

Dr. Ivo Geis

Datenschutzrecht

Szenarien und Fälle

Vorlesung Datenschutzrecht 02.345

Wintersemester 2005/2006

Hamburg, Dezember 2005

Inhalt

Anwendbarkeit des BDSG	3
Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten:	6
Beteiligte an der Erhebung, Verarbeitung und Nutzung personenbezogener Daten.....	10
Rechte der Betroffenen.....	12
Fall zur Anwendbarkeit des BDSG und zur Zulässigkeit der Erhebung, Verarbeitung und Nutzung	13
Werbung, Marketing und die Verarbeitung von Kundendaten	15
Grenzüberschreitender Datenaustausch	19
Datenschutz und Technik	21

Anwendbarkeit des BDSG

Fall:

Ein Unternehmen mit Sitz in der Bundesrepublik Deutschland plant die elektronische Verwaltung der Personalakten. Hierzu sollen die Papierakten durch Scannen in elektronische Daten umgewandelt und auf elektronischen Datenträgern gespeichert werden. Die Personalabteilung soll ausschließlich in elektronischer Form mit einer Personalbearbeitungssoftware erfolgen. Hierzu gehört das Erheben der Personaldaten und jede Form des Verarbeitens und Nutzens. Welche Anforderungen bestehen nach Datenschutzrecht?

1.0 Prüfung nach § 1 Abs. 2 BDSG

Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch öffentliche Stellen und durch nicht-öffentliche Stellen

1.1 personenbezogene Daten

Definition: § 3 Abs. 1 BDSG

„Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (Betroffener).“

1.2 öffentliche Stellen

1.2.1 öffentliche Stellen des Bundes

Definition: § 2 Abs. 1 BDSG

„Behörden, Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes“

1.2.2 öffentliche Stellen der Länder

Definition: § 2 Abs. 2 BDSG

„Behörden, Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen der Länder“

1.3 nicht-öffentliche Stellen

nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben

1.3.1 Definition nicht-öffentliche Stelle: § 2 Abs. 4 BDSG:

„Natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts“

1.3.2 Definition „Datenverarbeitungsanlage“: § 3 Abs. 2 S 1 BDSG

„Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen.“

2.0 Prüfung nach § 3 BDSG

2.1 Erheben

§ 3 Abs. 3 BDSG

„Ist das Beschaffen von Daten über den Betroffenen (§ 3 Abs. 1 BDSG).“

2.2 Verarbeiten

§ 3 Abs. 4 BDSG

„Ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten.“

2.2.1 Speichern, § 3 Abs. 4 Nr. 1 BDSG

Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger.

2.2.2 Verändern, § 3 Abs. 4 Nr. 2 BDSG

Das inhaltliche Umgestalten personenbezogener Daten

2.2.3 Übermitteln, § 3 Abs. 4 Nr. 3 BDSG

Bekanntgeben personenbezogener Daten an einen Dritten (§ 3 Abs. 8 S 2 BDSG), indem die Daten an den Dritten weitergegeben werden oder von dem Dritten eingesehen/abgerufen werden.

2.2.4 Sperren, § 3 Abs. 4 Nr. 4 BDSG

Kennzeichnen gespeicherter personenbezogener Daten, um die weitere Verarbeitung /Nutzung einzuschränken.

2.2.5 Löschen, § 3 Abs. 4 Nr. 5 BDSG

Unkenntlichmachen gespeicherter personenbezogener Daten.

2.2.6 Nutzen, § 3 Abs. 5 BDSG

Jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten:

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nach § 4 Abs. 1 BDSG nur zulässig, soweit dieses Gesetz oder eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Eine solche Rechtsvorschrift ist § 28 BDSG. In den Kreis dieser Rechtsvorschriften werden auch Betriebsvereinbarungen einbezogen.

1.0 §28 BDSG

1.1 § 28 Abs. 1 S 1 BDSG - Erfüllung eigener Geschäftszwecke

Datenerhebung, -verarbeitung und -nutzung ist zulässig

- im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen,
- zur Wahrung berechtigter Interessen der verantwortlichen Stelle, wenn das schutzwürdige Interesse des Betroffenen nicht überwiegt,
- die Entnahme der Daten aus allgemein zugänglichen Quellen und zur Durchführung wissenschaftlicher Forschung.

1.2 § 28 Abs. 1 Nr. 1 BDSG – Zweckbestimmung eines Vertrages

Wenn sie zur Erfüllung der Pflichten oder zur Wahrnehmung der Rechte aus einem mit dem Betroffenen geschlossenen Vertrag vorgenommen wird.¹

Problemfall: Einstellen von Personaldaten in das Internet.

Der Zweckbestimmung eines Anstellungsvertrages kann eine im Internet angebotene Kontaktmöglichkeit mit bloßer Funktionsbezeichnung des Mitarbeiters entsprechen, z.B. Bearbeitung von Beschwerden, Presseauskunft und im Internet-Vorlesungsverzeichnis Name, Kontaktadresse, Forschungsgebiet.²

Vertragsähnliches Vertrauensverhältnis, z.B.:

- Das Speichern von Bankauskünften und Bonitätsdaten über den potentiellen Kunden.
- Das Speichern von Bewerberdaten im arbeitsrechtlichen Anbahnungsverhältnis.

