien mit biometrischen Daten

Hier ist die Anwendbarkeit von § 6 c BDSG abgelehnt worden, sofern die entsprechende Ermächtigungsnorm nur ein Auslesen und Verwenden der biometrischen Merkmale zur Überprüfung der Echtheit des Mediums und zur Identitätsprüfung des Inhabers zulässt.[16] Die Definition in § 3 Abs. 10 BDSG stellt jedoch nicht darauf ab, ob auf dem Medium personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden *dürfen*, sondern ob sie derart verarbeitet werden *können*.

Entscheidend ist folglich eine Analyse der Funktionsweise einer Chipkarte in biometrischen Systemen. Hier sind unterschiedliche Varianten verfügbar.[17] Die Daten können ausgelesen und in der Peripherie abgeglichen werden, dies ist aber auch auf der Karte möglich (matching-on-card). Schließlich gibt es auch Lösungen, bei denen ein Sensor auf dem Medium genutzt wird.

Betrachtet man zunächst die erste Variante, so werden hier Daten auf der Karte gespeichert. Das reicht nach § 3 Abs. 10 Nr. 2 BDSG aber nicht aus. In Betracht kommt zwar ein Übermitteln, weil (anders als bei reinen Speichermedien) bei der Chipkartenlösung die Karte – eventuell nach einem Authentifizierungsvorgang gegenüber dem Lesegerät – Daten aus dem internen Speicher ausliest und aktiv übermittelt.

Eine solche Argumentation würde aber das Kriterium der über die Speicherung hinaus gehenden Verarbeitung aushebeln. Denn wenn jedes Auslesen aus einer Chipkarte nach der Speicherung eine Übermittlung im Sinne von § 3 Abs. 4 Nr. 3 BDSG wäre, würde im Ergebnis auch eine Chipkarte erfasst, die rein technisch ausschließlich zur Aufbewahrung von Daten geeignet ist. Dann aber entspricht sie funktional einer Magnetkarte. Nach Wortlaut, Gesetzesbegründung wie Schutzzweck von § 6 c BSDG sind derartige reine Speichermedien aber nicht von der Norm erfasst. Eine Karte, die lediglich das Ablegen und automatisierte Auslesen von biometrischen und anderen Identifikationsdaten ermöglicht, fällt damit nicht unter diese Vorschrift.[18]

Verfügt das Medium jedoch über einen Sensor, so erfüllt ihre Funktionsweise die Definition des Erhebens von Daten nach § 3 Abs. 3 BDSG. Fraglich ist nunmehr, ob dies für § 3 Abs. 10 Nr. 2 BDSG ausreicht. Zu beachten ist hierbei, dass dort nicht vom Verarbeiten, sondern vom *automatisierten* Verarbeiten von Daten die Rede ist.[19] Dieser Begriff wird aber nicht in § 3 Abs. 4, sondern in § 3 Abs. 2 BDSG definiert. Er umfasst – sprachlich missglückt[20] – den engeren Tatbestand des Verarbeitens nach § 3 Abs. 4 BDSG, darüber hinaus aber auch die Erhebung und Nutzung personenbezogener Daten, allerdings immer unter der Voraussetzung des Einsatzes von Datenverarbeitungsanlagen. Da letzteres beim automatisierten Erheben mittels Sensor auf der Chipkarte der Fall ist, fallen derartige Systeme unter § 3 Abs. 10 und damit auch unter § 6 c BDSG.

Schließlich erfüllt auch der Vergleich biometrischer Daten das Merkmal der automatisierten Verarbeitung.[21] Das gilt auch für Vergleiche auf der Karte. Da dem Betroffenen ein eigener Zugriff auf die im Ausweis gespeicherten Daten nicht möglich ist, ist auch das letzte Kriterium des § 3 Abs. 10 BDSG erfüllt. Im Ergebnis unterliegen Chipkarten mit biometrischen Sensoren und matching-on-card Prozesse den Anforderungen des § 6 c BDSG.

1.1.2 Signaturkarten

Als Anknüpfungspunkt für eine Datenverarbeitung nach § 3 Abs. 10 Nr. 2 BDSG ergeben sich bei einer Signaturkarte deren drei Funktionalitäten der Signatur, Authentifizierung und Verschlüsselung. Hinsichtlich der elektronischen Signatur kommt eine Verarbeitung wiederum für zwei Daten (Signaturschlüssel und Zertifikat) in Frage.

Ein *Zertifikat* ist personenbezogen, weil es die Namensangabe des Inhabers und die

ist einzig die Verarbeitungsmöglichkeit auf dem Medium *selbst* entscheidend.

[10] *Weichert* (Fn. 3), Rn. 22.

[11] Beides wird ignoriert von *Weichert* (Fn. 3), der im gesamten Text dem Problem der Verarbeitung „über die Speicherung hinaus" keine Zeile widmet.

[12] *Weichert* (Fn. 3), Rn. 1.

[13] Begründung des Änderungsantrags, BT-Drs. 14/5793, 60. Ebenso Simitis-*Bizer*, § 6 c Rn. 2; *Gola/Schomerus*, § 3 Rn. 59.

[14] Ebenso *Weichert* (Fn. 3), Rn. 10.