¹ Gola/Schomerus, BDSG-Kommentar, 8. Aufl. (2005), § 28 Rz. 13.

² Gola/Schomerus, BDSG-Kommentar, 8. Aufl. (2005), § 28 Rz. 22.

1.3 § 28 Abs. 1 Nr. 2 BDSG - Interessenabwägung

Die Zulässigkeitsnorm der Interessenabwägung wird als Begründung für die zielgruppenorientierte Werbung diskutiert. Die schutzwürdigen Interessen des Betroffenen gelten als verletzt, wenn Zusatzangaben wie „Kreditkäufer“, „Jagdartikelinteressent“, „Blindenwarenkäufer“ angegeben werden oder Mitgliederlisten eines Sportvereins für Werbezwecke an Sportartikelhersteller übermittelt werden.³

1.4 § 28 Abs. 1 Nr. 3 – allgemein zugängliche Daten

Als allgemein zugängliche Quellen gelten, Zeitungen, Zeitschriften, Rundfunk, Fernsehen, Internet. Öffentliche Register zählen dazu, wenn die Einsichtnahme nicht von einem besonderen berechtigten Interesse abhängig ist, so das Schuldnerverzeichnis, das Handelsregister, das Vereinsregister. Hierzu zählt nicht das Grundbuch, da ein berechtigtes Interesse zur Einsicht nachgewiesen muss.

1.5 Zweckbindung, Zweckänderung, Hinweispflichten

§ 28 Abs. 1 S. 2 BDSG.

Bei Erhebung der Daten ist die vorgesehene Zweckbestimmung schriftlich zu dokumentieren.

§ 28 Abs. 2 BDSG gestattet spätere Zweckänderungen und –erweiterungen, indem die Daten für zunächst nicht berücksichtigte oder bestehende Zwecke genutzt oder übermittelt werden dürfen, sofern der neue Zweck durch die Erlaubnistatbestände des Absatzes 1 Satz 1 gedeckt ist. Beispiel: Die Ausweitung eines auf ein Konzernunternehmen bezogenen Anstellungsvertrages auf den Gesamtkonzern.

§ 28 Abs. 3 S. 1 Nr. 1 und Nr. 2 BDSG

Die Übermittlung von Daten kann nicht nur durch die „eigenen Zwecke“ der übermittelnden Stelle, sondern auch durch bei einem Dritten bestehende Interessen bedingt sein. So die Übermittlung von Kundendaten im Rahmen der Betriebsübergabe an einen Nachfolger (§ 28 Abs. 3 S. 1 Nr. 1 BDSG) und die Übermittlung von Mieter- und Kundendaten an die Polizei, sofern keine speziell geregelte Mitteilungspflicht besteht (§28 Abs. 3 S. 1 Nr. 2 BDSG).

³ Gola/Schomerus, BDSG-Kommentar, 8. Aufl. (2005), § 28 Rz. 39.

§ 28 Abs. 5

Der Dritte darf die übermittelten Daten nur für den Zweck verarbeiten oder nutzen, der die Übermittlung rechtfertigt.⁴

2.0 Einwilligung, § 4a BDSG

Voraussetzungen

- freie Entscheidung des Betroffenen
- grundsätzlich Schriftform
- Einwilligung in Formularverträgen: AGB-Inhaltskontrolle
- Stillschweigende Einwilligung bei lang andauernder Geschäftsbeziehung

Widerruf der Einwilligung.

Das BDSG äußert sich nicht zu dem Fall, dass der Betroffene einer Verarbeitung, zu der er seine Einwilligung erteilt hat, später widerspricht. Es wird angenommen, dass der Betroffene grundsätzlich berechtigt ist, eine einmal erteilte Genehmigung auch wieder zurück zu nehmen. Ein Widerruf wird allerdings als unzulässig angesehen, wenn dadurch die weitere Abwicklung des Vertrages mit dem Betroffenen in Frage gestellt oder unbillig erschwert wird. So z.B. wenn der Betroffene eingewilligt hat, dass seine Daten an eine privatärztliche Verrechnungsstelle übermittelt werden. Nach erfolgter ärztlicher Behandlung wird er die Einwilligung für die weitere Abwicklung des Behandlungsvertrages nicht widerrufen können.⁵

3.0 Betriebsvereinbarung

Die Einbeziehung von Betriebs- und Dienstvereinbarungen in den Kreis der anderen Rechtsvorschriften, durch die die Zulässigkeit der Verarbeitung abweichend vom BDSG geregelt werden kann, wird als erforderlich angesehen, weil die Verarbeitung von Personaldaten im Betrieb sinnvoll nur nach einheitlichen Gesichtspunkten erfolgen kann.⁶

⁴ Siehe zu dem Abschnitt „Zweckbindung, Zweckänderung, Hinweispflichten“ *Gola/Schomerus*, BDSG-Kommentar, 8. Aufl. (2005), § 28 Rz. 50-52.

⁵ *Gola/Schomerus*, BDSG-Kommentar, 8. Aufl. (2005), § 4a Rz. 18.