[15] Begründung des Änderungsantrag, BT-Drs. 14/5793, 60; *Gola/Schomerus*, § 3 Rn. 58.

[16] S. z.B. Simitis-*Bizer*, § 6 c Rn. 19.

[17] Allgemein zu biometrischen Verfahren vgl. insbesondere TAB-Sachstandsbericht Biometrie, BT-Drs. 14/10005 und die zugrunde liegenden Gutachten.

[18] Ebenso Simitis-*Bizer*, § 3 Rn. 277.

[19] Das wird offensichtlich übersehen von Simitis-*Bizer*, § 6 c Rn. 16, der eine Anwendung (auf Signaturkarten) mit dem Argument ablehnt, die Daten würden „lediglich ... genutzt". Exakt dies erfüllt aber den Tatbestand des automatisierten Verarbeitens nach § 3 Abs. 2 BDSG.

[20] Simitis-*Dammann*, § 3 Rn. 64ff; *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts (2001), 31f.

[21] Für Fingerabdrücke Simitis-*Dammann*, § 3 Rn. 70.

Zuordnung eines Schlüssels zu ihm enthält. Der Schlüssel selbst ist über das Zertifikat personenbeziehbar. Was zunächst den Schlüssel anbelangt, so wird mit diesem auf der Chipkarte die elektronische Signatur für den Hash-Wert eines spezifischen Dokuments berechnet.[22] Dabei wird der Schlüssel selbst zwar nicht verarbeitet, sondern lediglich im Sinne von § 3 Abs. 5 BDSG genutzt.[23] Wie bereits erläutert, reicht aber genau dies für § 3 Abs. 10 Nr. 2 BDSG aus, da dieser auf den weiten Begriff der automatisierten Verarbeitung abstellt.[24] Eine solche liegt hier vor.

Bezüglich des qualifizierten Zertifikats des Karteninhabers gilt, dass auch dieses auf dem Chip gespeichert werden kann.[25] Der Inhaber hat das Zertifikat so stets für eine Aufnahme in ein signiertes Dokument oder für die Übermittlung parat. Bei diesen Vorgängen wird das Zertifikat aus der Chipkarte ausgelesen. Wie beim Auslesen der biometrischen Identifikationsdaten entspricht die Karte hier aber funktional einem reinen Speichermedium, womit eine Anwendung von § 3 Abs. 10 Nr. 2 BDSG ausscheidet.

Hinsichtlich der *Authentifizierung* arbeiten die meisten Karten im sogenannten challange-response-Verfahren. Dabei wird ein beliebiger Datensatz an die Karte gesendet, dort mit dem (vom Signaturschlüssel verschiedenen) Authentifizierungsschlüssel verschlüsselt, zurückgesandt und beim Gegenüber mittels des öffentlichen Schlüssels des Karteninhabers entschlüsselt. Stimmt das Ergebnis dieses Vorgangs mit dem ursprünglich gesendeten Datensatz überein, ist die Authentifizierung erfolgreich. Bei diesem Vorgang wird, ebenso wie bei der Signatur, ein personenbezogener Schlüssel des Karteninhabers genutzt. Auch hier liegt also eine automatisierte Datenverarbeitung vor.

Die *Verschlüsselungsfunktion* der Signaturkarte funktioniert folgendermaßen: Die Kartenchip des Absenders generiert einen einmaligen, symmetrischen Schlüssel, mit dem das Dokument in der Peripherie des Absenders verschlüsselt wird. Der verwendete symmetrische Schlüssel wird dann mit dem öffentlichen Schlüssel des Erklärungsempfängers verschlüsselt und zusammen mit dem verschlüsselten Dokument an diesen versandt. Der Empfänger entschlüsselt mit seinem geheimen Schlüssel auf seiner Signaturkarte den verwendeten symmetrischen Schlüssel und entschlüsselt hiernach mit diesem außerhalb seiner Karte das empfangene Dokument.

Betrachtet man dieses Verfahren unter dem Gesichtspunkt der automatisierten Verarbeitung, so werden sowohl auf der Seite des Absenders wie auf der Seite des Empfängers der jeweilige (personenbezogene) Schlüssel genutzt: Einmal zur Generierung des symmetrischen Schlüssels, einmal zu dessen Entschlüsselung. Auch hier ist damit das Kriterium des § 3 Abs. 10 Nr. 2 BDSG erfüllt.

Findet somit bei allen drei Funktionalitäten der Signaturkarte auf dieser eine automatisierte Verarbeitung statt, so ist der Tatbestand des § 3 Abs. 10 Nr. 2 BDSG aber trotzdem deshalb zweifelhaft, weil der gesamte Vorgang des Signierens, Authentifizierens und Ver- wie Entschlüsselns unter der alleinigen Kontrolle des Signaturkarteninhabers stattfindet. Zwar führt das Erfordernis einer PIN-Eingabe als solches nicht zur Unanwendbarkeit von § 3 Abs. 10 Nr. 2 BDSG, weil diese lediglich der Authentifizierung des Inhabers dient, und dem eigentlichen Verarbeitungsvorgang damit zeitlich vorgelagert ist.[26]

Bei den beschriebenen Vorgängen ist aber auch nach der Eingabe der PIN keine andere Stelle involviert. Damit wird der Karteninhaber zwar noch nicht zur verantwortlichen Stelle im Sinne von § 3 Abs. 7 BDSG, es fehlt aber auch an einer anderen datenverarbeitenden Stelle. Die Daten werden nicht „durch die ausgebende oder eine andere Stelle“, sondern durch den Karteninhaber verarbeitet. Das gilt sogar dann, wenn die Karte in einer fremden Umgebung verwendet wird, weil der ausschließliche Zugriff des Inhabers erhalten bleibt.[27] Damit ist für Signaturkarten weder § 3 Abs. 10 noch § 6 c BDSG einschlägig.[28]

1.2 Verpflichtete Stelle und Berechtigter

Nach § 6 c BDSG sind mehrere Stellen zur Information verpflichtet. Neben der ausgebenden Stelle treffen die Informationspflichten auch Stellen, die sich mit automatisierten Verarbeitungsverfahren in der Weise befassen, dass sie diese auf das Speichermedium aufbringen, auf diesem ändern oder hierzu bereithalten. Das letzte Merkmal erfasst etwa Anbieter, die Verfahren zur Installation durch den Betroffenen vertreiben.[29] Hinter dieser Verpflichtung steht der Gedanke, dass durch das Aufbringen oder Verändern derartiger Verfahren das tatsächliche Potential, und damit die datenschutzrechtliche Relevanz des mobilen Mediums verändert wird. Deshalb soll eine Aufklärung erfolgen.

Unterrichtungsberechtigter ist der Betroffene. Wird über ein Medium informiert, das noch keine Verfahren enthält oder Daten verarbeitet, so ist der Begriff des Betroffenen in § 6 c BDSG allerdings weiter als die allgemeine Definition in § 3 Abs. 1 BDSG und umfasst auch den zukünftig Betroffenen.[30]

1.3 Verhältnis zu Regelungen in LDSG

§ 1 Abs. 2 Nr. 2 BDSG schließt die Anwendung des BDSG aus, soweit eine landesgesetzliche Regelung besteht. Das bedeutet, dass eine Norm des Bundesgesetzes immer dann anwendbar bleibt, wenn das LDSG keine Regelung im sachlichen Geltungsbereich dieser Norm getroffen hat.[31] Hinsichtlich mobiler Speicher- und Verarbeitungsmedien ist die Rechtslage in den Bundesländern uneinheitlich.[32] Soweit einige Län-

[22] Zur Funktionsweise der Signaturerstellung s. *Struif*, GMD-Spiegel 1/1998, 38; *Hammer*, DuD 1993, 636 ff. und *Roßnagel* in: *Ders*., Recht der Multimediadienste, Einl. SigG Rn. 11 ff.

[23] Simitis-*Bizer*, § 3 Rn. 16. Eine Übermittlung darf schon deshalb nicht erfolgen, weil der Schlüssel nach § 15 Abs. 1 Satz 2 SigV nicht preisgegeben werden darf.

[24] Deswegen ist die Argumentation von Simitis-*Bizer*, § 6 c Rn. 16 nicht stichhaltig, der aus der Tatsache der „lediglichen“ Nutzung folgert, § 3 Abs. 10 BDSG sei nicht erfüllt.

[25] Das wird übersehen von Simitis-*Bizer*, § 6 c Rn. 16 f., der hinsichtlich qualifizierter elektronischer Signaturen lediglich die Verwendung des Schlüssels untersucht, für fortgeschrittene Signaturen hingegen eine Speicherung und eventuelle Verarbeitung des Zertifikats auf der Karte annimmt.

[26] Simitis-*Bizer*, § 6 c Rn. 26.

[27] Ob dies auch dann noch gilt, wenn Signaturkarten (z.B. am Arbeitsplatz) in Abhängigkeitsverhältnissen unter fest vorgegebenen Bedingungen in fremdem Interesse genutzt werden, muss der weiteren Entwicklung auf der Prozessebene vorbehalten bleiben.

[28] Für Signaturkarten gelten allerdings die Unterrichtungspflichten des § 6 SigG.

[29] Z.B. nach Herunterladen aus dem Internet, vgl. Begründung, BT-Drs. 14/5793, 63.

[30] Begründung, BT-Drs. 14/5793, 60; Simitis-*Bizer*, § 6 c Rn 31.

[31] Simitis-*Dammann* § 1 Rn. 124 f.

[32] Ein Überblick fehlt hier bislang. Bereits vorhandene sind teilweise unrichtig, etwa der von

der noch keine Novellierung des Datenschutzrechtes vorgenommen oder dabei auf eine Regelung zu mobilen personenbezogenen Speicher- und Verarbeitungsmedien verzichtet haben,[33] bindet § 6 c BDSG auch die öffentlichen Stellen der Länder.

Finden sich in den Landesgesetzen Regelungen, die – bei sprachlichen Abweichungen – inhaltlich § 6 c BDSG entsprechen,[34] so gelten für die öffentlichen Stellen der Länder die entsprechenden landesrechtlichen Normen, ohne das sich daraus allerdings sachliche Unterschiede ergeben.