⁶ *Gola/Schomerus*, BDSG-Kommentar, 8. Aufl. (2005), § 4 Rz. 10.

4.0 Allgemeine Regeln der Erhebung, Verarbeitung und Nutzung

4.1 Datenvermeidung, § 3a S.1 BDSG

Durch die Gestaltung der Systemstrukturen soll die Erhebung, Verarbeitung, Nutzung personenbezogener Daten möglichst vermieden werden.

4.2 Anonymisieren und Pseudonymisieren, § 3a S. 2 BDSG

Personenbezogene Daten sollen möglichst anonymisiert oder pseudonymisiert werden.

Anonymisieren ist das Verändern von Daten, sodass eine Zuordnung zu einer Person erschwert ist, § 3 Abs. 6 BDSG. Pseudonymisieren ist das Ersetzen des Namens, § 3 Abs. 6a BDSG.

4.3 Datengeheimnis, § 5 BDSG

Im nicht-öffentlichen Bereich sind Beschäftigte auf das Datengeheimnis zu verpflichten.

Besteht diese Verpflichtung bereits aufgrund dienstlicher Vorschriften entfällt eine Verpflichtung nach § 5 BDSG.

Beteiligte an der Erhebung, Verarbeitung und Nutzung personenbezogener Daten

Fall 1

Ein Unternehmen erhebt und verarbeitet Personaldaten in elektronischen Systemen.

Es handelt sich um die Erhebung und Verarbeitung personenbezogener Daten durch eine nicht-öffentliche Stelle. Das BDSG ist damit gemäß § 1 Abs. 2 BDSG anwendbar. Das Unternehmen ist die verantwortliche Stelle (§ 3 Abs. 7 BDSG), die Mitarbeiter sind die Betroffenen (§ 3 Abs. 1 BDSG).

Die Datenverarbeitung ist nach § 28 Abs. 1 Nr. 1 BDSG zulässig, wenn sie der Zweckbestimmung des Vertragsverhältnisses mit dem Betroffenen dient. Die Datenverarbeitung entspricht dem Zweck des Arbeitsvertrages zwischen dem Unternehmen als verantwortlicher Stelle und den Mitarbeitern als Betroffenen

Fall 2

Das Unternehmen beabsichtigt, die Personaldaten durch ein anderes Unternehmen als Dienstleister bearbeiten (Outsourcing) zu lassen.

Das dienstleistende Unternehmen befindet sich außerhalb der verantwortlichen Stelle und ist damit Dritter (§ 3 Abs. 8 S. 2). Die Dienstleistung wird nicht durch den Zweck der Arbeitsverträge gedeckt, da das dienstleistende Unternehmen nicht Vertragspartner der Mitarbeiter ist. Die Zulässigkeit der Datenverarbeitung ergibt sich damit nicht aus § 28 Abs. Nr. 1 BDSG. Notwendig ist eine Einwilligung der Mitarbeiter oder eine Betriebsvereinbarung.

Betroffener

Eine natürliche Person, die durch Einzelangaben über persönliche oder sachliche Verhältnisse bestimmt oder bestimmbar ist, § 3 Abs. 1 BDSG.

Verantwortliche Stelle

Der Sammelbegriff für die in § 2 BDSG als Normadressat des Gesetzes beschriebene öffentlich und nicht-öffentliche Stelle. Jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt, § 3 Abs. 7 BDSG

Empfänger

ist jede Person oder Stelle, die Daten erhält, § Abs. 8 S. 1 BDSG.

Dritter

Ist jede Person oder Stelle außerhalb der verantwortlichen Stelle, § 3 Abs. 8 S. 2 BDSG.

Dritte sind nicht

- der Betroffene
- Personen und Stellen, die personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen. Der Auftragnehmer darf nach § 11 Abs. 3 BDSG die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.

Rechte der Betroffenen

Die Betroffenen haben die Rechte auf Benachrichtigung, Auskunft, Berichtigung, Löschung, Sperrung und Schadensersatz.

1. Benachrichtigung

Durch den Grundsatz der Direkterhebung nach § 4 Abs. 2 BDSG erhält der Betroffene Kenntnis von der Erhebung, Verarbeitung, Nutzung der Daten. Werden die Daten nicht direkt erhoben, so ist der Betroffene über die Erhebung, Verarbeitung und Nutzung zu benachrichtigen.

Die Benachrichtigung ist für den öffentlichen Bereich (§ 19a BDSG) und nicht-öffentlichen Bereich (§ 33 BDSG) gleich geregelt. Der Betroffene ist

- über die Speicherung,
- über die Identität der verantwortlichen Stelle
- über die Zweckbestimmung der Erhebung, Verarbeitung und Nutzung,
- über die Empfänger, soweit der Betroffene nicht mit der Übermittlung rechnen musste zu unterrichten.

2. Auskunft

Der Betroffene hat ein Recht auf Auskunft, das im öffentlichen Bereich (§ 19 BDSG) und nicht-öffentlichen Bereich (§ 34 BDSG) gleichartig ausgestaltet ist. Die Auskunft ist zu erteilen

- über die zu seiner Person gespeicherten Daten,
- die Empfänger, an die die Daten weitergegeben werden,
- den Zweck der Speicherung.