Derartige Unterschiede bestehen dagegen etwa hinsichtlich der schon erwähnten Mediendefinition, die teilweise einen automatisierten Austausch mit dem Peripheriesystem[35] oder das Anstoßen von Verarbeitungsvorgängen dort[36] ausreichen lassen und so auch reine Speichermedien erfassen. Auch bei den verpflichteten Stellen gibt es Unterschiede. So verpflichtet § 5 b des Hamburgischen LDSG lediglich die ausgebende, nicht jedoch auch eine mit automatisierten Verfahren befasste Stelle.[37] In Bremen wird die „verantwortliche", d.i. datenverarbeitende oder beauftragende Stelle verpflichtet.[38] In Mecklenburg-Vorpommern gelten die Rechte gegenüber der ausgebenden und jeder anderen Stelle, die das Medium zur Datenverarbeitung einsetzt.[39]

In Nordrhein-Westfahlen ist die Ausgabe mobiler Systeme nur mit Einwilligung des Betroffenen und nach dessen Aufklärung zulässig.[40] In anderen Bundesländern wird dem die Variante einer gesetzlichen Ermächtigung zur Seite gestellt.[41] Teilweise ist die erforderliche Unterrichtung auf Wunsch des Betroffenen schriftlich zu erteilen.[42] In Bremen wird auf die Unterrichtung über die Maßnahmen bei Verlust und Zerstörung,[43] in Hessen auf die über die Funktionsweise des Mediums[44] verzichtet. Überwiegend ist schließlich eine Angabe über Identität und Anschrift des Verpflichteten nicht erforderlich.[45]

Sofern die unterschiedlichen LDSG auf von den Ländern ausgegebene Medien Anwendung finden, sind die beschriebenen Unterschiede unproblematisch. Schwierigkeiten ergeben sich aber für den Fall, in dem die Bundesländer ein bundeseinheitlich konzipiertes Medium ausgeben. Das größte Problem dürfte hier der Verzicht einiger Landesgesetze auf ein Verarbeiten auf der Karte selbst sein. Dies könnte dazu führen, dass ein Medium, das nicht unter die engeren, § 6 c BDSG entsprechenden Definitionen fällt, in Brandenburg, Hamburg und Mecklenburg-Vorpommern Unterrichtungspflichten auslösen würde, nicht aber im Rest des Bundesgebietes. Um eine derartige Rechtszersplitterung zu vermeiden, sollte in diesem Fall eine bereichsspezifische Regelung auf Bundesebene für eine einheitliche Unterrichtung sorgen.[46] Je nach Situation und Medium könnte diese auch über den Regelungsgehalt von § 6 c BDSG hinausgehen.

2 Der Regelungsgehalt des § 6 c BDSG

§ 6 c BDSG soll das datenschutzrechtliche Transparenzgebot dadurch fördern, dass der Betroffene bei der Entscheidung unterstützt wird, ob er seine Daten in einem Verfahren unter Einsatz des Mediums bereitstellen will.[47] Wortlaut wie Regelungszweck von § 6 c BDSG sind allerdings auch dann einschlägig, wenn Medien zwangsweise abgegeben werden.

2.1 Rechtmäßigkeit oder Aufklärungsanspruch?

§ 6 c BDSG enthält kein Rechtmäßigkeitserfordernis an die Erhebung und Verarbeitung der Daten auf dem Medium.[48] Zwar würde ein solches die Durchsetzung der Norm erleichtern und auch der engen Verwandtschaft mit §§ 4, 4a BDSG Rechnung tragen, deren Verletzung eine Rechtswidrigkeit der Datenerhebung nach sich zieht[49]. In der Gesetzesbegründung ist aber lediglich davon die Rede, dass die Norm Transparenz hinsichtlich mobiler Medien erreichen soll, nicht aber von einer eventuellen Unrechtmäßigkeit der Datenerhebung mit ihren weitreichenden Folgen. Außerdem spricht § 6 c BDSG davon, dass die jeweilige Stelle „unterrichten muss". Das ist ein deutlicher Unterschied zu der Fassung anderer Normen über die Rechtmäßigkeit der Datenerhebung, in denen es regelmäßig heißt, diese sei „nur zulässig, wenn"[50].

Damit ist jedoch die weitere Frage, ob § 6 c Abs. 1 BDSG einen echten, durchsetzungsfähigen Anspruch enthält, noch nicht beantwortet. Dies könnte deshalb zweifelhaft sein, weil die Norm weder in den Abschnitten über die Rechte des Betroffenen, noch im Rahmen von § 6 BDSG erwähnt wird. Auch die Gesetzesmaterialien sprechen lediglich von Unterrichtungspflichten, nicht jedoch explizit von korrespondierenden Rechten des Betroffenen.

Die Frage muss deshalb nach den allgemeinen Regeln über das vorliegen subjektiver Rechte entschieden werden. Hierbei ist zwischen öffentlichen und nichtöffentlichen Stellen zu differenzieren. Für letztere gilt der allgemeine Grundsatz, dass im Verhältnis zwischen Privaten der Rechtspflicht des einen regelmäßig ein Rechtsanspruch des anderen gegenüber steht.[51] Das gilt auch im vorliegenden Zusammenhang.