3. Berichtigung, Löschung, Sperrung

Der Betroffene hat ein Recht auf Berichtigung, Löschung, Sperrung, das im öffentlichen Bereich (§ 20 BDSG) und nicht-öffentlichen Bereich (§ 35 BDSG) gleichartig ausgestaltet ist:

- Die Daten sind zu berichtigen, wenn sie unrichtig sind,
- Die Daten sind zu löschen, wenn die Speicherung unzulässig ist oder die Daten zur Erfüllung der Aufgaben nicht mehr erforderlich sind,
- Die Daten sind zu sperren statt zu löschen, wenn Aufbewahrungspflichten bestehen, schutzwürdige Interessen oder der Aufwand für die Löschung zu hoch ist.

4. Schadensersatzansprüche des Betroffenen

Im öffentlichen Bereich besteht nach § 8 BDSG eine Gefährdungshaftung für einen Schaden, der durch rechtswidrige Erhebung, Verarbeitung, Nutzung personenbezogener Daten entsteht.

Im nicht-öffentlichen Bereich kann sich nach § 7 BDSG die verantwortliche Stelle von der Haftung exculpieren, indem sie nachweist, dass sie die nach den Umständen gebotene Sorgfalt beachtet hat.

Fall zur Anwendbarkeit des BDSG und zur Zulässigkeit der Erhebung, Verarbeitung und Nutzung

Die Muttergesellschaft eines in der Bundesrepublik Deutschland ansässigen Konzerns beschließt im Rahmen der Umstrukturierung und Kostensenkung, dass die Personalabteilungen der Konzerngesellschaften die Personaldaten an die zentrale „Personal AG“ senden. Für dieses Outsourcing werden zwei Modelle diskutiert

- die Personal AG verarbeitet auf Weisung der Tochtergesellschaften Gehaltslisten oder
- die Personal AG hat weitergehende Funktionen wie die Karriereplanung.

Der Vorstand fordert eine Stellungnahme je Outsourcingmodell zu folgenden Fragen an:

1. Ist das BDSG anwendbar?
2. Welche Anforderungen stellt das BDSG an die Zulässigkeit des Outsourcens?

Der Gesamtbetriebsrat des Konzerns möchte wissen,

1. ob die Mitarbeiter über das Outsourcingmodell zu benachrichtigen sind und
2. ob den Mitarbeitern Rechte aus dem BDSG zustehen, um die rechtmäßige Erhebung, Verarbeitung und Nutzung ihrer Daten zu kontrollieren.

Lösung:

Ein privatrechtlich organisiertes Unternehmen erhebt, verarbeitet und nutzt personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen. Damit ist das BDSG nach § 1 Abs. 2 BDSG anwendbar.

Wird die Personaldatenverarbeitung an die „Personal AG“ mit der Weisung übertragen Gehaltslisten zu verarbeiten, so wird die „Personal AG“ im Rahmen der Weisungen des Auftraggebers tätig. Eine darüber hinausgehende selbständige Tätigkeit der „Personal AG“ ist nicht gegeben. Die Vertragsbeziehung ist damit als Auftragsdatenverarbeitung nach § 11 BDSG zu bewerten. Die „Personal AG“ ist als Auftragnehmer nicht Dritter, § 3 Abs. 8 S. 3 BDSG. Die Konzerngesellschaften bleiben als Auftraggeber für die Einhaltung der Vorschriften des Datenschutzrechts verantwortlich. Die gesetzliche Grundlage für die Erstellung der Gehaltslisten entspricht dem Zweck des Arbeitsvertrages gemäß § 28 Abs. 1

Nr. 1 BDSG. Eine Einwilligung der Arbeitnehmer oder eine Betriebsvereinbarung ist nicht notwendig.

Übernimmt die „Personal AG“ weitere Funktionen wie die Karriereplanung so ist der enge Rahmen des § 11 Abs. 3 BDSG „Rahmen der Weisungen“ verlassen, so dass keine Auftragsdatenverarbeitung gegeben ist und die Rechtsgrundlage des § 28 Abs. 1 Nr. 1 BDSG entfällt. Eine Rechtsgrundlage kann entstehen durch Einwilligung der Betroffenen oder durch Betriebsvereinbarung.

Der Gesamtbetriebsrat ist zu informieren, dass die Mitarbeiter über das Outsourcen in beiden Modellen zu benachrichtigen sind (§ 33 BDSG), dass sie ein Recht auf Auskunft haben (§ 34 BDSG), auf Berichtigung, Löschung und Sperrung der Daten, wenn diese unrichtig sind (§ 35 BDSG).

Werbung, Marketing und die Verarbeitung von Kundendaten

1.0 Datenverarbeitung zu Zwecken der Werbung, Markt – und Meinungsforschung

1.1 Das Listenprivileg

Für Unternehmen, die Daten primär für eigene Zwecke verarbeiten und ausnahmsweise zum Zweck der Werbung übermitteln oder zur Nutzung zu diesem Zweck erhalten, besteht das Listenprivileg des § 28 Abs. 3 S. 1 Nr. 3 BDSG. Erforderlich ist ein listenmäßig oder sonst zusammengefasster Datenbestand, der einheitliche Angaben zu einer Personengruppe enthält.⁷ Ist die Werbung für den Betroffenen unerwünscht, so hat er einen zivilrechtlichen Unterlassungsanspruch.⁸

1.2 Der zivilrechtliche Unterlassungsanspruch

Nach der deutschen Rechtsprechung ist die Versendung elektronischer Werbepost ohne vorherige Zustimmung des Empfängers rechtswidrig. Damit gilt das Opt-In-Prinzip, wonach bereits die erstmalige Versendung von Werbung ohne vorherige Zustimmung des Empfängers untersagt ist.⁹ Die Begründung ist für die private E-Mail-Adresse und den geschäftlich genutzten E-Mail-Anschluss unterschiedlich. Werbung, die ohne tatsächliches oder mutmaßliches Einverständnis des Empfängers an eine private E-Mail-Adresse gesandt wird, gilt als rechtswidriger Eingriff in das allgemeine Persönlichkeitsrecht gemäß § 823 Abs. 1 BGB und begründet damit gegen den Versender unerbetener Werbung einen Unterlassungsanspruch gemäß § 1004 BGB.¹⁰ Unerwünschte Werbung, die an einen geschäftlich genutzten E-Mail-Anschluss gerichtet ist, wird von der Rechtsprechung als Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb gewertet, der ebenfalls einen Unterlassungsanspruch nach § 823 Abs. 1 i.V.m. § 1004 BGB begründet.¹¹ Im Rechtsstreit muss der Absender das Einverständnis des Empfängers beweisen.¹² Diese Rechtsprechung

⁷ Gola/Schomerus, BDSG-Kommentar, 8. Aufl. (2005), § 28 Rz. 56.

⁸ Gola/Schomerus, BDSG-Kommentar, 8. Aufl. (2005), § 28 Rz. 54.

⁹ OLG Koblenz v. 10.6.2003, CR 2003, 766 = MMR 2003, 590; LG Berlin v. 16.5.2002, CR 2002, 606 = MMR 2002, 631; Härtling/Eckart, CR 2004, 119.

¹⁰ LG Berlin v. 19.9.2002, CR 2003, 219.

¹¹ KG v. 8.1.2002, MMR 2002, 685; LG München v. 15.4.2003, CR 2003, 615; LG Berlin v. 16.5.2002, CR 2002, 206 = MMR 2002, 631.

¹² BGH v. 11.3.2004, CR 2004, 445 ff.

findet ihre Bestätigung jetzt auch in der seit dem 8.7.2004 geltenden Fassung des § 7 Abs. 2 Nr. 3 UWG, die für Verbraucher und Unternehmer gilt.¹³

1.3 Das datenschutzrechtliche Widerspruchsrecht

Um diesem Anspruch des Betroffenen auf die Abwehr unerwünschter Werbung Rechnung zu tragen, räumt ihm § 28 Abs. 4 BDSG ein uneingeschränktes Widerspruchsrecht gegenüber der verantwortlichen Stelle bezüglich der Nutzung oder Übermittlung seiner Daten zu Zwecken der Werbung oder Markt- und Meinungsforschung ein. Über die Form des Widerspruchs äußert sich das Gesetz nicht. Ein Telefonanruf muss deshalb genügen.¹⁴ Nach § 28 Abs. 4 S. 2 BDSG hat die verantwortliche Stelle, die die werbliche Ansprache durchführt, gegenüber dem Betroffenen eine Belehrungs- und Informationspflicht über sein Widerspruchsrecht.¹⁵

2.0 Kundendaten und Marketing

2.1 Datawarehouse, Datamining, Scoring

Die Datenverarbeitung verändert sich grundlegend durch die multifunktionelle Nutzung eines globalen und vernetzten Datenbestandes bei wachsenden Speicherkapazitäten.¹⁶ Datenbestände werden durch eine Data-Warehouse Strategie in Datenbanken verfügbar gehalten. Durch Klassifikation und Verknüpfung werden diese Daten verdichtet. Hierdurch werden zusätzliche Informationen und bisher unbekannte Trends generiert und verarbeitet. Data-Mining Tools ermöglichen die automatisierte Suche nach zusätzlichen Daten in käuflichen Adressdateien. Durch intelligente Menüführung können Abfragen formuliert und ausgewertet werden. Spezifische Eigenschaften von Personengruppen als Kunden, Stellenbewerber oder Arbeitnehmer können in einem automatisch ermittelten Punktwert, dem Scorewert, abgebildet werden.¹⁷ Die Personen können in einem skalierenden Vergleich nach Kaufkraft, Kaufgewohnheiten, Interessengebieten und Kreditwürdigkeit bewertet und als Zielgruppen definiert werden. Dies ermöglicht die zielgerichtete Ansprache und das zielgerichtete Angebot von Produkten.

¹³ Siehe hierzu *Köhler*, NJW 2004, 2121, 2125.

¹⁴ *Gola/Schomerus*, BDSG-Kommentar, 8. Aufl. (2005), § 28 Rz. 59.