Gola/Schomerus, § 6 c Rn. 12. Siehe dazu im Folgenden.

[33] Das betrifft Bayern, Sachsen und Thüringen.

[34] Siehe etwa § 31 c LDSG Bln (wörtliche Übereinstimmung), § 6 a LDSG Nds. und § 35 LDSG RP (leichte sprachliche Abweichungen), § 25 LDSG SA (Verzicht auf eine § 6 c Abs. 2 BDSG entsprechende Regelung), § 20 a LDSG Brem. und § 5 Abs. 2 LDSG BW (mit deutlichen sprachlichen Unterschieden und einer Verpflichtung der „verantwortlichen" Stelle).

[35] § 5 b LDSG HH, § 3 Abs. 10 LDSG MV.

[36] § 5 Abs. 3 LDSG Bbg.

[37] Unrichtig deshalb *Gola/Schomerus*, § 6 c Rn. 12, wonach die Regelung inhaltlich identisch mit § 6 c BDSG sei. Wie in Hamburg: § 5 Abs. 3 LDSG Bbg, § 29a LDSG NW und § 18 LDSG SH.

[38] § 20 a i.V.m. § 2 Abs. 3 Nr. 1 LDSG Brem.

[39] § 36 Abs. 4 LDSG MV.

[40] § 29 LDSG NW.

[41] § 25 LDSG SA (mit der weiteren Variante der Zulässigkeit zum Einsatz von Zugangskontrollsystemen) und § 18 LDSG SH. Diese Variante wird in beiden Fällen übersehen von *Gola/Schomerus*, § 6 c Rn. 12. Entsprechend § 20 a Abs. 1 LDSG Brem. und § 36 Abs. 1 LDSG MV (dort auch im Rahmen von tarifvertraglichen Regelungen und Dienstvereinbarungen zulässig).

[42] § 20 a Abs. 2 S. 1 LDSG Brem. und § 36 Abs. 2 S. 2 LDSG MV.

[43] § 20 a Abs. 2 LDSG Brem.

[44] § 8 Abs. 2 HDSG. Die Norm, obgleich seit 1999 in Kraft, fehlt in der Aufstellung von *Gola/Schomerus*, § 6 c Rn. 12.

[45] Ausnahmen sind etwa § 31 c LDSG Bln, § 6 a LDSG Nds und § 35 LDSG RP.

[46] Eine Alternative wäre ein abgestimmtes Vorgehen der Länder in den jeweiligen Ausführungsgesetzen. Dies ist aber aufwändiger und birgt die Gefahr neuer inhaltlicher Unterschiede.

[47] Begründung des Änderungsantrags, BT-Drs. 14/5793, 63.

[48] *Gola/Schomerus*, § 6 c Rn. 5; Simitis-*Bizer*, § 6 c Rn. 11.

[49] B. Simitis-*Simitis*, § 4 a Rn. 73.

[50] Vgl. etwa §§ 4 Abs. 1, 13 Abs. 1 und Abs. 3, 14 Abs. 1 und 2, 15 Abs. 1, 16 Abs. 1, 28 Abs. 1, 3 und 6, 29 Abs. 1 und 2, 30 Abs. 2 BDSG.

[51] Das liegt daran, dass es im Verhältnis zwischen Privaten die Funktion des Rechts darin besteht, Interessen der Bürger auszugleichen und gegeneinander abzugrenzen. Die Pflichten und Beschränkungen des einen bestehen gerade im

Für öffentliche Stellen sind die Voraussetzungen des subjektiven öffentlichen Rechts maßgeblich. Nach der Schutznormtheorie liegt ein solches Recht dann vor, wenn der Betroffene vom Geltungsbereich des Gesetzes erfasst ist und die Norm nicht nur im öffentlichen Interesse besteht, sondern – zumindest auch – den Interessen des Betroffenen zu dienen bestimmt ist.[52] § 6 c Abs. 1 BDSG dient dem Schutz des Grundrechts auf informationelle Selbstbestimmung des Betroffenen in einem besonders sensiblen Bereich. Insofern ist der notwendige Subjektbezug gegeben.

Aus § 6 c Abs. 1 Nr. 3 BDSG lässt sich überdies ableiten, dass ein enger Zusammenhang der Norm mit den Rechten aus §§ 19, 20, 34 und 35 BDSG besteht. Die Unterrichtungspflicht wirkt quasi unterstützend in deren Vorfeld. Soll § 6 c Abs. 1 BDSG die tatsächliche Wirksamkeit dieser Rechte sichern, so ist es notwendig, auch in der Norm selbst einen durchsetzungsfähigen Anspruch zu sehen. Schließlich lässt sich ein Argument aus der Tatsache gewinnen, dass die Verpflichtung aus § 6 c BDSG nicht bußgeldbewehrt ist. Ohne Anspruch des Betroffenen wäre deshalb jedes Durchsetzungsmittel abgeschnitten. Im Ergebnis enthält § 6 c Abs. 1 BDSG damit für den öffentlichen wie nichtöffentlichen Bereich einen durchsetzbaren Anspruch des Betroffenen auf Unterrichtung.