¹⁵ *Gola/Schomerus*, BDSG-Kommentar, 8. Aufl. (2005), § 28 Rz. 62.

¹⁶ *Bizer*, in: Simitis (Hrsg.), Kommentar zum BDSG, 5. Aufl. (2003), § 3a, Rn. 15.

¹⁷ Zum Scoringverfahren: *Bizer*, in: Simitis (Hrsg.), Kommentar zum BDSG, 5. Aufl. (2003), § 3a, Rn. 30 ff.

2.2 Bewertung nach Datenschutzrecht

2.2.1 Das Verbot des § 28 Abs. 1 BDSG

Datawarehouse und Datamining ist nach § 28 BDSG nicht legitimiert. Das Verfahren entspricht nicht dem Zweck des zwischen verantwortlicher Stelle und Betroffenen bestehenden Vertrag (§ 28 Abs. 1 Nr. 1 BDSG) und kann auch nicht mit berechtigten Interessen der verantwortlichen Stelle nach § 28 Abs. 1 Nr. 2 BDSG begründet werden.¹⁸ Im Datawarehouse und Datamining bedarf das informationelle Selbstbestimmungsrecht des besonderen Schutzes.¹⁹

2.2.2 Informationelles Selbstbestimmungsrecht und das Recht auf den Kernbereich privater Lebensgestaltung

Personenbezogene Daten werden nach dem Volkszählungsurteil des Bundesverfassungsgerichts durch das Recht auf informationelle Selbstbestimmung verfassungsrechtlich geschützt: die Befugnis, über die Preisgabe und Verwendung der eigenen persönlichen Daten zu bestimmen.²⁰ Das Bundesverfassungsgericht verdeutlicht im Volkszählungsurteil, dass es das informationelle Selbstbestimmungsrecht nicht in einer sphärenbezogenen Weise interpretiert, sondern dass dieses Recht vor Gefahren schützt, die sich aus der Zusammenfügung mit anderen Datensammlungen zu einem mehr oder weniger vollständigen Persönlichkeitsbild ergeben, dessen Richtigkeit und Verwendung der Betroffene nur unzureichend kontrollieren kann.²¹ Damit entfaltet das Recht auf informationelle Selbstbestimmung einen flexiblen, gegenüber technischen und gesellschaftlichen Entwicklungen reagiblen und an der konkreten Gefährdungssituation ausgerichteten Gewährleistungsgehalt.²² Als absolutes Nutzungs- und Verfügungsrecht analog dem Eigentum ist das informationelle Selbstbestimmungsrecht nicht anerkannt.²³ Die Konstruktion als absolutes Nutzungs- und Verfügungsrecht gilt als nicht angemessen, da der Betroffene kein Herrschaftsrecht über Informationen beanspruchen kann, die erst der Verwender aus einem Bestand von Daten konstruiert hat.²⁴ Schutzwürdig ist aber sein Recht, die

¹⁸ *Gola/Schomerus*, BDSG-Kommentar, 2005, 8. Aufl., § 28 Rz. 12.

¹⁹ *Gola/Schomerus*, BDSG-Kommentar, 2005, 8. Aufl., § 1 Rz. 8.

²⁰ BVerfGE 65, 1 (41 ff.).

²¹ BVerfGE 65, 1 (42).

²² Auf die Gefährdungsabhängigkeit stellt *Trute*, Verfassungsrechtliche Grundlagen, in: Rossnagel (Hrsg.), Handbuch des Datenschutzrechts, 2003, S. 156 ff., Rn. 14, ab.

²³ So aber *Ladeur*, DuD2000, 12, 18.

²⁴ *Trute*, Verfassungsrechtliche Grundlagen, in: Rossnagel (Hrsg.), Handbuch des Datenschutzrechts, 2003, S. 156 ff., Rn. 21.

Verwendung seiner persönlichen Daten durch Dritte kennen und kontrollieren zu können.²⁵ Dies gilt besonders dann, wenn diese Verwendung sich für ihn selbst als folgenreich erweist. Denn nicht allein Art und Umfang der erhobenen Daten sind grundrechtsrelevant, vielmehr kommt es auch auf die denkbaren Verwendungen und das jeweilige Missbrauchspotential an.²⁶ Dies wird von der aktuellen Rechtsprechung des Bundesverfassungsgerichts bestätigt: Durch die Urteile des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung vom 3.3.2004²⁷ und vom 27.7.2005²⁸ zu dem Gesetz des Landes Niedersachsen zur präventiven Verbrechensbekämpfung durch Datenspeicherung ist der „Kernbereich privater Lebensgestaltung“ entwickelt worden. Dieser kann durch die Erhebung und Weitergabe von Informationen aus diesem Bereich beeinträchtigt werden. In den „Kernbereich privater Lebensgestaltung“ sollte deshalb auch das Recht einbezogen werden, über die Erhebung und Verarbeitung der Daten informiert zu sein. Im Ergebnis ist Datawarehouse, Datamining und Scoring nach dem informationellen Selbstbestimmungsrecht und dem Recht auf den Kernbereich privater Lebensgestaltung nur möglich, wenn diese Formen der Datenverarbeitung dem Betroffenen bekannt gegeben werden und ihm die Möglichkeit gegeben ist, dies abzulehnen oder einzuwilligen.