2.2 Unterrichtung

§ 6 c Abs. 1 Nr. 1 BDSG verpflichtet die unterrichtende Stelle zunächst zur Angabe ihrer *Identität und Anschrift*, was dem Zweck der erleichterten Geltendmachung von Rechten dieser gegenüber dient.[53] Deshalb muss die Unterrichtung den datenschutzrechtlichen Auskunftsanspruch sowie eine eventuelle gerichtliche Durchsetzung ermöglichen.[54]

Nr. 2 bezieht sich sodann auf die *Funktionsweise des Mediums* einschließlich der Art der zu verarbeitenden personenbezogenen Daten.[55] Das betrifft eine sehr breite Gruppe von Fragestellungen, etwa bezüglich des verwendeten Chips und Betriebssystems, der verwendeten Daten, der Zugriffsbefugnisse verschiedener Stellen, des Ablaufs von Auslesevorgängen (einschließlich etwaiger außerhalb des mobilen Mediums ablaufender Verfahrensschritte),[56] der Sicherungsmechanismen gegen unbefugtes Auslesen durch Dritte (insbesondere durch Verschlüsselung), des Potentials des Mediums hinsichtlich zukünftiger Nutzbarkeiten bis hin zu seiner Handhabung im Alltag.

Die Unterrichtung hat hier in „allgemein verständlicher Form“ zu erfolgen. Die besondere Herausforderung liegt dabei darin, Ausdrucksformen für komplizierte technische Vorgänge zu finden, die zwar möglichst jeden Nutzer erreichen, ohne aber gleichzeitig durch eine Übervereinfachung des technischen Ablaufs inkorrekt zu werden. Da eine Typisierung des Unterrichtungsvorgangs unvermeidbar ist, muss insoweit eine Orientierung an den das Medium typischerweise nutzenden Personen erfolgen.[57] Durch eine – nicht vom Gesetz geforderte[58] – Angabe über die Möglichkeit, sich weiterführende Informationen über die technische Funktionsweise des Mediums zu beschaffen, kann daneben der Transparenzgedanke wesentlich gestärkt werden.

§ 6 c Abs. 1 Nr. 3 BDSG verpflichtet zur Auskunft über die *Ausübbarkeit der Betroffenenrechte* aus §§ 19, 20, 34 und 35 BDSG. Hier müssen Angaben zum Verfahrensablauf gemacht werden, außerdem ergibt sich eine Verbindung zu § 6 c Abs. 2 BDSG. Über die dort genannten Geräte oder Einrichtungen zur Wahrnehmung des Auskunftsrechts ist auch im Rahmen von § 6 c Abs. 1 Nr. 3 BDSG, etwa hinsichtlich Standort und Funktionsweise, aufzuklären.[59] Schließlich muss die verpflichtete Stelle gemäß Nr. 4 über die *Maßnahmen* unterrichten, die der Betroffene *bei Verlust oder Zerstörung* des Mediums zu treffen hat.

§ 6 c Abs. 1 BDSG schreibt keine Schriftlichkeit der Unterrichtung vor. Denkbar wäre, in einer Analogie zu §§ 4a Abs. 1 Satz 3, 34 Abs. 3 BDSG auch für § 6 c Abs. 1 BDSG eine solche zu fordern. Ein generelles Schriftformerfordernis war aber vom Gesetzgeber nicht gewollt,[60] weswegen es insoweit an der erforderlichen Regelungslücke fehlt.[61] Allerdings muss die Unterrichtung effektiv sein, und aus diesem Gedanken ergeben sich zwingende rechtliche Anforderungen an die Form der Unterrichtung.

§ 6 c BDSG würde seines Sinns entleert, wenn etwa zwar eine Unterrichtung über die Ausübung von Betroffenenrechten nach § 6 c Abs. 1 Nr. 3 BDSG erfolgt, dies jedoch in einer Art und Weise geschieht, die dazu führt, dass der Betroffene zu dem Zeitpunkt, zu dem er eines dieser Rechte wahrnehmen möchte, nicht mehr auf die Unterrichtung zurückgreifen kann.

Bezüglich der weitaus größten Zahl mobiler Speicher- und Verarbeitungsmedien ergibt sich insoweit, dass wegen der Komplexität der Funktionsweise der Karte und der verwendeten Verarbeitungsverfahren, wie auch wegen des inhaltlichen Umfangs der Unterrichtungspflicht von einer effektiven Information nur gesprochen werden kann, wenn die Inhalte der Unterrichtung dem Karteninhaber dauerhaft, das heißt entweder schriftlich, oder auf einem diesem zur Verfügung gestellten Datenträger, übergeben werden. Selbst wo dies bei sehr simplen Medien nicht gilt, dürfte etwa die Effektivität der Angabe der Anschrift des Verpflichteten nach § 6 c Abs. 1 Nr. 1 BDSG ohne dauerhaftes Medium im Regelfall nicht mehr gegeben sein.

2.3 Zeitpunkt der Unterrichtung

Der *Zeitpunkt* der Unterrichtung wird in § 6 c BDSG nicht angesprochen. Ihrem Sinn und Zweck nach muss sie aber so früh wie möglich erfolgen. Könnte der Betroffene das Medium vor der Aufklärung bereits nutzen, so würde der Zweck der Norm gefährdet. Die Unterrichtung hat damit zum

Interesse des anderen. Vgl. *Maurer*, Allgemeines Verwaltungsrecht (2002), § 8 Rn. 7.

[52] *Maurer* (Fn. 51), § 8 Rn. 8; *Schenke*, Verwaltungsprozessrecht (2002), Rn. 495ff.

[53] Begründung, BT-Drs. 14/5793, 63.

[54] Damit sind die Anforderungen des § 130 Nr. ZPO gemeint. Vgl. im Einzelnen Simitis-*Bizer*, § 6 c Rn. 39.

[55] Siehe Simitis-*Bizer*, § 6 c Rn. 44 ff. und Begründung, BT-Drs. 14/5793, 63.

[56] Begründung, BT-Drs. 14/5793, 63. Zur Notwendigkeit einer Gesamtsicht von Karte und Peripherie zur korrekten Einschätzung der datenschutzrechtlichen Risiken bereits 24. TB HDSG 1995, 169; *Weichert*, DuD 1997, 266, 268.

[57] Simitis-*Bizer*, § 6 c Rn. 49.

[58] Auch die Gesetzesbegründung (BT-Drs. 14/5793, 63) betont, dass detaillierte technische Beschreibungen über § 6 c Abs. 1 BDSG nicht beansprucht werden können.

[59] *Gola/Schomerus*, § 6 c Rn. 7.

[60] Die Begründung (BT-Drs. 14/5793, 64) spricht davon, es liege „in der Eigenverantwortung des Betroffenen, ihm ausgehändigte Handzettel und Broschüren aufzubewahren bzw. sich Notizen über erfolgte Unterrichtungen zu machen“.

[61] Methodisch insoweit inkorrekt Simitis-*Bizer*, § 6 c Rn. 35 f., der dennoch eine „Orientierung“ an der Schriftform nach §§ 4a Abs. 1 S. 4, § 34 Abs. 3 BDSG fordert. Zu den Erfordernissen der rechtlichen Analogiebildung s. allgemein *Larenz/Canaris*, Methodenlehre der Rechtswissenschaft (1995), 191ff.

Zeitpunkt der Übergabe des Mediums bzw. der Aufbringung, Änderung oder Bereithaltung des Verfahrens zu erfolgen. Dies wird für die Übergabe z.B. in § 5b Satz 2 des Hamburgischen LDSG vorgeschrieben.

Eine *Einschränkung* der Unterrichtungspflicht enthält § 6 c Abs. 1 BDSG a.E., wonach die Pflicht entfällt, sofern „der Betroffene ... bereits Kenntnis erlangt hat". Auf den ersten Blick fällt die sprachliche Parallele zu § 19 a Abs. 2 Nr. 1 und § 33 Abs. 2 Nr. 1 BDSG auf. Dort ist jeder Fall erfasst, in dem eine solche Kenntnis auf anderem Wege als durch Benachrichtigung der zuständigen Stelle zustande gekommen ist.[62]

Ausweislich der Gesetzesmaterialien ist dies bei § 6 c Abs. 1 BDSG jedoch nicht gemeint.[63] Dort soll es vielmehr nur darum gehen, bei einer Änderung der angesprochenen Verfahren die Informationspflicht auf den Umfang der Änderung zu beschränken. Es muss damit keine erneute umfassende Unterrichtung erfolgen, sondern es obliegt dem Betroffenen, frühere Informationsquellen aufzubewahren.

Angesichts dieser eindeutigen Gesetzesbegründung ist eine andere Interpretation der Einschränkung nicht möglich.[64] Eine Verneinung der Unterrichtungspflicht in all den Fällen, in denen der Betroffene auf anderem Wege als durch Unterrichtung der verpflichteten Stelle Kenntnis erlangt hat, würde auch der Eindeutigkeit und Effektivität der Unterrichtung widersprechen und die Anbieter von mobilen Medien und den darauf ablaufenden Verarbeitungsverfahren unnötig aus ihrer Informationspflicht entlassen.

Das ändert aber nichts daran, dass die Gesetzesformulierung missglückt ist. Sowohl die sprachliche Fassung der Einschränkung selbst, als auch das Zusammenspiel mit § 19 a Abs. 2 Nr. 1 und § 33 Abs. 2 Nr. 1 BDSG lassen den gesetzgeberischen Willen nicht erkennen, sondern deuten eher auf eine Auslegung der „anderweitigen Kenntnisnahme" entsprechend der zu diesen Normen hin. § 6 c Abs. 1 BDSG sollte deshalb im Wege der Gesetzesänderung klargestellt werden.

2.4 Sonstige Anforderungen

Nach § 6 c Abs. 2 BDSG hat die durch Abs. 1 verpflichtete Stelle die Pflicht, Geräte oder Einrichtungen[65] für die *Wahrnehmung des Auskunftsrechts* in angemessenem Umfang kostenlos zur Verfügung zu stellen.