²⁵ *Trute*, Verfassungsrechtliche Grundlagen, in: Rossnagel (Hrsg.), Handbuch des Datenschutzrechts, 2003, S. 156 ff., Rn. 19.

²⁶ Vgl. BVerfGE 65, 1 (46).

²⁷ BVerfG, Urt.v.3.3.2004, NJW 2004, 999.

²⁸ BVerfG, Urt.v.27.7.2005, NJW 2005, 2603.

Grenzüberschreitender Datenaustausch

Fall 1: Elektronischer Buchhandel

Europaweite Verarbeitung von Kundendaten

Unternehmen mit Sitz in BRD übermittelt Daten in EU-Mitgliedsland, um Daten im Rahmen des Vertragszwecks zu verarbeiten.

§ 4b Abs. 1 BDSG

Entscheidend ist die Berechtigung nach deutschem Recht.

Besteht nach § 28 Abs. 1 Nr. 1 BDSG.

Fall 2: Lufthansa

Verarbeitung von Flugdaten einer Fluggesellschaft mit Sitz in der BRD in USA, um den Reisevertrag abzuwickeln.

§ 4b Abs. 2 BDSG:

Erforderlich ist, dass ein „angemessenes Datenschutzniveau gewährleistet“ wird.

§ 4b Abs. 3 BDSG

Angemessenheit des Schutzniveaus ist unter Berücksichtigung aller Umstände zu beurteilen, die ...von Bedeutung sind.

§ 4c Abs. 1 BDSG

Ist ein angemessenes Datenschutzniveau nicht gewährleistet, so ist die Übermittlung zulässig, wenn

- der Betroffene eingewilligt hat,
- die Übermittlung zur Erfüllung eines Vertrages zwischen Betroffenenem und verantwortlicher Stelle erforderlich ist.

Fall 3 Konzernweite Datenflüsse

Die Muttergesellschaft eines Konzerns mit Sitz in Deutschland übermittelt Daten ihrer Mitarbeiter an eine Tochtergesellschaft mit Sitz in USA

§ 4c Abs. 1 Nr. 2 BDSG (Vertragszweck) ist nicht Rechtsgrundlage, da der Vertrag des Betroffenen mit der Muttergesellschaft nicht aber mit der Tochtergesellschaft in USA besteht.

Dann kann nach § 4c Abs. 2 BDSG die Genehmigung durch die Aufsichtsbehörde die Datenübermittlung ermöglichen. Voraussetzung sind ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts. Dies ist möglich, indem sich der Empfänger zur Beachtung des Datenschutzrechts entsprechend BDSG verpflichtet. Dies geschieht durch Betriebsvereinbarungen, Standardvertragsklauseln und Codes of Conduct.

Fall 4 Datenverarbeitung von EU-Unternehmen in BRD

Erhebt, verarbeitet und nutzt ein Unternehmen mit Sitz in einem EU-Mitgliedsland Daten in der BRD, so gilt nach § 1 Abs. 5 S 1 BDSG das Datenschutzrecht des EU-Mitgliedslandes, in dem das Unternehmen seinen Sitz hat.

Fall 5 Datenverarbeitung von Nicht-EU-Unternehmen in BRD

Erhebt, verarbeitet und nutzt ein Unternehmen mit Sitz in einem anderen Nicht-EU-Mitgliedsland Daten in der BRD, so gilt nach § 1 Abs. 5 S 2 BDSG das BDSG.

Datenschutz und Technik

Automatisierte Einzelentscheidung, § 6a BDSG

Scoringverfahren

Videoüberwachung, § 6b BDSG

Mobile personenbezogene Speicher und Verarbeitungsmedien, § 6c BDSG

Chipkarten, Smart Cards, RFID-Funktion

Automatisierte Verarbeitung, § 10 BDSG

Automatisierter Abruf von Daten, wie Kontenabfrage der Finanzbehörden bei Banken, Abruf der zentralen Personalverarbeitungsgesellschaft bei Konzerngesellschaften.

Technische und organisatorische Maßnahmen, § 9 BDSG

Vor allem Eingabekontrolle, Verfügbarkeitskontrolle, getrennte Verarbeitung nach unterschiedlichen Zwecken.

Automatisierte Einzelentscheidung, § 6a BDSG

Scoringverfahren

Personenbezogene Daten des potentiellen Kunden werden unter Verwendung mathematisch-statistischer Verfahren für die Einschätzung des zukünftigen Zahlungsverhaltens ausgewertet. Das Ergebnis sind Positiv- oder Negativpunkte, der sogenannte „Score“. Weist der Kunde ein Persönlichkeitsprofil auf, bei dem aufgrund des Verhaltens anderer Personen mit gleichen Merkmalen die statistische Vermutung dafür spricht, dass er seinen Zahlungsverpflichtungen wahrscheinlich nicht nachkommen wird, so erhält er keinen Kredit oder keine auf Rechnung gelieferte Ware.

Der Betroffene soll vor solchen belastenden Bewertungsentscheidungen, die ausschließlich auf eine automatisierte Verarbeitung gestützt sind, durch § 6a BDSG geschützt werden.