§ 6 c Abs. 2 BDSG normiert zwar keinen eigenen Auskunftsanspruch, sondern bezieht sich auf die Rechte aus §§ 19 und 34 BDSG. Die Regelung führt aber zu einer gewichtigen Verschiebung der Verantwortlichkeiten. Denn während normalerweise die verantwortliche Stelle i.S.v. § 3 Abs. 7 BDSG (also regelmäßig die Daten verarbeitende oder nutzende Stelle) zur Realisierung des Auskunftsrechts des Betroffenen verpflichtet ist, trifft nach § 6 c Abs. 2 BDSG die Medien ausgebende oder mit einem Verfahren befasste Stelle die Pflicht, die infrastrukturellen Voraussetzungen für die Wahrnehmung des Auskunftsrechts zu schaffen. Je nach Medium und Verfahren können hiermit erhebliche finanzielle Belastungen verbunden sein.

Mit der Beschränkung auf ein zur Verfügung stellen „im angemessenen Umfang" wird auf den konkreten Einzelfall verwiesen. Dabei können Faktoren wie die Sensibilität der im Einzelfall betroffenen personenbezogenen Daten, der wirtschaftliche Aufwand der Auskunftserteilung, die Verbreitung eines Verfahrens und der technischen Fortschritt in die Bewertung mit einfließen.[66] Eine Ausgabe von entsprechenden Lesegeräten an den Betroffenen ist möglich,[67] kann aber aus § 6 c Abs. 2 BDSG nicht beansprucht werden.[68]

Normiert § 6 c Abs. 1 BDSG lediglich eine einmalige Informationspflicht, so muss nach Abs. 3 *jeder Kommunikationsvorgang*, der auf dem Medium eine Datenverarbeitung auslöst, für den Betroffenen eindeutig *erkennbar* sein.[69] Rechtswidrig wäre danach etwa eine Datenverarbeitung, die kontaktlos und ohne sonstige Kenntlichmachung, zum Beispiel beim Vorbeilaufen an einem Terminal, erfolgt.[70] Art und Weise der Erkennbarkeit werden in § 6 c Abs. 3 BDSG nicht normiert. Denkbar sind optische oder akustische Signale, die den Kommunikationsvorgang begleiten. Diese müssen so erfolgen, dass ein Abbruch des Geschehensablaufs noch möglich ist. Wenn durch den Verarbeitungsvorgang dauerhaft Daten auf dem Medium geändert wurden, hat der Betroffene danach die Möglichkeit, sich über seinen Auskunftsanspruch hiervon Kenntnis zu verschaffen.[71]

3 Fazit

§ 6 c BDSG stellt für den in Zukunft immer wichtiger werdenden Bereich mobiler Speicher- und Verarbeitungsmedien einen ersten Ansatz in Richtung auf eine Infrastrukturaufklärung dar. Aufgrund des Erfordernisses einer Verarbeitung auf dem Medium über die Speicherung hinaus ist allerdings eine sorgfältige Analyse der jeweiligen Funktionsweise des Mediums unerlässlich. Bei der Anwendung landesrechtlicher Parallelnormen ergeben sich teilweise erhebliche Unterschiede. Auf der inhaltlichen Ebene verlangt § 6 c Abs. 1 BDSG ausführliche Unterrichtungen, deren Effektivität in weiten Bereichen eine Schriftlichkeit voraussetzt. Schließlich verschiebt § 6 c Abs. 2 BDSG eine Reihe von Verpflichtungen in Bezug auf das Auskunftsrecht weg von der Daten verarbeitenden und hin zur Medien ausgebenden oder Verfahren anbietenden Stelle.

[62] *Gola/Schomerus*, § 33 Rn. 29; Simitis-*Mallmann*, § 33 Rn. 47. Erfasst ist etwa auch die Kenntnis durch Mitteilung von dritter Seite, ebd., Rn. 48.

[63] Begründung, BT-Drs. 14/5793, 64.

[64] S.a. *Gola/Schomerus*, § 6 c Rn. 8. A.A. anscheinend *Bizer* in: *Möller/v. Zezschwitz*, Verwaltung im Zeitalter des Internet (2002), 31, der die Einschränkung wegen der Beweispflicht der ausgebenden und Daten verarbeitenden Stelle über den Umstand der anderweitigen Kenntniserlangung für praktisch folgenlos hält. Das kann sich nur auf eine anderweitige Kenntnisnahme außerhalb eines früheren Informationsakts beziehen, weil dieser durch die Behörde leicht beweisbar ist.

[65] Näher zu diesem Begriff Simitis-*Bizer*, § 6 c Rn. 61 ff.

[66] Begründung, BT-Drs. 14/5793, 64; Simitis-*Bizer*, § 6 c Rn. 66 ff.

[67] *Gola/Schomerus*, § 6 c Rn. 9.

[68] Begründung, BT-Drs. 14/5793, 64.

[69] Dies wurde bereits vor Einführung von § 6 c Abs. 3 BDSG de lege lata angenommen von *Weichert*, DuD 1997, 266, 274. Auch dieser forderte allerdings (S. 276) eine gesetzliche Klarstellung.

[70] Begründung, BT-Drs. 14/5793, 64.

[71] Simitis-*Bizer*, § 6 c Rn. 72.