§ 6a Abs. 1., 1. Alternative BDSG: die Entscheidung zieht eine rechtliche Folge nach sich.

§ 6a Abs. 1., 2. Alternative BDSG: die Entscheidung beeinträchtigt den Betroffenen erheblich.

Ausnahmen nach § 6a Abs. 2 BDSG

- dem Begehren des Betroffenen wird statt gegeben.
- Die berechtigten Interessen des Betroffenen werden gewährleistet.
Beispiel: der Betroffene hat die Möglichkeit seinen Standpunkt zu wahren, widerspricht der Betroffene, so wird auf die Ermittlung des Scorewerts verzichtet.

Nach § 6a Abs. 3 BDSG besteht der Auskunftsanspruch auf den logischen Aufbau der automatisierten Verarbeitung. Hierdurch soll veranschaulicht werden, was mit den Daten des Betroffenen geschieht.

Videüberwachung, § 6b BDSG

Adressat der Regelung sind öffentliche Stellen des Bundes und nicht öffentliche Stellen.

Beobachtung ohne eine Speicherung der Bilder ist nach § 6b Abs. 1 BDSG zulässig zur Überwachung öffentlicher Räume, zur Wahrnehmung des Hausrechts und anderer berechtigter Interessen, wie der Gebäudesicherheit.

Nach § 6b Abs. 2 BDSG muss die Videüberwachung erkennbar sein.

Zulässigkeit der Verarbeitung oder Nutzung der erhobenen personenbezogenen Daten gemäß § 6a Abs. 3 BDSG nur soweit die Verarbeitung erforderlich ist, z.B. wegen Rechtsverfolgung.

Benachrichtigung des Betroffenen nach § 6a Abs. 4 BDSG, wenn der Betroffene identifizierbar ist, z.B. Videüberwachung in Arbeitsräumen.

Löschungspflicht der Daten, wenn sie nicht mehr erforderlich sind, § 6a Abs. 5 BDSG.

Mobile personenbezogene Speicher und Verarbeitungsmedien, § 6c BDSG

Definition nach § 3 Abs. 10 BDSG:

- Ausgabe an den Betroffenen (Nr. 1).
- Automatisierte Verarbeitung über die Speicherung hinaus (Nr. 2).
- Der Betroffene kann die Verarbeitung nur durch den „Gebrauch“ des Mediums beeinflussen (Nr. 3).

Dies sind Chipkarten, Smart Cards, Karten mit aktiver RFID-Funktion, die mit einem eigenen Prozessor ausgestattet sind, der mehr Verarbeitungsvorgänge ermöglicht, als das Lesen der auf der Karte aufgebrachten Daten. Hierunter fallen also nicht „Karten“, die nur eine Lesemöglichkeit eröffnen, wie Pässe, die mit automatisiert auswertbaren biometrischen Daten ausgestattet sind.

Gebrauch: das Medium wird in Kontakt mit einem Lesegerät gebracht. Hierunter fallen nicht Mobiltelefone, da diese der Nutzer durch Eingabe von Befehlen steuert.

Die Stelle, die das Medium ausgibt,

- muss den Betroffenen unterrichten (§ 6c Abs. 1 BDSG),
- muss die zur Auskunft erforderlichen Geräte zur Verfügung halten (§ 6c Abs. 2 BDSG),
- muss die Verarbeitung erkennbar machen, § 6c Abs. 3 BDSG.

Automatisierte Verarbeitung, § 10 BDSG

Beispiele:

Seit dem Auslaufen der Steueramnestie am 1. April 2005 können Finanzämter und Sozialbehörden in Bankencomputern Stammdaten abrufen.

In einem Konzern kann die zentrale Personaldatenverarbeitungsgesellschaft bei den Tochtergesellschaften Personaldaten abrufen. Dies gilt soweit sie nicht Auftragsdatenverarbeiter ist.

Anforderungen an die Zulässigkeit:

- § 10 Abs. 1 BDSG: Angemessenheit zwischen dem schutzwürdigen Interesse des Betroffenen und dem Geschäftszweck der abrufenden Stelle.
Gegeben bei Massenübermittlungen.
- § 10 Abs. 2 BDSG: Kontrollmöglichkeit durch schriftliche Festlegung des Abrufverfahrens.
- § 10 Abs. 3 BDSG: Die zum Abruf berechtigte Stelle trägt die Verantwortung für die Zulässigkeit des Abrufverfahrens.

Technische und organisatorische Maßnahmen, § 9 BDSG

Es handelt sich um Maßnahmen der Datensicherheit, die in der Anlage zu § 9 Satz 1 BDSG konkretisiert sind.

Neben der Zutrittskontrolle, der Zugangskontrolle, der Zugriffskontrolle, der Weitergabekontrolle soll gewährleistet werden,

- dass kontrolliert werden kann wer Daten in ein Datenverarbeitungssystem eingegeben, verändert, entfernt hat (Eingabekontrolle),
- dass Daten gegen Verlust geschützt sind (Verfügbarkeitskontrolle),
- dass Daten zu unterschiedlichen Zwecken getrennt verarbeitet werden.